COMMONWEALTH OF MASSACHUSETTS | STANDARD CONTRACT FORM

This form is jointly issued and published by the Office of the Comptroller, the Executive Office for Administration and Finance, and the Operational Services Division as the default contract for all Commonwealth Departments when another form is not prescribed by regulation or policy. The Commonwealth deems void any changes made on or by attachment (in the form of addendum, engagement letters, contract forms or invoice terms) to the terms in this published form or to the Standard Contract Form Instructions and Contractor Certifications, the Commonwealth Terms and Conditions, the Commonwealth Terms and Conditions for Human and Social Services, or the Commonwealth IT Terms and Conditions which are incorporated by reference herein. Additional non-conflicting terms may be added by Attachment. Contractors are required to access forms at macomptroller.org/forms or mass.gov/lists/osd-forms.

CONTRACTOR INFORMATION		COMMONWEALTH INFORMATION	
Contractor Legal Name Massachusetts Behavioral Health Partnership		**Department** Executive Office of Health and Human Services	**MMARS Code** EHS
d/b/a		**Contract Manager Name** Alejandro Garcia Davalos	
Legal Address *As entered on Form W-9 or Form W-4* 200 State Street, Suite 305, Boston, MA 02109		**Business Mailing Address** One Ashburton Place, 11th Fl., Boston, MA 02108	
Contract Manager Name Jill Lack		**Billing Address** *If Different* 600 Washington Street, Boston, MA 02111	
Phone 571-837-1457	**Fax**	**Phone** 781-227-1913	**Fax**
Email Jill.Lack@carelon.com		**Email** Alejandro.E.GarciaDavalos@mass.gov	
Vendor Code VC 6000182737		**MMARS Doc ID(s)** N/A	
Vendor Code Address ID *e.g. "AD001".* AD 001 *Note: The Address ID must be set up for Electronic Funds Transfer (EFT) payments.*		**RFR/Procurement or Other ID Number** BD-22-1039-EHS01-EHS01-70615	

○ NEW CONTRACT

Procurement or Exception Type (Check one option only)

☐ **Statewide Contract**
(OSD or an OSD-designated department.)

☐ **Collective Purchase**
(Attach OSD approval, scope, and budget.)

☐ **Department Procurement** - *Includes all Grants 815 CMR 2.00.*
(Attach Solicitation Notice or RFR, and Response or other procurement supporting documentation.)

☐ **Emergency Contract**
(Attach justification for emergency, scope, and budget.)

☐ **Contract Employee**
(Attach Employee Status Form, scope, and budget.)

☐ **Interim Contract with new Contractor**
(Attach justification for Interim Contract and updated scope/budget.)

☐ **Other Procurement Exception**
(Attach authorizing language, legislation with specific exemption or earmark, and exception justification, scope, and budget.)

◉ CONTRACT AMENDMENT

Current Contract End Date *PRIOR* to Amendment	Amendment Amount *Or Enter "No Change"*
December 31, 2027	No Change

Amendment Type
Check one option only. Attach details of amendment changes.

☑ **Amendment to Date, Scope, or Budget**
(Attach updated scope and budget.)

☐ **Interim Contract with Current Contractor**
(Attach justification for Interim Contract and updated scope/budget.)

☐ **Contract Employee**
(Attach any updates to scope or budget.)

☐ **Other Procurement Exception**
(Attach authorizing language/justification and updated scope/budget.)

TERMS AND CONDITIONS

The Standard Contract Form Instructions and Contractor Certifications and the following document are incorporated by reference into this Contract and are legally binding.
Check ONE option:

◉ *Commonwealth Terms and Conditions* ○ *Commonwealth Terms and Conditions for Human and Social Services* ○ *Commonwealth IT Terms and Conditions*

COMPENSATION

Check ONE option.

The Department certifies that payments for authorized performance accepted in accordance with the terms of this Contract will be supported in the state accounting system by sufficient appropriations or other non-appropriated funds, subject to intercept for Commonwealth owed debts under 815 CMR 9.00.

◉ **Rate Contract (No Maximum Obligation).** *(Attach details of all rates, units, calculations, conditions or terms and any changes if rates or terms are being amended.)*

○ **Maximum Obligation Contract.** *Total maximum obligation for total duration of this contract (or new total if contract is being amended):*

MMARS Doc ID(s) N/A

PROMPT PAYMENT DISCOUNTS (PPD)

Commonwealth payments are issued through Electronic Funds Transfer (EFT) 45 days from invoice receipt. See Prompt Pay Discounts Policy.

Contractors requesting accelerated payments must identify a PPD as follows:

Payment issued within:	**10 days**	*% PPD.*
	15 days	*% PPD.*
	20 days	*% PPD.*
	30 days	*% PPD.*

If PPD percentages are left blank, identify reason:

☐ **Statutory/legal** ☐ **Ready Payments** (*M.G.L. c. 29, § 23A*) ☑ **Agree to standard 45-day cycle** ☐ **Only initial payment**

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE or REASON FOR AMENDMENT

Enter the Contract title, purpose, fiscal year(s) and a detailed description of the scope of performance or what is being amended for a Contract Amendment.
Attach all supporting documentation and justifications.

The First Amended and Restated MBHV Contract includes various updates to programmatic policy, effective 1/1/2026: required updates for RY26 rates and programmatic policy changes.

SUPPLIER DIVERSITY PROGRAM (SDP) PLAN

Does the Supplier Diversity Program apply?

○ **YES** *If YES, the Contractor's annual SDP commitment for this Contract is*

◉ **NO** *If NO, and the department is an Executive Department, enter the appropriate exemption:* Insurance.

ANTICIPATED START DATE *(Complete ONE option only.)*

The Department and Contractor certify for this Contract, or Contract Amendment, that Contract obligations:

◉ *1. may be incurred as of the Effective Date (latest signature date below) and no obligations have been incurred prior to the Effective Date.*

○ *2. may be incurred as of , **20** , a date **LATER** than the Effective Date below and **no** obligations have been incurred **prior** to the Effective Date.*

○ *3. were incurred as of , **20** , a date **PRIOR** to the Effective Date below, and the parties agree that payments for any obligations incurred prior to the Effective Date are authorized to be made either as settlement payments or as authorized reimbursement payments, and that the details and circumstances of all obligations under this Contract are attached and incorporated into this Contract. Acceptance of payments forever releases the Commonwealth from further claims related to these obligations.*

CONTRACT END DATE

Contract performance shall terminate as of December 31 *,* **20** 27 *, with no new obligations being incurred after this date unless the Contract is properly amended, provided that the terms of this Contract and performance expectations and obligations shall survive its termination for the purpose of resolving any claim or dispute, for completing any negotiated terms and warranties, to allow any close out or transition performance, reporting, invoicing or final payments, or during any lapse between amendments.*

CERTIFICATIONS

Notwithstanding verbal or other representations by the parties, the **"Effective Date"** *of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified above, subject to any required approvals. The Contractor certifies that they have accessed and reviewed all documents incorporated by reference as electronically published and the Contractor makes all certifications required under the Standard Contract Form Instructions and Contractor Certifications under the pains and penalties of perjury, and further agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein according to the following hierarchy of document precedence, the applicable Commonwealth Terms and Conditions, this Standard Contract Form, the Standard Contract Form Instructions and Contractor Certifications, the Request for Response (RFR) or other solicitation, the Contractor's Response (excluding any language stricken by a Department as unacceptable), and additional negotiated terms, provided that additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.*

AUTHORIZING SIGNATURE FOR THE CONTRACTOR *Signature and date must be captured at time of signature.*			**AUTHORIZING SIGNATURE FOR THE DEPARTMENT** *Signature and date must be captured at time of signature.*		
Signature		**Date** 12/22/25	**Signature** Mike Levine (Dec 22, 2025 15:53:37 EST)		**Date** 12/22/2025
Print Name Jill Lack	**Print Title** CEO		**Print Name** Mike Levine	**Print Title** Undersecretary	

COMMONWEALTH OF MASSACHUSETTS

EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

Managed Behavioral Health Vendor Contract

Between the

EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

1 ASHBURTON PLACE

BOSTON, MA 02108

and

THE MASSACHUSETTS BEHAVIORAL HEALTH PARTNERSHIP

1000 WASHINGTON STREET

BOSTON, MA 02118

This Managed Behavioral Health Vendor Contract is by and between the Massachusetts Executive Office of Health and Human Services ("EOHHS," or "MassHealth") and the Massachusetts Behavioral Health Partnership (MBHP), a general partnership under BeaconHealth Options Inc., of Boston, MA, with principal offices at 1000 Washington Street, Boston, MA 02118 ("Contractor").

WHEREAS, The Massachusetts Executive Office of Health and Human Services (EOHHS) is the single state agency responsible for administering the Medicaid program and the state's Children's Health Insurance Program (CHIP) within Massachusetts (collectively, MassHealth), pursuant to M.G.L. c.118E, Title XIX of the Social Security Act (42 U.S.C. § 1396 et seq.), Title XXI of the Social Security Act (42 U.S.C. § 1397aa et seq.), and other applicable laws and waivers; and

WHEREAS, EOHHS issued a Request for Responses For a Vendor to Provide a Comprehensive Behavioral Health Program and Management Support Services, and DMH Specialty Programs on March 17, 2022 (the RFR); and

WHEREAS, EOHHS selected the Contractor, based on their response to the RFR submitted by the deadline for responses, to provide behavioral health services to MassHealth members, as set forth in the RFR and the Contract; and

WHEREAS, EOHHS seeks and the Contractor agrees to provide innovative, cost-effective, high-quality care management services, network management services, quality management activities and comprehensive Behavioral Health Services for certain MassHealth members, including but not limited to a Care Management Program for individual Enrollees with complex medical and/or behavioral health conditions; and

WHEREAS, EOHHS seeks and the Contractor agrees to continue and enhance recovery, resiliency, family-centered and strength-based approaches to the provision of care; and

WHEREAS, EOHHS seeks and the Contractor agrees to develop a robust medical and behavioral health system of care, that is integrated both at the system level and at the individual level in order to improve health care outcomes for MassHealth members; and

WHEREAS, EOHHS seeks to implement the Commonwealth's payment reform initiatives to promote the most efficient and effective use of resources; and

WHEREAS, EOHHS and the Contractor enter this Contract with an Operational Start Date of January 1, 2023, and entered into various amendments thereafter; and

WHEREAS, in accordance with **Section 5.8** of the Contract, EOHHS and the Contractor desire to amend and restate the Contract effective January 1, 2026, and

WHEREAS, the parties agree that the rates and terms stated herein are subject to the approval of the federal Centers for Medicare and Medicaid Services (CMS);

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the Contractor and EOHHS agree as follows:

TABLE OF CONTENTS

Section 1. Definitions and Acronyms 1

Section 1.1 Definitions 1

Section 1.2 Acronyms 22

Section 2. Contractor Responsibilities 26

Section 2.1 Compliance 26

Section 2.2 Contract Transition/Contract Readiness 26

Section 2.3 Administration and Contract Management 36

Section 2.4 Enrollment and Education Activities 64

Section 2.5 Care Management, Care Coordination and Supporting Dispositions from the ED 67

Section 2.6 Covered Services 80

Section 2.7 BH Provider Contracts and Related Responsibilities 130

Section 2.8 BH Provider Network and Network Management 168

Section 2.9 Accessibility and Availability of BH Covered Services 193

Section 2.10 Customer Services for Covered Individuals 199

Section 2.11 Marketing Activity Requirements 208

Section 2.12 Inquiries, Ombudsman Services, Grievances, and Appeals 211

Section 2.13 Quality Management and Quality Improvement 225

Section 2.14 Data Management, Information Systems, and Reporting Requirements 235

Section 2.15 Financial Stability Requirements 249

Section 2.16 Operational Audits 257

Section 2.17 Additional Enrollee Groups 257

Section 2.18 Third-Party Liability Benefit Coordination and Recovery 258

Section 2.19 PCC Plan Support Services (PSS) Program 260

Section 2.20 Health Equity 270

Section 2.21 COVID-19 Efforts 276

Section 3. EOHHS Responsibilities 278

Section 3.1 Contract Management 278

Section 3.2 Coordination of Benefits 281

Section 3.3 Enrollment and Disenrollment 281

Section 3.4 Information Systems 282

Section 3.5 Marketing 282
Section 3.6 Additional Covered Individual Groups 283
Section 4. Payment and Financial Provisions 284
Section 4.1 Rating Categories (RCs) for Covered Individuals 284
Section 4.2 Payment Provisions and Methodologies 285
Section 4.3 Payment Reconciliation Process 298
Section 4.4 BH Covered Services Continuing Services Reconciliation 301
Section 4.5 In-State Acute Hospital Add-on/Pursuant to Section 2.7.F.3.n 302
Section 4.6 Performance Incentive Arrangements 302
Section 4.7 Risk-Sharing Arrangements 304
Section 4.8 Reinsurance 306
Section 4.9 Option to Audit 306
Section 4.10 Behavioral Health Quality Incentive Payment 306
Section 4.11 Clinical Quality Incentive for Acute Hospitals 306
Section 4.12 Community Behavioral Health Incentive Program 307
Section 5. Additional Terms and Conditions 308
Section 5.1 Administration 308
Section 5.2 Data Privacy and Security (including Health Insurance Portability and Accountability Act (HIPAA)) 316
Section 5.3 General Terms and Conditions 322
Section 5.4 Record Retention, Inspection and Audit 335
Section 5.5 Termination of Contract 336
Section 5.6 Contract Term 339
Section 5.7 Additional Modifications to the Contract Scope 339
Section 5.8 Amendments 340
Section 5.9 Order of Precedence 341
Section 5.10 Managed Care Activities Vacated by the Court 342
Section 5.11 Written Notices 342

LIST OF APPENDICES

Appendix A: Clinical Services

A-1 Behavioral Health Covered Services

A-2 Required Network Provider Lists

Appendix B: Contract Compliance

B-1 Contract Implementation Readiness Review

B-2 Material Subcontractor Checklist

B-3 Federally Required Disclosures

Appendix C: PCC Plan Provider Contract

Appendix D: Encounter Data Set Request

D-1 Paid Claims Encounter Data Set Request

D-2 Denied Claims Encounter Data Set Request

D-3 Standardized Encounter Data Program (SENDPro) Specifications (PLACEHOLDER)

Appendix E: Reports and Certifications

E-1 Program Reporting Requirements

E-2 Certification of Data Accuracy

E-3 Annual Certification

E-4 Financial Reports

Appendix F: Incident Report Form

Appendix G: Behavioral Health Incentives

Appendix H: Payment Provisions

H-1 Payment and Risk-Sharing Provisions

H-2 Performance Guarantee Requirements

Appendix I: [Reserved]

Appendix J: Credentialing Websites

Appendix K: Data Management and Confidentiality

K-1 Data Management and Confidentiality Agreement

K-2 Artificial Intelligence

Appendix L: Commonwealth of Massachusetts Behavioral Health Minimum Fee Schedule, Unique Code/Modifier Combinations

Appendix M: [Reserved]

Appendix N: [Reserved]

Appendix O: Health Related Social Needs (HRSN) Supplemental Services

Appendix P: Behavioral Health Network Availability Standards

Section 1. DEFINITIONS AND ACRONYMS

Section 1.1 Definitions

The following terms appearing capitalized throughout this Contract and its Appendices have the following meanings unless the context clearly indicates otherwise.

N.B.: The word "day," whenever it appears in these documents, refers to a calendar day unless otherwise specified.

Abuse – actions or inactions by Providers (including the Contractor) and/or Members that are inconsistent with sound fiscal, business or medical practices, and that result in unnecessary cost to the MassHealth program, including, but not limited to practices that result in MassHealth reimbursement for services that are not Medically Necessary, or that fail to meet professionally recognized standards for health care.

Accountable Care Organization (ACO) – a provider-led entity that contracts with MassHealth to provide a managed comprehensive set of covered services to a MassHealth member who chooses to or is assigned to received care from a Primary Care Provider (PCP) within the ACO's provider network. ACOs include Accountable Care Partnership Plans (ACPPs) and Primary Care ACOs (PCACOs).

Actuarially Sound Capitation Rates – capitation rates that, as described in 42 CFR 438.4, have been developed in accordance with generally accepted actuarial principles and practices; are appropriate for the populations to be covered and the services to be furnished under the contract; have been certified as meeting the requirements of 42 CFR 438.4 by actuaries who meet the qualification standards established by the American Academy of Actuaries and follow the practice standards established by the Actuarial Standards Board; and have been approved by CMS. This includes capitation rates based on public or private payment rates for comparable services for comparable populations, consistent with actuarially sound principles as defined at 42 CFR 457.10

Adjustment – a compromise between the Contractor and the Covered Individual reached at any time after an Adverse Action but before the BOH issues a decision on a BOH Appeal.

Administrative Component of the BH Covered Services Capitation Rate – a Per-Member (Covered Individual) Per-Day rate paid by EOHHS to the Contractor for the administration of the BH Covered Services for the applicable Rating Category according to **Section 4** and **Appendix H-1**.

Adverse Action – any one of the following actions or inactions by the Contractor shall be considered an Adverse Action:

(1) the failure to provide MassHealth Covered Services in a timely manner in accordance with the accessibility standards in **Section 2.9**;

(2) the denial or limited authorization of a requested service, including the determination that a requested service is not a MassHealth Covered Service;
(3) the reduction, suspension, or termination of a previous authorization by the Contractor for a service;
(4) the denial, in whole or in part, of payment for a service, where coverage of the requested service is at issue; provided that procedural denials for requested services do not constitute Adverse Actions, including but not limited to denials based on the following:
    - failure to follow prior authorization procedures;
    - failure to follow referral rules;
    - failure to file a timely Claim;
(5) the failure to act within the timeframes for making authorization decisions; and
(6) the failure to act within the timeframes for reviewing an Internal Appeal and issuing a decision.

Alternative Formats – provision of Covered Individual Information in a format that takes into consideration the special needs of those who, for example, are visually limited or have limited reading proficiency. Examples of Alternative Formats shall include, but not be limited to, Braille, large font, audio tape, video tape, and Covered Individual Information read aloud to a Covered Individual by the Contractor's customer services representative.

Alternative Lock-up Programs – Human service agencies contracted with the Commonwealth of Massachusetts Department of Children and Families to provide a temporary placement resource for the Commonwealth of Massachusetts state and local police departments in their efforts to comply with federal and state regulations regarding the placement of juveniles in their custody for either status or non-violent delinquent offenses.

AMCI Amount – the total amount paid for AMCI services provided under the Contract to Uninsured Individuals and persons covered by Medicare only.

Appeal Representative – any individual that the Contractor can document has been authorized by the Covered Individual in writing to act on the Covered Individual's behalf with respect to all aspects of a Grievance, Internal Appeal, or BOH Appeal. The Contractor must allow a Covered Individual to give a standing authorization to an Appeal Representative to act on his/her behalf for all aspects of Grievances and Internal Appeals. Such standing authorization must be done in writing according to the Contractor's procedures, and may be revoked by the Covered Individual at any time. When a minor is able, under law, to consent to a medical procedure, that minor can request an appeal of the denial of such treatment without parental/guardian consent and appoint an Appeal Representative without the consent of a parent or guardian.

ASD-ID for MCPAP Regional Behavioral Health Team – a unit of contracted and credentialed providers responsible for specific geographic centers across the state, which are affiliated with MCPAP Teams. Each unit shall include at least one Licensed Applied Behavior Analyst.

ASD-ID for MCPAP Statewide Physician Consultation Team – a single centralized team of contracted and credentialed providers consisting of at least one full time equivalent physician specialized in treating ASD-ID (e.g., psychiatrist, neurologist).

Autism Spectrum Disorder-Intellectual Disability (ASD-ID) for MCPAP – a statewide program in the Commonwealth to assist Behavioral Health providers and medical professionals in supporting the mental and Behavioral Health of individuals up to age 26 with Autism Spectrum Disorder - Intellectual Disability (ASD-ID). Through ASD-ID for MCPAP, providers can consult with a Licensed Applied Behavior Analyst and ASD-ID-specialized prescribers. ASD-ID for MCPAP improves AMCI/YMCI and emergency department providers' competencies in behavioral assessment and intervention, parent coaching, and in making effective referrals for patients who need community-based services and provides access to pharmacological consultation on an emergency basis.

Autism Support Center – a center that provides an array of information and referral services, resources, and supports to children and young adults with autism spectrum disorder.

Barrier – something that bars access to or gets in the way of obtaining Behavioral Health Treatment. This could be stigma, discrimination, transportation, insurance, cost, language, etc**.**

Behavioral Health (BH) – the promotion of emotional health; the prevention of mental illnesses and substance use disorders; and treatments and services for mental and/or substance use disorders.

Behavioral Health Clinical Assessment – the comprehensive clinical assessment of a Covered Individual that includes a full bio-psycho-social and diagnostic evaluation that informs Behavioral Health treatment planning. It is performed when a Covered Individual begins Behavioral Health treatment and is reviewed and updated during the course of treatment. Behavioral Health Clinical Assessments provided to Covered Individuals under the age of 21 require the use of the CANS Tool to document and communicate assessment findings.

Behavioral Health Community Partner (BHCP) – an entity qualified by EOHHS to work with PCACOs to coordinate Behavioral Healthcare for certain PCACO members.

Behavioral Health Covered Services (or BH Covered Services) – the services the Contractor is responsible for providing to Covered Individuals, as applicable and as described in **Appendix A-1**.

Behavioral Health Help Line – A statewide, multichannel entry point (telephone, text, chat, website, etc.) providing Behavioral Health information, resources, and referrals in a supportive, coordinated, and user-friendly approach, including 24/7 referral and dispatch to AMCI/YMCI for Behavioral Health crises.

Behavioral Health Network Provider (or BH Network Provider) – a provider that has contracted with the Contractor to provide Behavioral Health Covered Services under the BH Program.

Behavioral Health Program (BHP) – that portion of the Contract related to the administration, coordination, delivery and management of the BH Covered Services described in **Appendix A-1**.

Behavioral Health Supports for Justice Involved Individuals (BH-JI) – BH-JI Supports involve a range of functions that assist MassHealth Covered Individuals with justice involvement, either currently incarcerated or detained in a correctional facility, released from a correctional institution within one year, or who are under the supervision of the Massachusetts Probation Service or the Massachusetts Parole Board, in navigating and successfully engaging with health care services, with an emphasis on Behavioral Health services. BH-JI Supports include in-reach and re-entry supports for individuals released from correctional facilities as well as community supports post-release. When directed by EOHHS, the community supports for managed care Covered Individuals post-release will be administered by MassHealth Plans as CSP-JI as described in **Section 2.6.D.7**.

Behavioral Health Treatment and Referral Platform – a web-based searchable database that contains up-to-date information on the number of available beds for admission to psychiatric hospitals.

Behavioral Health Urgent Care (BHUC) Program – the delivery of same-day or next-day appointments for diagnostic evaluation of new clients and urgent appointments for existing clients; psychopharmacology appointments and Medication for Addiction Treatment (MAT) and Medication for Opioid Use Disorder (MOUD) within a timeframe defined by EOHHS; all other treatment appointments within 14 calendar days; and extended availability outside of weekday hours between 9am and 5pm, as specified by EOHHS and provided by certain Mental Health Centers (MHC) designated to provide BHUC, or other providers as directed by EOHHS.

Board of Hearings (BOH) – the Board of Hearings within the Executive Office of Health and Human Services' Office of Medicaid.

BOH Appeal – a written request to the BOH, made by a Covered Individual or Appeal Representative, to review the correctness of an Internal Appeal decision by the Contractor.

Bureau of Substance Addiction Services (BSAS) – a division of the Massachusetts Department of Public Health (DPH) that is responsible for setting substance use policy in the Commonwealth.

Calendar Year – the 12-month period beginning January 1 of each year.

Capitation Rate – The Administrative Component and Medical Component of the BH Covered Services Capitation Rate for the applicable Rating Category according to **Section 4** and **Appendix H-1**.

Care Coordination – management of care activities performed by the Contractor on behalf of a Covered Individual to improve health outcomes and may include medical, Behavioral Health, and pharmacy management and medication reconciliation among providers, agencies, and community social supports, as described in **Section 2.5**.

Care Management Program (CMP) – the administration and provision of certain clinical management and support activities to certain Enrollees and Providers, as described in **Section 2.5**.

Care Team – a group of individuals led by the care coordinator or care manager, including the Enrollee, the Primary Care Clinician (PCC), and any other medical or Behavioral Health provider, case manager from another state agency, and any family member or other individual requested as part of the team by the Covered Individual.

Centers for Medicare and Medicaid Services (CMS) – the federal agency which oversees states' Medical Assistance programs and states' Children Health Insurance Programs (CHIP) under Titles XIX and XXI of the Social Security Act and waivers thereof.

Child and Adolescent Needs and Strengths (CANS) Tool – a tool that provides a standardized way to organize information gathered during Behavioral Health Clinical Assessments and during the discharge planning process from Inpatient Psychiatric Hospitalizations, Intensive Community-Based Acute Treatment Services, and Community-Based Acute Treatment Services. A Massachusetts version of the CANS Tool has been developed and is intended to be used as a treatment decision support tool for Behavioral Health Providers serving MassHealth Members under the age of 21.

CANS IT System – a web-based application designated by EOHHS into which Behavioral Health Providers serving MassHealth Members under the age of 21 will input: (1) the information gathered using the CANS Tool; and (2) the determination whether or not the assessed Member is suffering from a Serious Emotional Disturbance.

Certified Mental Health Peer Specialist (CPS) – a person who has been trained by an agency approved by the Department of Mental Health (DMH) who is a self-identified person with lived experience of a mental health disorder, recovery and wellness that can effectively share their experiences and serve as a mentor, advocate or facilitator for a member experiencing a mental health disorder.

Children's Behavioral Health Initiative (CBHI) – an interagency undertaking by EOHHS and MassHealth whose mission is to strengthen, expand and integrate Behavioral Health services for MassHealth Members under the age of 21 into a comprehensive system of community-based, culturally competent care.

Children's Behavioral Health Initiative Services (or CBHI Services) – any of the following services: Intensive Care Coordination (ICC), Family Support and Training, In-Home Behavioral Services (including Behavior Management Therapy and Behavior Management Monitoring) and Therapeutic Mentoring Services, In-Home Therapy Services (including Therapeutic Clinical Intervention and Ongoing Therapeutic Training and Support), Family-Based Intensive Treatment, and Youth Mobile Crisis Intervention.

Children in the Care and/or Custody of the Commonwealth – children who are Covered Individuals and who are in the care or protective custody of the Department of Children and

Families (DCF), or in the custody of the Department of Youth Services (DYS). Children in the Care and/or Custody of the Commonwealth are eligible to receive services through the BHP without being required to enroll in the PCC Plan or a Primary Care ACO; however, any such children who are enrolled in the PCC Plan are considered Enrollees.

Chronic Homelessness – a definition established by the U.S. Department of Housing and Urban Development (HUD) of a disabled individual who has been continuously homeless on the streets or in an emergency shelter or safe haven for 12 months or longer, or has had four or more episodes of homelessness (on the streets, or in an emergency shelter, or safe haven) over a three-year period where the combined occasions must total at least 12 months (occasions must be separated by a break of at least seven nights; stays in institution of fewer than 90 days do not constitute a break). To meet the disabled part of the definition, the individual must have a diagnosable substance use disorder, serious mental illness, developmental disability, post-traumatic stress disorder, cognitive impairment resulting from a brain injury, or chronic physical illness, or disability, including the co-occurrence of two or more of those conditions.

Claim – a Provider's bill for services, a line item of service, or all services for one Covered Individual, Uninsured Individual, or Individual without Mobile Crisis Coverage.

Clean Claim – a Claim that can be processed without obtaining additional information from the provider of the service or from a third party. It may include a Claim with errors originating from the Contractor's claims system. It does not include a Claim from a Provider who is under investigation for fraud or abuse or a Claim under review for Medical Necessity.

Clinical Criteria – the criteria used to determine the most clinically appropriate and necessary Level of Care, and intensity of services, to ensure the provision of Medically Necessary Behavioral Health Covered Services.

Cold-call Marketing – any unsolicited personal contact by the Contractor, its employees, Network Providers, agents or Material Subcontractors with a Member who is not enrolled in the PCC Plan or its BHP that EOHHS can reasonably interpret as influencing the Member to enroll in the PCC Plan or its BHP or either not to enroll in, or to disenroll from, a MassHealth managed care organization, accountable care organization, or the PCC Plan's BHP. Cold-call Marketing shall not include any personal contact between a Network Provider and a Member who is a prospective, current or former patient of that Network Provider regarding the provisions, terms or requirements of MassHealth as they relate to the treatment needs of that particular Member.

Community Behavioral Health Center (CBHC) – A comprehensive community behavioral health center offering crisis, urgent, and routine substance use disorder and mental health services, care coordination, peer supports, and screening and coordination with primary care. A CBHC will provide access to same-day and next-day services and expanded service hours including evenings and weekends. A CBHC must provide services to adults and youth, including infants and young children, and their families. CBHC services for adults are collectively referred to as the "adult component," and CBHC services for youth are referred to as the "youth component." CBHCs include an Adult Mobile Crisis Intervention (AMCI), Youth Mobile Crisis

Intervention (YMCI), Adult Crisis Stabilization (Adult CCS) and Youth Crisis Stabilization (YCCS).

Community Crisis Amount – the total amount paid for AMCI/YMCI, including follow-up, and Community Crisis Stabilization services provided under the Contract to Uninsured Individuals and persons covered by Medicare only.

Community Partner (CP) – entities qualified by EOHHS to enter into contract with PCACOs to coordinate care for certain PCACO members as further specified by EOHHS. There are two types of CPs – Long-Term Services and Supports CPs (LTSS CPs) and Behavioral Health CPs (BH CPs).

Community Service Agency (CSA) – a community-based Behavioral Health provider organization whose function is to facilitate access to the continuum of Behavioral Health services by providing an organized pathway to care for children and families where the child is referred for Intensive Care Coordination. A primary mechanism through which CSAs serve this function is as the provider of Intensive Care Coordination and Family Support and Training Services, which are defined as BH Covered Services.

Continuing Services – BH Covered Services that were previously authorized by the Contractor and are the subject of an Internal Appeal or BOH Appeal, if applicable, involving a decision by the Contractor to terminate, suspend, or reduce the previous authorization and which are provided by the Contractor pending the resolution of the Internal Appeal or BOH Appeal, if applicable.

Contract – this agreement executed between the Contractor and EOHHS pursuant to EOHHS's Request for Responses (RFR) for a Vendor to Provide a Comprehensive Behavioral Health Program and Management Support Services, and DMH Specialty Programs issued March 17, 2022, and any amendments thereto. This Managed Behavioral Health Vendor Contract incorporates by reference all attachments and appendices to the RFR relative to the programs included in this Contract, including the Contractor's response to the RFR.

Contract Year – A twelve-month period commencing January 1 and ending December 31, unless otherwise specified by EOHHS.

Contractor – the entity that executes this Contract with EOHHS.

Correctional Facility – Any state prison, county jail or house of correction, or youth correctional facility in the Commonwealth of Massachusetts.

Coverage Type – a scope of medical services, other benefits, or both, that are available to individuals who meet specific MassHealth eligibility criteria. Coverage Types for this Contract include MassHealth Standard, CommonHealth, Family Assistance, and CarePlus. See 130 CMR 450.105 for an explanation of each Coverage Type.

Covered Individual – a MassHealth Member who is eligible to receive Behavioral Health Covered Services under the Contract, including PCC Plan Enrollees, Members enrolled in a

Primary Care ACO, Children in the Care and/or Custody of the Commonwealth, and children in MassHealth Standard or CommonHealth with other insurance.

Covered Individual at Risk of Homelessness – any Covered Individual who does not have sufficient resources or support networks (e.g., family, friends, faith-based or other social networks) immediately available to prevent them from moving to an emergency shelter or another place not designed for or ordinarily used as a regular sleeping accommodation for human beings.

Covered Individual Days – the sum of the number of days each Covered Individual is enrolled with the Contractor.

Covered Individual Experiencing Homelessness – any Covered Individual who lacks a fixed, regular, and adequate nighttime residence who: (1) has a primary nighttime residence that is a public or private place not designed for or ordinarily used as a regular sleeping accommodation for human beings including a car, park, abandoned building, bus or train station, airport, or camping group; or (2) is living in a supervised publicly or privately operated emergency shelter designated to provide temporary living arrangements, including congregate shelters, transitional housing, and hotels and motels paid for by charitable organizations or by federal, state, or local government programs for low-income individuals.

Covered Individual Information – information about the Contractor for Covered Individuals that includes, but is not limited to, a Provider Directory that meets the requirements of **Section 2.7.G**, and a Covered Individual Handbook that meets the requirements of **Section 2.10.A.3**.

Credentialing Criteria – criteria that a Provider must meet to be qualified as a Network Provider.

Crisis Prevention/Response Plan – a plan directed by the Covered Individual, or in the case of Covered Individuals under age 18, their legal guardian, designed to expedite a consumer- or family-focused clinical disposition in the event of a psychiatric crisis, based on the experience gained from past treatment. The Crisis Prevention Plan provides a thorough checklist of the triggers that may lead to or escalate a psychiatric crisis and strategies that the individual and providers may use to support de-escalation. The plan also includes potential clinical presentations and a preferred disposition and treatment plan for each of these presentations as well as the Covered Individual's preferences with respect to involvement of the Covered Individual, his/her family and other supports, such as Behavioral Health providers, community social service agencies, and natural community supports. With the Covered Individual's consent, the plan may be implemented by an AMCI or YMCI provider, CBHC, other BH Network Provider, the PCC, the staff from the CSA, or another provider. This type of plan may also be referred to as a Wellness Recovery Action Plan (WRAP) for adults with Severe and Persistent Mental Illness (SPMI), and a Risk Management Safety Plan for children with Severe Emotional Disturbance (SED) and their families.

Crisis Service Safety Initiative (also referred to as Living Room Model) – a peer-delivered alternative to traditional clinical emergency services that provides a safe space, allowing an individual experiencing a mental health crisis to access direct, mutual support with peers.

Culturally and Linguistically Appropriate Services (CLAS) – the National CLAS Standards are intended to advance health equity, improve quality, and help eliminate health care disparities by establishing a blueprint for health and health care organizations. CLAS aims to provide effective, equitable, understandable, and respectful quality care and services that are responsive to diverse cultural health beliefs and practices, preferred languages, health literacy, and other communication needs.

Date of Action – the effective date of an Adverse Action.

Deliverable – any tangible work product, including but not limited to, a report, a document, or other building block of an overall project, whether in hard copy or electronic form, specifically created or developed in accordance with the terms of the Contract.

Department of Children and Families (DCF) – the department within the Massachusetts Executive Office of Health and Human Services that provides social services to children and families.

Department of Developmental Services (DDS) – the department within the Massachusetts Executive Office of Health and Human Services that provides supports for individuals with intellectual and developmental disabilities.

Department of Mental Health (DMH) – the department within the Massachusetts Executive Office of Health and Human Services designated as the Commonwealth's mental health authority pursuant to M.G.L. c. 19 and M.G.L. c. 123, et seq.

Department of Youth Services (DYS) – the juvenile justice agency in Massachusetts.

Direct Costs – Contractor-incurred costs directly related to the administration of the Contract. Direct Costs include but are not limited to: clinical, administrative, technical and support staff assigned to the Contract; and related administrative expenses. Direct Costs do not include federal and state taxes except sales tax and taxes attributable to personnel.

Direct Service Reserve Account (DSRA) – an interest-bearing trust account maintained by the Contractor in a bank located in Massachusetts and approved by EOHHS in accordance with the provisions of the Contract, into which payments to the Contractor are deposited when paid by EOHHS.

Discharge Planning – the evaluation of a Covered Individual's medical and Behavioral Health care needs and coordination of any other support services in order to arrange for safe and appropriate care after discharge from one Level of Care to another Level of Care, including referral to appropriate services.

Dual Diagnosis – co-occurring mental health and substance use conditions.

Effective Date of Enrollment – as of 12:01 a.m. on the first day, as determined by EOHHS, on which the Contractor is responsible for providing the activities described in this Contract, to an Enrollee and as reflected in the HIPAA 834 Outbound Enrollment File.

Effective Date of Disenrollment – up to 11:59 p.m. on the last day, as determined by EOHHS, on which the Contractor is responsible for providing the activities described in this Contract to an Enrollee and as reflected in the HIPAA 834 Outbound Enrollment File.

Eligible Days – depending on the context, the total number of days in a month for which Covered Individuals were eligible for Behavioral Health Covered Services, as determined by EOHHS; or the total number of days in a month for which Enrollees were eligible for the PCC Plan, as determined by EOHHS.

Eligibility Verification System (EVS) – EOHHS's computerized system for verifying MassHealth Member eligibility.

Emergency Department Crisis Evaluation Payment – payment for initial crisis evaluation services in the emergency department provided under the Contract when not covered otherwise to Uninsured Individuals and persons covered by Medicare only.

Emergency Medical Condition – a medical condition, whether physical or mental, manifesting itself by acute symptoms of sufficient severity, including severe pain, that, in the absence of prompt medical attention, could reasonably be expected by a prudent layperson who possesses an average knowledge of health and medicine to result in placing the health of a beneficiary or another person or, in the case of a pregnant woman, the health of the woman or her unborn child, in serious jeopardy, serious impairment to bodily function, or serious dysfunction of any body organ or part; or, with respect to a pregnant woman, as further defined in Section 1867(e)(1)(B) of the Social Security Act. (42 U.S.C. § 1395dd(e)(1)(B).)

Emergency Services – MassHealth Covered Services that are furnished to a Covered Individual by a provider qualified to furnish such services under Title XIX of the Social Security Act, and that are needed to evaluate or stabilize a Covered Individual's Emergency Medical Condition.

Encounter – a professional contact between a patient and a provider who delivers health care services.

Engagement – in-person or telehealth encounter(s) with an Enrollee, for the purposes of completing a comprehensive health assessment, and creating and implementing an Individual Care Plan (ICP).

Engagement Rate – the number of Participants in the Care Management Program as a percent of the total number of Enrollees successfully engaged for whom the Contractor conducts outreach for the CMP.

Engagement Target – the minimum projected number of Enrollees in each Tier the Contractor is required to successfully enroll in the CMP each Contract Year.

Enrollee – a person determined eligible for MassHealth who is enrolled in the PCC Plan, either by choice or by assignment by EOHHS.

Enrollee Days – the sum of the number of days each Enrollee is enrolled in the PCC Plan.

Enrollment Broker – the EOHHS-contracted entity that provides MassHealth Members with assistance in enrollment into MassHealth Managed Care plans, including the PCC Plan and Primary Care ACOs.

EOHHS-Certified ENS Vendor – An ENS vendor that is certified by EOHHS under 101 CMR 20.11.

EPSDT Periodicity Schedule – the Early and Periodic Screening, Diagnosis and Treatment (EPSDT) Medical and Dental Protocol and Periodicity Schedules that appears in **Appendix W of all MassHealth provider manuals** and is developed and periodically updated by MassHealth in consultation with the Massachusetts Chapter of the American Academy of Pediatrics, Massachusetts DPH and DMH, dental professionals, the Massachusetts Health Quality Partners, and other organizations concerned with children's health. The Schedule consists of screening procedures arranged according to the intervals or age levels at which each procedure is to be provided.

Estimated Administrative Payment – a prospective monthly payment made by EOHHS to the Contractor for the administration of the BHP, based on an approximation of the number of Covered Individuals eligible for services under the Contract for that month multiplied by the applicable PMPM Administrative Component of the BH Capitation Rate.

Estimated Capitation Payment – a prospective monthly payment made by EOHHS to the Contractor, based on an approximation of the number of Covered Individuals eligible for services under the Contract for that month multiplied by the applicable PMPM Capitation Rate. The payment is made regardless of whether the Covered Individual receives services during the period covered by the payment.

Estimated PCC Plan Support Services Payment – a prospective monthly payment made by EOHHS to the Contractor, based on an approximation of the number of Enrollees in the PCC Plan multiplied by the PMPM PCC Plan Support Services Rate.

Executive Office of Health and Human Services (EOHHS) – the executive agency within Massachusetts that is the single state agency responsible for the administration of the MassHealth program (Medicaid), pursuant to M.G.L. c. 118E, Titles XIX and XXI of the Social Security Act, and other applicable laws and waivers thereto.

Expedited Psychiatric Inpatient Admission (EPIA) – an escalation protocol for securing placement for individuals in emergency departments awaiting disposition to inpatient psychiatric hospital level of care.

External Quality Review Activities (EQR Activities) – activities performed by an entity with which EOHHS contracts in accordance with 42 CFR 438.350 through 42 CFR 438.370.

External Quality Review Contractor (EQR Contractor) – the entity with which EOHHS contracts to perform External Quality Review Activities.

Fast Healthcare Interoperability Resources (FHIR) – FIHR is a next-generation interoperability standard created by the standards development organization Health Level 7 (HL7®). FHIR is designed to enable health data, including clinical and administrative data, to be quickly and efficiently exchanged.

Federal Financial Participation (FFP) – the federal share of the costs associated with states' administration of entitlement programs such as the Medicaid program.

FHIR-based APIs – HL7® FHIR® includes specifications for an API, based on established web standards and modern information exchange that has been extended to create a full interoperability solution for health care.

Fraud – an intentional deception or misrepresentation made by a person or corporation with the knowledge that the deception could result in some unauthorized benefit under the MassHealth program to himself, the corporation, or some other person. It also includes any act that constitutes fraud under applicable federal or state health care fraud laws. Examples of provider fraud include: lack of referrals by PCPs to specialists, improper coding, billing for services never rendered, inflating bills for services and/or goods provided, and providers who engage in a pattern of providing and/or billing for medically unnecessary services. Examples of Covered Individual fraud include improperly obtaining prescriptions for controlled substances and card sharing.

Grievance – any expression of dissatisfaction by a Covered Individual or Appeal Representative about any action or inaction by the Contractor other than an Adverse Action. Possible subjects for Grievances include, but are not limited to, quality of care or services provided, aspects of interpersonal relationships such as rudeness of a Provider or employee of the Contractor, or failure to respect the Covered Individual's rights.

Health Disparities – avoidable differences in health outcomes experienced by people with one characteristic (e.g., race, gender, sexual orientation) as compared to the socially dominant group (e.g., white, male, cis-gender, heterosexual, etc.).

Healthcare Effectiveness Data and Information Set (HEDIS) – a standardized set of health plan performance measures developed by the National Committee for Quality Assurance (NCQA) and utilized by EOHHS and other purchasers and insurers.

Health Equity – means that everyone has a fair and just opportunity to attain their optimal health regardless of race, ethnicity, disability, gender identity, sexual orientation, or socioeconomic status. Advancing health equity is a process of addressing limited access to economic resources, education, housing, etc. When focusing specifically on racial equity in health, advancing health equity means dismantling the systemic racism that underlies differences in the opportunity to be healthy.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – federal legislation (Pub. L. 104-191, as amended), enacted to improve the continuity of health insurance coverage in group and individual markets, combat waste, fraud, and abuse in health insurance and health-care delivery, simplify the administration of health insurance and protect the confidentiality and security of individually identifiable health information.

Health Needs Assessment – a tool that identifies and quantifies an Enrollee's physical and Behavioral Health status and needs based on morbidity and mortality risk, derived from the collection and review of demographic, physical and Behavioral Health and lifestyle information.

Health-Related Social Need (HRSN) -The immediate daily necessities that arise from the inequities caused by the social determinants of health. These needs are often defined by a lack of access to basic resources like stable housing, an environment free of life-threatening toxins, healthy food, utilities including heating and internet access, transportation, physical and mental health care, safety from violence, education and employment, and social connection. When they go unmet, Health Related Social Needs not only reduce an individual's ability to take care of their health, but also increase health care costs and lead to avoidable health care utilization.

Health Safety Net – unpaid hospital charges, as defined in M.G.L. c. 118G, for Medically Necessary services provided to: (1) patients deemed financially unable to pay, in whole or in part, for their care; (2) uninsured patients who receive Emergency care for which the costs have not been collected after reasonable efforts; or (3) patients in situations of medical hardship where major expenditures for health care have been depleted or can reasonably be expected to deplete the financial resources of the individual to the extent that medical services will be unpaid.

Homeless – individuals who lack regular, fixed, and adequate nighttime residence, and who, on a temporary or permanent basis, have a primary residence that is a shelter or similar facility, or who have no primary residence and utilize public areas for sleep, shelter, and daily living activities.

HRSN Service Manual – The MassHealth manual detailing requirements for the provision of HRSN Services, which may be accessed here [https://www.mass.gov/info-details/informationfor-masshealth-acos-and-hrsn-providers].

Indian Enrollee – An individual who is an Indian (as defined in Section 4(c) of the Indian Health Care Improvement Act of 1976 (25 U.S.C. 1603(c)).

Indian Health Care Provider – an Indian Health Care Provider or an Urban Indian Organization as defined in the American Recovery and Reinvestment Act of 2009.

Indirect Costs – costs charged to the Contractor by its parent to support administration of the Contract, including management, financial or other corporate functions provided to support operation of the program, and exclusive of Direct Costs. Indirect Costs do not include federal and state taxes except sales tax and taxes attributable to personnel.

Individual Care Plan (ICP) – the plan of care developed by a Clinical Care Manager in conjunction with an individual's Care Team, when appropriate and possible. The ICP includes:

(1) the individual's detailed and comprehensive needs assessment; (2) identified short-term and long-term treatment goals; (3) a service plan to meet those goals; and (4) the creation of a defined course of action to enhance the individual's functioning and quality of life.

Individuals without Mobile Crisis Coverage – those individuals who are not MassHealth eligible and are not Uninsured Individuals, and for whom mobile crisis intervention services are not covered otherwise.

Integrated Care Management Program (ICMP) – an enhanced care management program for Enrollees with complex medical, mental health and/or substance use disorders.

Internal Appeal – a request by a Covered Individual or Appeal Representative made to the Contractor for review of an Adverse Action. The Contractor may only have one level of Internal Appeal for Covered Individuals consistent with 42 CFR 438.402(b).

Level of Care – a differentiation of services depending on the setting in which care is delivered and the intensity of the services.

Marketing – any communication from the Contractor, its employees, Network Providers, agents or Material Subcontractors to a Member who is not enrolled in a PCACO, the PCC Plan or its BHP that EOHHS can reasonably interpret as influencing the Member to enroll in a PCACO, the PCC Plan or its BHP or either not to enroll in, or to disenroll from, a MassHealth managed care organization, accountable care organization, or the PCC Plan's BHP. Marketing shall not include any personal contact between a Provider and a Member who is a prospective, current or former patient of that Provider regarding the provisions, terms or requirements of MassHealth as they relate to the treatment needs of that particular Member.

Marketing Materials – materials that are produced in any medium, by or on behalf of the Contractor, and that EOHHS can reasonably interpret as Marketing to Members. This includes the production and dissemination by or on behalf of the Contractor of any promotional material or activities by any medium including, but not limited to, oral presentations and statements, community events, print media, audio visual tapes, radio, television, billboards, Yellow Pages, and advertisements that explicitly or implicitly refer to MassHealth Managed Care or Title XIX and Title XXI of the Social Security Act, and are targeted in any way toward Members.

Massachusetts Behavioral Health Access (MABHA) System – a web-based searchable database maintained by the Contractor that contains up-to-date information on the number of available beds or available service capacity for certain MassHealth Behavioral Health services, including psychiatric hospitals, Community-Based Acute Treatment Providers, and providers of Intensive Home and Community-Based Services.

Massachusetts Child Psychiatry Access Program (MCPAP) – consists of four psychiatric and behavioral consultation programs, two of which (ASD-ID for MCPAP and Early Childhood) are included in this Contract and further detailed in **Section 2.6.D.2**.

MassHealth – the Medicaid program of the Commonwealth of Massachusetts, administered by EOHHS pursuant to M.G.L. c. 118E, Titles XIX and XXI of the Social Security Act, and other applicable laws and waivers thereto.

MassHealth CarePlus – a MassHealth Coverage Type that offers health benefits to certain individuals at least the age of 21 and under the age of 65 who qualify under EOHHS's MassHealth CarePlus eligibility criteria.

MassHealth CommonHealth – a MassHealth Coverage Type that offers health benefits to certain disabled children under age 18, and certain working or non-working disabled adults between the ages of 18 and 64.

MassHealth Covered Services – medical and Behavioral Health services or related care provided to Covered Individuals, in accordance with the lists of covered services associated with the MassHealth Coverage Type specified in 130 CMR 505.001 through 505.009.

MassHealth Family Assistance – a MassHealth Coverage Type that offers health benefits to certain eligible Members, including families and children under the age of 18.

MassHealth Managed Care – the provision of Primary Care, Behavioral Health, and other medical services through a contracted managed care organization, accountable care organization, or the PCC Plan, in accordance with the provisions of 130 CMR 450.117 et seq. and 130 CMR 508.000 et seq.

MassHealth Managed Care Organization (MCO) – an entity that contracts with MassHealth to provide a managed comprehensive set of covered services to MassHealth Enrollees that select to enroll or who are assigned to an MCO.

MassHealth Member (Member) – any individual determined by EOHHS to meet the requirements of 130 CMR 505.002 or 130 CMR 505.005.

MassHealth Provider – a participating individual, facility, agency, institution, organization, or other entity that has appropriate credentials and licensure and has entered into an agreement with EOHHS for the delivery of MassHealth Covered Services to MassHealth Members.

MassHealth Standard – a MassHealth Coverage Type that offers a full range of health benefits to certain eligible Members, including families, children under age 18, pregnant women, and disabled individuals under age 65.

Material Subcontractor – any entity from which the Contractor procures, reprocures, or proposes to subcontract with, for the provision of all or part of its Administrative Services for any program area or function that relates to the delivery, management or payment of BH Covered Services, including but not limited to claims processing, the Care Management Program and other care management activities, PCC Plan Support Services, and Utilization Management.

MCPAP Teams – multiple units of contracted and credentialed MCPAP Providers with each unit responsible for specific geographic centers across the state. Each unit shall include MCPAP

Providers experienced in providing pediatric mental health and substance use disorder consultation.

Medicaid – see MassHealth.

Medicaid Management Information System (MMIS) – the management information system of software, hardware, and manual procedures used to process Medicaid claims and to retrieve and produce eligibility information, service utilization and management information for Members.

Medically Necessary (or Medical Necessity) – a service is "Medically Necessary" if:

(1) it is reasonably calculated to prevent, diagnose, prevent the worsening of, alleviate, correct, or cure conditions in the Member that endanger life, cause suffering or pain, cause physical deformity or malfunction, threaten to cause or to aggravate a handicap, or result in illness or infirmity; and
(2) there is no other medical service or site of service, comparable in effect, available, and suitable for the Member requesting the service, that is more conservative or less costly to the MassHealth agency. Services that are less costly to the MassHealth agency include, but are not limited to, health care reasonably known by the provider, or identified by the MassHealth agency pursuant to a prior-authorization request, to be available to the Member through sources described in 130 CMR 450.317(C), 503.007, or 517.007. See, 130 CMR 450.204.

Medication for Addiction Treatment (MAT) – use of a medication approved by the federal Food and Drug Administration (FDA) for the treatment of a substance use disorder.

Medication for Opioid Use Disorder (MOUD) – use of a medication approved by the federal Food and Drug Administration (FDA) for the treatment of an opioid use disorder.

Medication Review and Reconciliation – the process of avoiding inadvertent inconsistencies in medication prescribing that may occur in transition of a patient from one care setting to another (e.g., at hospital admission or discharge, or in transfer from a hospital intensive care unit to a general ward) by reviewing the patient's complete medication regimen at the time of admission, transfer and discharge and comparing it with the regimen being considered for the new care setting.

Member – a person determined by EOHHS to be eligible for MassHealth.

Member Identification Number (MID) – the 10-digit identification number assigned to each MassHealth Member.

Mobile Crisis Intervention Uncompensated Care Payment – payment for AMCI/YMCI including follow-up, Community Crisis Stabilization, and up to three units of outpatient CBHC bundle services provided under the Contract when not covered otherwise to Individuals without Crisis Coverage who are experiencing a behavioral health crisis.

Network (or Provider Network) – the collective group of Network Providers who have entered into Provider Agreements with the Contractor for the delivery of BH Covered Services.

Non-Medical Programs and Services – an item or service which the Contractor decides to make available to its Covered Individuals, which is not a Behavioral Health Covered Service. The Contractor must use its own funds to provide such Non-Medical Programs and Services and may not include the costs of such Non-Medical Programs and Services as medical service costs or administrative costs for purposes of MassHealth rate development.

Ombudsman – a neutral entity that has been contracted by MassHealth to assist Covered Individuals (including their families, caregivers, representatives and/or advocates) with information, issues, or concerns.

Operational Start Date – the date, as determined by EOHHS, on which the Contractor assumes responsibility for the administration, delivery and coordination of the functions and responsibilities described in this Contract.

Opioid Treatment Programs (OTP) – Substance Abuse and Mental Health Services Administration (SAMHSA)-certified programs, usually comprised of a facility, staff, administration, patients, and services, that engages in supervised assessment and treatment, using approved medications, of individuals who have opioid use disorders in accordance with 105 CMR 164.300 and 42 CFR Part 8.

Other Provider Preventable Condition (OPPC) – a condition that meets the requirements of an "Other Provider Preventable Condition" pursuant to 42 C.F.R. 447.26(b). OPPCs may occur in any health care setting and are divided into two subcategories:

(1) National Coverage Determinations (NCDs) – The NCDs are mandatory OPPCs under 42 C.F.R. 447.26(b) and consist of the following:
    a. Wrong surgical or other invasive procedure performed on a patient;
    b. Surgical or other invasive procedure performed on the wrong body part;
    c. Surgical or other invasive procedure performed on the wrong patient.

    For each of a. through c., above, the term "surgical or other invasive procedure" is defined in CMS Medicare guidance on NCDs.

(2) Additional Other Provider Preventable Conditions (Additional OPPCs) – Additional OPPCs are state-defined OPPCs that meet the requirements of 42 C.F.R. 447.26(b). EOHHS has designated certain conditions as "Additional OPPCs."

Outpatient Crisis Payment – payment for up to 3 units of outpatient CBHC bundle services provided to Uninsured Individuals and persons covered by Medicare who are experiencing a behavioral health crisis.

Outreach Target – the projected number of Enrollees the Contractor will attempt to Engage annually for Enrollment in the Care Management Program each Contract Year.

Participant – an Enrollee who is enrolled in the Care Management Program with an ICP.

Pay for Performance (P4P) – Performance Incentive Arrangement payments the Contractor may earn as described in Contract **Section 4.6**.

Payment Month – the month in which an Estimated Capitation Payment is issued to the Contractor.

PCC Panel Enrollee – an Enrollee who is assigned to the PCC Plan Provider.

PCC Plan Providers – primary care providers that serve PCC Plan Enrollees.

Peer Support – activities to support recovery and rehabilitation provided to consumers of Behavioral Health services by other individuals with personal experience with Behavioral Health conditions and services.

Per-Member (Enrollee or Covered Individual) Per-Month (PMPM) – the average monthly payment per Enrollee or Covered Individual, depending on context.

Performance Incentive Arrangement – a payment mechanism under which the Contractor may earn payments for meeting targets in the Contract. See 42 CFR 438.6(b).

Permanent Supportive Housing (PSH) – a model of housing that combines ongoing subsidized housing matched with flexible health Behavioral Health, social, and other support services.

Plan Type – an identifier used by MassHealth's MMIS to identify the Rating Category in which a Covered Individual is enrolled in the BHP.

Post-stabilization Care Services – Covered Inpatient and Outpatient Services, related to an Emergency medical condition that are provided after a Covered Individual is stabilized in order to maintain the stabilized condition, or when covered pursuant to 42 CFR 438.114(e) to improve or resolve the Covered Individual's condition.

Practice Based Care Management (PBCM) – A model of Integrated Care Management that is delivered by Primary Care Providers to improve member experience, improve care coordination and improve integration of physical and Behavioral Health care.

Practice Guidelines – systematically developed descriptive tools or standardized specifications for care to assist provider and patient decisions about appropriate health care for specific circumstances. Practice Guidelines are typically developed through a formal process and are based on authoritative sources that include clinical literature and expert consensus.

Pre-release Covered Individuals - Members, as designated by EOHHS, who are incarcerated and pre-enrolled in the Contractor's Plan under the Reentry Demonstration Initiative or related initiatives. Upon release from incarceration into the community, a Pre-release Covered Individual becomes a Covered Individual under the Contract.

Prevalent Languages – those languages spoken by a significant percentage of potential Covered Individuals and Covered Individuals. EOHHS has determined the current Prevalent Languages spoken by potential Covered Individuals and Covered Individuals are English, Spanish, Portuguese, Haitian Creole, simplified Chinese, and Vietnamese. EOHHS may identify

additional or different languages as Prevalent Languages at any time, in a form and format at EOHHS' discretion, during the term of the Contract.

Primary Care – all health care services and laboratory services customarily furnished by or through a family physician, internal medicine physician, obstetrician/gynecologist, pediatrician, or nurse practitioner, to the extent the furnishing of those services is legally authorized by the Commonwealth, as further described in 130 CMR 450.101.

Primary Care Accountable Care Organization (Primary Care ACO or PCACO) – a Primary Care Case Management entity that is an advanced provider-led entity contracted with EOHHS. PCACOs contract directly with MassHealth and deliver well-coordinated care and population health management.

Primary Care Clinician (PCC) – an EOHHS-contracted Primary Care Practitioner participating in the Managed Care program pursuant to 130 CMR 450.118. PCCs provide comprehensive Primary Care and certain other medical services to PCC Plan Enrollees and function as the referral source for most other MassHealth services.

PCC Performance Dashboard – a component of the PCC Plan Support Services. These PCC-specific and/or PCC service location-specific reports shall contain agreed upon indicators to help PCCs and their service locations monitor their performance and to identify opportunities for quality improvement. The PCC Performance Dashboard is the provider profiling report for PCC Plan Providers.

PCC Plan – a MassHealth Managed Care option, which includes EOHHS's network of PCCs, specialty care providers and the BHP.

PCC Plan Support Managers – Contractor staff dedicated solely to the Contract, with appropriate network management, QM, provider relations, and relevant clinical background and experience.

PCC Plan Support Materials – educational materials distributed by the Contractor to PCCs (and other providers as appropriate) to promote improvement in the delivery of health care services and in Enrollee health outcomes.

PCC Plan Support Services (PSS) – services designed to support MassHealth in managing the PCC Plan in a cohesive fashion with a focus on quality management and operational support.

PCC Provider Contract – a PCC's written agreement with EOHHS to be a PCC in the PCC Plan. The PCC may hold a contract for one or more PCC Service Locations.

PCC Service Location – the site at which an Enrollee is enrolled once an Enrollee chooses or is assigned to the PCC Plan. A PCC Service Location is denoted by a Provider Identification and Service Location (PID/SL) number which is system-generated by the EOHHS MMIS. A PCC may have one Service Location or multiple Service Locations.

Peer Recovery Coach – an individual currently in recovery who has lived experience with substance use and/or co-occurring mental health disorders and has been trained to help their

peers with a similar experience to gain hope, explore recovery, and achieve life goals. The focus of the Recovery Coach role is to create a relationship between equals that is non-clinical and focused on removing obstacles to recovery; linking individuals to recovery community and serving as a personal guide and mentor.

Primary Care Practitioner (PCP) – a health care professional who provides Primary Care services.

Privacy Rule – the standards for privacy of individually identifiable health information required by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA), and the associated regulations (45 CFR parts 160 and 164, as currently drafted and subsequently amended).

Protected Health Information (PHI) – any information in any form or medium: i) relating to the past, present or future, physical or mental condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual, and ii) identifying the Individual or with respect to which there is a reasonable basis to believe can be used to identify the Individual. PHI shall have the same meaning as used in the Privacy Rule. PHI constitutes Personal Data as defined in M.G.L. c. 66A, § 1.

Provider – an individual, group, facility, agency, institution, organization, or business that furnishes or has furnished medical services to Covered Individuals.

Provider Agreement – a binding agreement between the Contractor and a BH Network Provider that includes, among other things, all of the provisions set forth in **Section 2.7.A.**

Provider Preventable Conditions (PPC) – as identified by EOHHS through bulletins or other written statements policy, which may be amended from time to time, a condition that meets the definition of a "Health Care Acquired Condition" or an "Other Provider Preventable Condition" as defined by CMS in federal regulations at 42 C.F.R. 447.26(b).

Qualified Behavioral Health Professional – a qualified behavioral health professional shall include, but not be limited to, a: (i) licensed physician who specializes in the practice of psychiatry; (ii) licensed psychologist; (iii) licensed independent clinical social worker; (iv) licensed certified social worker; (v) licensed mental health counselor; (vi) licensed physician assistant who practices in the field of psychiatry; (vii) advanced practice registered nurses who practice in the field of psychiatry, including but not limited to licensed nurse practitioners and licensed psychiatric clinical nurse specialists; or (viii) healthcare provider qualified within the scope of the individual's license to conduct an evaluation of a mental health condition, including an intern, resident or fellow pursuant to the policies and practices of the hospital and medical staff.

Quality Management (QM) – the process of reviewing, measuring and continually improving the outcomes of care delivered.

Query and Retrieve – Or, query-based exchange, refers to the ability for providers to find and/or request information on a patient from other providers, often used for unplanned care.

Rating Category (RC) – a specific group of Covered Individuals for which a discrete BH Covered Services Capitation Rate applies, as described in **Section 4.1**.

Reentry Demonstration Initiative – the initiative authorized under the Massachusetts 1115 Waiver demonstration that allows MassHealth to provide certain services for qualifying Members up to 90 days prior to release from a Correctional Facility

Reportable Adverse Incident – an occurrence that represents actual or potential serious harm to the well-being of a Covered Individual, or to others by the actions of a Covered Individual, who is receiving services managed by the Contractor or has recently been discharged from services managed by the Contractor.

Restoration Center – a site that provides Behavioral Health Services to adults 18 and older, who are at risk of becoming involved with the criminal justice system due to their Behavioral Health status, and who could benefit from urgent access to Behavioral Health Services that could prevent law enforcement contact, including diverting individuals experiencing mental health or substance use disorder crises from arrest and from emergency department (ED) utilization.

Serious Emotional Disturbance (SED) – a Behavioral Health condition that meets the definition set forth in the Individuals with Disabilities Education Act (IDEA), 20 U.S.C. § 1401(3)(A)(i) and its implementing regulations or the definition set forth in regulations governing the Substance Abuse and Mental Health Services Administration (SAMHSA) of the United States Department of Health and Human Services, 58 Fed. Reg. 29422-02 (May 10, 1993), as currently drafted and subsequently amended.

Serious and Persistent Mental Illness (SPMI) – a mental illness that includes a substantial disorder of thought, mood, perception, which grossly impairs judgment, behavior, capacity to recognize reality or the ability to meet the ordinary demands of life; and is the primary cause of a functional impairment that substantially interferes with or limits the performance of one or more major life activities, and is expected to do so in the succeeding year; and meets diagnostic criteria specified within the Diagnostic and Statistical Manual of Mental Disorders (5th ed., text revision) American Psychiatric Association, Washington, DC (2013), which indicates that the individual has a serious, long term mental illness that is not based on symptoms primarily caused by: (a) developmental disorders usually first diagnosed in infancy, childhood or adolescence, such as mental retardation or pervasive developmental disorders; or (b) cognitive disorders, including delirium, dementia or amnesia; or (c) mental disorders due to a general medical condition not elsewhere classified; or (d) substance-related disorders.

Serious Reportable Event (SRE) – an event as defined by All Provider Manual Appendix U: DPH-Designated Serious Reportable Events That Are Not Provider Preventable Conditions.

Service Compensation Rate – a dollar amount to be paid monthly by EOHHS to the Contractor for the delivery of AMCI/YMCI, including follow-up, and Community Crisis Stabilization services to Uninsured Individuals and persons covered by Medicare only as set forth in this Contract.

Statewide ENS Framework – An event notification service framework created as a Mass HIway-facilitated service by EOHHS under 101 CMR 20.11.

Telehealth – provision of a Behavioral Health Covered Service remotely by a physician or practitioner through the use of interactive telecommunications equipment. Also referred to as telemedicine or telepsychiatry.

Therapeutic Milieu – A setting including but not limited to a partial hospital program, psychiatric day treatment program, or CBAT, where Behavioral Health services are provided.

Third-Party Liability (TPL) – other insurance resources, such as Medicare and commercial insurance, available for services delivered to MassHealth Members.

Uninsured Individuals – those individuals who are not MassHealth eligible, and do not have insurance coverage.

Urgent Care – the delivery of same-day or next-day appointments for diagnostic evaluation of new clients and urgent appointments for existing clients; psychopharmacology appointments and Medication for Addiction Treatment (MAT) and Medication for Opioid Use Disorder (MOUD) within a timeframe defined by EOHHS.

Utilization Management (UM) – the process of evaluating the clinical necessity, appropriateness, and efficiency of care and services. This may include service authorizations and prospective, concurrent, and retrospective review of services and care delivered by Providers.

Virtual Gateway – an internet portal designed and maintained by EOHHS to provide the general public, medical providers, community-based organizations, MassHealth Managed Care contractors, and EOHHS staff with online access to health and human services.

Wellness Programs – programs that promote an active process to help individuals become aware of and learn to make healthy choices that lead toward a longer and more successful existence.

Section 1.2 Acronyms

The following acronyms are commonly used in the health care industry and/or frequently found throughout this Contract and its Appendices:

Acronym	Description
ABA	Applied Behavior Analysis
ACA (or PPACA)	Patient Protection and Affordable Care Act of 2010
ACBAT	Autism Community Based Acute Treatment
ACO	Accountable Care Organization
ACPP	Accountable Care Partnership Plan
Adult CCS	Adult Community Crisis Stabilization
ALP	Alternative Lock-up Programs
AMCI	Adult Mobile Crisis Intervention
AND	Administratively Necessary Days

Acronym	Description
API	Application Programming Interface
ASAM	American Society for Addiction Medicine
ASC	Autism Support Center
ASD	Autism Spectrum Disorder
ASD-ID	Autism Spectrum Disorder-Intellectual Disability
ATS	Acute Treatment Services
BBA	Balanced Budget Act of 1997
BH	Behavioral Health
BHP	Behavioral Health Program
BH-JI	Behavioral Health-Justice Involved
BHUC	Behavioral Health Urgent Care
BOH	Board of Hearings
BORIM	Board of Registration in Medicine
CANS	Child and Adolescent Needs and Strengths
CBAT	Community Based Acute Treatment
CBHC	Community Behavioral Health Center
CBHI	Children's Behavioral Health Initiative
CCS	Community Crisis Stabilization
CFR	Code of Federal Regulations
CMP	Care Management Program
CMR	Code of Massachusetts Regulations
CMS	the federal Centers for Medicare and Medicaid Services
CPS	Certified Peer Specialist
CSA	Community Service Agency
CSP-CHI	Community Support Program for Chronically Homeless Individuals
CSP-JI	Community Support Program-Justice Involved
CY	Contract Year
D/HoH	Deaf and/or Hard of Hearing
DCF	the Massachusetts Department of Children and Families
DDCAT	Dual Diagnosis Capability in Addiction Treatment
DDS	the Massachusetts Department of Developmental Services
DMH	the Massachusetts Department of Mental Health
DPH	the Massachusetts Department of Public Health
DPH/BSAS	Bureau of Substance Abuse Services of the Mass. Department of Public Health
DRM	Document Review Measure
DSRA	Direct Service Reserve Account
DUR	drug utilization review
DYS	the Massachusetts Department of Youth Services
ECC	Enhanced Care Coordination
ECMH	Early Childhood Mental Health
ED	emergency department
ENS	Event Notification Service
EOHHS	the Massachusetts Executive Office of Health and Human Services
EPIA	Expedited Psychiatric Inpatient Admission

Acronym	Description
EPSDT	Early and Periodic Screening, Diagnosis and Treatment
EQR	external quality review
EVS	Eligibility Verification System
FFP	Federal Financial Participation
FFS	fee-for-service
FIT	Family-based Intensive Treatment
FTE	full-time equivalent
FY	fiscal year
HCBS	Home and Community-Based Services
HEDIS	Healthcare Effectiveness Data and Information Set
HIPAA	Health Insurance Portability and Accountability Act of 1996
HNA	Health Needs Assessment
HQEC	Health Quality and Equity Committee
HRSN	Health-Related Social Needs
IBNR	incurred but not reported
ICC	intensive care coordination
ICM	intensive clinical management
ICMP	Integrated Care Management Program
IDD	Intellectual or Developmental Disability
IECMH	Infant Early Childhood Mental Health
IHBS	In-Home Behavioral Services
IHT	In-Home Therapy
ITS	Individualized Treatment Services
LABA	Licensed Applied Behavior Analyst
LEIE	Office of the Inspector General List of Excluded Individuals Entities
MABHA	Massachusetts Behavioral Health Access
MBR	MassHealth benefit request (application) form
MCI	mobile crisis intervention
MCO	Managed Care Organization
MCPAP	Massachusetts Child Psychiatry Access Program
MFD	Medicaid Fraud Division
MGL	Massachusetts General Laws
MHC	Mental Health Center
MID	Member Identification Number
MIS	Management Information System
MLR	Medical Loss Ratio
MMIS	Medicaid Management Information System
MOUD	Medication for Opioid Use Disorder
NCQA	National Committee for Quality Assurance
NPI	National Provider Identifier
NQTL	Non-Quantitative Treatment Limitation
OCA	Office of Clinical Affairs
OTP	Opioid Treatment Program
P4P	Pay For Performance
PAP	Pre-Arraignment Protocol

Acronym	Description
PBCM	Practice Based Care Management
PCACO	Primary Care ACO
PCC	Primary Care Clinician
PCP	Primary Care Practitioner
PD	PCC Performance Dashboard
PDT	Psychiatric Day Treatment
PFR	Pay For Reporting
PHI	Protected Health Information
PHP	Partial Hospitalization
PID/SL	Provider Identification and Service Location
PIHP	Prepaid Inpatient Health Plan
PMPM	Per Member (Enrollee or Covered Individual) Per Month
POPS	Pharmacy Online Processing System
PPC	Provider Preventable Conditions
PPHSD	Preventive Pediatric Health-Care Screening and Diagnosis
PPPM	per participant (in the Care Management Program) per month
PRC	Peer Recovery Coach
PRC-PP	Peer Recovery Coach for Pregnant and Postpartum Members
PSH	Permanent Supportive Housing
PSS	PCC Plan Support Services
QI	quality improvement
QIP	Quality Improvement Project
QM	Quality Management
QLT	Quantitative Treatment Limitation
RC	Rating Category
RRS	Residential Rehabilitation Services (Level 3.1)
RSN	Recovery Support Navigator
RSN-PP	Recovery Support Navigator for Pregnant and Postpartum Members
S2BI	Screening to Brief Intervention
SED	Serious Emotional Disturbance
SOAP	Structured Outpatient Addiction Program
SPMI	Serious and Persistent Mental Illness
SRE	Serious Reportable Event
TCM	Therapeutic Class Management
TM	Therapeutic Mentor
TPL	Third-Party Liability
UM	Utilization Management
VG	Virtual Gateway
YCCS	Youth Community Crisis Stabilization
YMCI	Youth Mobile Crisis Intervention

Section 2. CONTRACTOR RESPONSIBILITIES

Section 2.1 Compliance

A. General

1. The Contractor shall comply, to the satisfaction of EOHHS, with (1) all provisions set forth in this Contract and (2) all applicable provisions of state and federal laws, regulations, and waivers.

2. If the Contractor does not achieve the desired outcomes or maintain compliance with contractual obligations, EOHHS may take non-compliance actions as specified in **Section 5.3.L** and **Section 5.3.M** of this Contract, which include but are not limited to, requiring the Contractor to hire additional staff and the application of sanctions.

B. Federal Managed Care Law

The contractor shall comply with applicable provisions of 42 U.S.C. § 1396u-2 et seq. and 42 CFR 438 et seq. at all times during the term of this Contract.

C. Conflict of Interest

Neither the Contractor nor any Material Subcontractor shall, for the duration of the Contract, have any interest that will conflict, as determined by EOHHS, with the performance of services under the Contract, or that may be otherwise anticompetitive. Without limiting the generality of the foregoing, EOHHS requires that neither the Contractor nor any Material Subcontractor have any financial, legal, contractual or other business interest in EOHHS's Enrollment Broker or the External Quality Review Contractor.

D. Systems Interface

The Contractor or its designated subcontractor shall take all steps necessary, as determined by EOHHS, to ensure that the Contractor's systems are always able to interface with the Medicaid Management Information System (MMIS), the Virtual Gateway, and other EOHHS IT applications.

Section 2.2 Contract Transition/Contract Readiness

A. Contract Transition Phase

The Contractor shall comply with all requirements related to the Transition Phase of the Contract as detailed herein and in **Appendix B-1**. The Contract Transition Phase includes, but is not limited to, the period between the Contract Effective Date and the Contract Operational Start Date.

1. Transition Schedule

The Transition Phase will begin after the Contract is executed. The Transition Phase must be completed no later than the Contract Operational Start Date.

2. Transition Workplan

a. No later than five business days following the Contract Effective Date, the Contractor shall submit to EOHHS, for its review and approval, a Transition Workplan which shall be used by EOHHS to monitor the Contractor's progress toward achieving Contract Readiness, as detailed in **Section 2.2.B** below. At a minimum, the Transition Workplan must address all of the items listed in **Sections 2.2.B** and **2.2.C** below, and **Appendix B-1** unless otherwise directed by EOHHS.

b. The Transition Workplan must list each task, the date by which it will be completed, how it will be completed, and the documentation that will be provided to EOHHS as evidence that the task has been completed.

B. Contract Readiness Review

1. During the Transition Phase, EOHHS will conduct a readiness review of the Contractor, which must be completed successfully prior to the Contract Operational Start Date.

2. The readiness review shall be conducted prior to enrollment of Covered Individuals with the Contractor's Plan, and at other times during the Contract period at the discretion of EOHHS. EOHHS will conduct the readiness review to verify the Contractor's assurances that the Contractor is ready and able to meet its obligations under the Contract. EOHHS reserves the right to conduct an additional readiness review in the event that additional populations become managed care eligible.

3. Scope of Readiness Review

The Contractor agrees to provide all materials required to complete the readiness review by the dates established by EOHHS. The scope of the Readiness Review shall include, but may not limited to:

a. An assessment of the Contractor's ability and capability to perform, at a minimum, its obligations under the Contract satisfactorily in the following areas consistent with 42 CFR 438.66(d)(4):

1) Operational and Administration, specifically:

a) Staffing and resources, including Key Personnel and functions directly impacting on Enrollees (e.g., adequacy of Enrollee Services staffing), in accordance with **Section 2.3**;

b) Delegation and oversight of Contractor responsibilities, including but not limited to capabilities of Material Subcontractors in accordance with **Section 2.2.B.6 and Appendix B-2.**;

c) Enrollee and Provider communications;

d) Internal Grievance and Appeal policies and procedures, in accordance with **Section 2.12**;

e) Enrollee services and outreach, including capabilities (materials, processes and infrastructure, e.g., call center capabilities), in accordance with **Section 2.10**;

f) Provider Network management, including Provider Network composition and access, in accordance with **Section 2.9.B through D**;

g) Program integrity and compliance, including Fraud and Abuse and other program integrity requirements in accordance with **Section 2.3.C.3**;

2) Service Delivery

a) Case management, care coordination, and service planning in accordance with **Section 2.5**;

b) Quality improvement, including comprehensiveness of quality management/quality improvement strategies, in accordance with **Section 2.13;** and

c) Utilization Review, including comprehensiveness of Utilization Management strategies, in accordance with **Section 2.6.C**

3) Financial Management

a) Financial reporting and monitoring; and

b) Financial solvency, in accordance with **Section 2.15**;

4) Systems Management

a) Claims management; and

b) Encounter Data and enrollment information, as applicable, management, including but not limited to, at the request of EOHHS, a walk-through of any information systems, including but not limited to enrollment, claims payment system performance, interfacing and reporting capabilities

and validity testing of Encounter Data, in accordance with **Section 2.14**, including IT testing and security assurances.;

b. A review of other items specified in the Contract, including but not limited to:

1) All deliverables that EOHHS has specified must be in place prior to the Contract Operational Start Date, as set forth in **Appendix B-1**;

2) Marketing materials, in accordance with **Section 2.11**;

3) Content of Provider Contracts, including any Provider Performance Incentives, in accordance with **Sections 2.7.A**; and

4) Content of Material Subcontracts with Community Partners, in accordance with **Sections 2.5.K.**

4. EOHHS will identify to the Contractor all areas where the Contractor is not ready and able to meet its obligations under the Contract. The Contractor must provide EOHHS with a corrective action plan within 10 business days after being informed of any deficiency EOHHS identifies during the readiness review. EOHHS, may, in its discretion, modify or reject any such corrective action plan, in whole or in part.

5. EOHHS may, in its discretion, postpone the Contract Operational Start Date if the Contractor fails to satisfy all readiness review requirements. If, for any reason, the Contractor does not fully satisfy EOHHS that it is ready and able to perform its obligations under the Contract prior to the Contract Operational Start Date, and EOHHS does not agree to postpone the Contract Operational Start Date, or extend the date for full compliance with the applicable Contract requirement, then EOHHS may terminate the Contract and shall be entitled to recover damages from the Contractor.

6. The Contractor shall demonstrate to EOHHS's satisfaction that the Contractor and its Material Subcontractors, if any, are ready and able to meet all Contract requirements identified in the readiness review within a timeline and workplan identified by EOHHS. Requirements will need to be met between 60 and 15 business days prior to the Contract Operational Start Date. The Contractor shall provide EOHHS with a certification, in a form and format specified by EOHHS, demonstrating such readiness.

7. Covered Individuals shall not be enrolled with the Contractor unless and until EOHHS determines that the Contractor is ready and able to perform its obligations under the Contract as demonstrated during the readiness review, except as provided below.

8. EOHHS may, in its discretion, enroll Covered Individuals with the Contractor as of the Contract Operational Start Date provided the Contractor and EOHHS agree on a corrective action plan to remedy any deficiencies EOHHS identifies pursuant to this Section.

9. The readiness provisions in this Section shall also apply, as determined appropriate by EOHHS, upon the implementation of changes in scope to this Contract and new programs or initiatives as described in **Sections 5.7** of this Contract.

C. Continuity of Care for New Covered Individuals

The Contractor shall develop and implement policies and procedures to ensure continuity of care for new Covered Individuals that are enrolling with the Contractor, including from an Accountable Care Partnership Plan, an MCO or a commercial carrier. Such policies and procedures:

1. Shall be for the purpose of minimizing the disruption of care and ensuring uninterrupted access to Medically Necessary Behavioral Health Covered Services;

2. Shall address continuity of care for all such Covered Individuals and include specific policies and procedures for the following individuals at a minimum:

   a. Covered Individuals who, at the time of their enrollment:

      1) Are pregnant;

      2) Have significant health care needs or complex medical conditions;

      3) Are currently receiving ABA Services, including through MassHealth, an Accountable Care Partnership Plan, MCO, or a commercial carrier and have a current prior authorization for ABA Services in place;

      4) Are children in the care or custody of DCF, and youth affiliated with DYS (either detained or committed) or receiving services from DDS;

      5) Are hospitalized; or

      6) Are receiving treatment for behavioral health or substance use; or

   b. Covered Individuals who have received prior authorization for Behavioral Health Covered Services, including but not limited to inpatient services.

3. Shall include, at a minimum, provisions for:

   a. Identifying and communicating with Covered Individuals for whom continuity of care is required in accordance with this Section, and those

Covered Individuals' providers (including but not limited to Network Providers);

b. Facilitating continuity of care so that new Covered Individuals may continue to see their current providers (including but not limited to Network Providers) for Medically Necessary Behavioral Health Covered Services for at least 90 days from the Operational Start Date, or otherwise 90 days after the Effective Date of Enrollment except where specified below, including but not limited to:

1) Ensuring that Covered Individuals currently receiving inpatient care from a hospital, including non-Network hospitals, at the time of their enrollment may continue to receive such care from such hospital as long as such care is Medically Necessary. The Contractor shall make best efforts to contact such hospital to ensure such continuity of care;

2) Ensuring that, for at least 90 days from the Operational Start Date or 90 days after the Effective Date of Enrollment, new Covered Individuals receiving outpatient Behavioral Health or substance use disorder care, including but not limited to Covered Individuals with upcoming appointments, ongoing treatments or services, or prior authorizations, may continue to seek and receive such care from providers (including non-Network) with whom they have an existing relationship for such care;

3) Ensuring that, for at least 90 days from the Operational Start Date or 90 days after the Effective Date of Enrollment, Covered Individuals actively receiving ABA Services may continue to receive such services from providers (including non-Network) with whom they have an existing relationship for such care. The Contractor shall develop related protocols that include at a minimum the use of single-case agreements, full acceptance and implementation of existing prior authorizations for ABA Services, and individual transition plans.

4) Otherwise making accommodations for:

a) Upcoming appointments;

b) Ongoing treatments or services;

c) Inpatient care; and

d) Other medically necessary services.

c. Ensuring that all such providers are able to confirm or obtain any authorization, if needed, for any such services from the Contractor;

d. Honoring all prior authorizations and prior approvals for services for the duration of such prior authorizations and prior approvals or, if the Contractor chooses to modify or terminate a prior authorization and prior approval, then the Contractor shall treat such modification or termination as an Adverse Action and follow the appeal rights policy and procedures, including notification to the Covered Individual and the Covered Individual's provider in question;

e. Ensuring appropriate medical record documentation or any continuity of care or transition plan activities as described in this Section;

f. Ensuring that all Covered Individuals, including new Covered Individuals, may access Emergency Services at any emergency room, including from out-of-Network Providers, and that such Services are provided at no cost to the Covered Individual, as described in **Section 2.9**;

g. For Covered Individuals affiliated with other state agencies, coordination and consultation with such agencies as described in **Section 2.5**;

h. Accepting and utilizing medical records, claims histories, and prior authorizations from a Covered Individual's previous Accountable Care Partnership Plan or MassHealth-contracted MCO or from MassHealth. Provisions shall also include accepting and utilizing available medical records, claims histories, and prior authorizations from a Covered Individual's previous commercial carrier to the extent such information is made available by the Covered Individual, the Covered Individual's provider, or MassHealth. The process shall require the Contractor to, at a minimum:

    1) Ensure that there is no interruption of Behavioral Health Covered Services for Covered Individuals;

    2) Accept the transfer of all medical records and care management data, as directed by EOHHS;

    3) Accept the transfer of all administrative documentation, as directed by EOHHS, including but not limited to:

        a) Provider Fraud investigations;

        b) Complaints from Covered Individuals;

        c) Grievances from Providers and Covered Individuals;

        d) Quality Management Plan; and

e) Quality Improvement project records;

i. As directed by EOHHS, participating in any other activities determined necessary by EOHHS to ensure the continuity of care for Covered Individuals, including making best efforts to:

1) Outreach to new Covered Individuals within two business days of such new Covered Individual's Effective Date of Enrollment for a period at the start of the Contract to be specified by EOHHS and expected to last no more than 120 days from the Contract Operational Start Date. Such outreach may include telephone calls, mail, or email, as appropriate and compliant with all applicable laws;

2) Obtain any necessary consents from Covered Individuals who were formerly Covered Individuals or Covered Individuals leaving the Contractor's Plan, in order to transfer certain information specified by EOHHS to such Member's or Covered Individual's new MassHealth Accountable Care Partnership Plan or MCO Plan; and

3) As directed by EOHHS, transferring all information related to prior authorizations.

j. No later than one month prior to the Contract Operational Start Date, accepting transfer of all authorizations that are valid for dates of service after the Contract Operational Start Date; and each business day beginning 30 days prior to the Contract Operational Start Date, transferring from the previous behavioral health vendor contract information on all services that were registered the previous day and that are valid for dates of service after the Contract Operational Start Date;

k. Prior to the Contract Operational Start Date, providing written instructions to those network and non-network providers from the previous behavioral health vendor contract regarding any changes from the previous contract to the Contractor's service authorization requirements and procedures for using the service authorization system, and schedule training sessions with Network Providers to review policies and procedures for any such changes, as necessary; and

l. For any Covered Services authorized under the previous behavioral health vendor contract, adjudicating and paying claims from BH Network Providers under the previous contract for services provided on or after the Contract Operational Start Date;

4. Shall include designating a specific contact person to respond to EOHHS requests and concerns related to continuity of care. The Contractor shall provide EOHHS with such individual's name, telephone number, and email address, and shall

ensure such individual is available to EOHHS during business hours and at other times specified by EOHHS; and

5. Shall be submitted to EOHHS for approval on a date specified by EOHHS.

Section 2.3 Administration and Contract Management

A. Organization, Staffing and Key Personnel

The Contractor shall have in place organizational, operational, managerial, and administrative structures and systems capable of fulfilling all Contract requirements.

1. Organizational Performance and Quality Control

The Contractor shall:

a. Comply with Office of State Comptroller (OSC) and the Committee of Sponsoring Organization (COSO) Internal Control Standards.

b. Have in place a process for investigating and resolving any EOHHS dissatisfaction with the Contractor's performance and for improvements in its internal systems.

c. Maintain internal quality standards, indicators and written procedures to ensure accurate, timely, and consistent Contract activities to promote:

1) Adherence to Contract deadlines for the submission of accurate and timely reports and other materials;

2) Accurate and consistent dissemination of oral and written information by Contractor staff;

3) Accurate, clear documentation of the Contractor's activities (programmatic and financial) required by EOHHS;

4) Data integrity and confidentially of the Contractor's MIS, including maintenance of history files; and

5) Any other EOHHS-specified operational and reporting performance criteria.

d. Monitor internal quality control measures, standards, and procedures on a continuous basis and update them as needed to keep them current with standards.

e. Report to EOHHS in writing all internal quality control issues and findings when and if they arise.

2. Staffing Requirements

a. The Contractor shall recruit and maintain an appropriately qualified and diverse workforce, sufficient in number for the efficient execution of all Contract responsibilities.

1) The Contractor's resource allocation shall be adequate to achieve positive outcomes in all functional areas within the organization. Adequacy shall be evaluated based on outcomes and compliance with the requirements of the Contract.

2) The Contract must ensure that it properly allocates and tracks the time expended by Key Personnel and, as appropriate, other personnel among the administration of the PCC Plan's BHP, PCC Plan Support Services and DMH Specialty Programs administration.

b. The Contractor shall recruit and maintain an adequate number of appropriately qualified and diverse staff in order to perform Network Management activities efficiently in the communities across the Commonwealth, so that Covered Individuals and BH Network Providers, PCCs and Providers have timely access to Contractor staff in all regions of Massachusetts.

c. The Contractor must maintain a staff that reflects the cultural, linguistic and demographic characteristics of Covered Individuals, including a sufficient number of bilingual staff capable of communicating in English and Spanish, and other languages as appropriate.

d. The Contractor shall not employ or subcontract with any individual who has been debarred, suspended, or otherwise lawfully prohibited from participating in any federal healthcare program. The Contractor shall screen all potential employees and Subcontractors to determine whether any of them have been excluded from participation in federal healthcare programs utilizing, at a minimum, the following websites:

1) Office of Inspector General (OIG) List of Excluded Individuals/Entities (LEIE);

2) The System of Award Management (SAM); and

3) Other applicable sites as may be determined by EOHHS.

e. The Contractor shall conduct an annual criminal background check on all current or potential employees or Subcontractors who have access to Covered Individual protected health information. The Contractor shall, upon request, provide EOHHS with a satisfactory criminal background check or an attestation that a satisfactory criminal background check has

been completed for any of its staff or Subcontractor's staff assigned to or proposed to be assigned to any aspect of the performance of this Contract.

f. The Contractor shall provide a copy of the Contractor's organizational chart with reporting structures, names, and positions to EOHHS annually and upon request. The organizational chart shall show the ongoing leadership and program support that will be provided to the Contractor by the Contractor's parent organization, if any.

g. The Contractor may terminate any of its employees designated to perform work or services under this Contract, as permitted by applicable law.

3. Key Personnel

a. The Contractor shall employ the following or similarly titled or functional full-time personnel designated as key personnel under the Contract, employed in the key personnel position only upon review and approval by EOHHS. All Key Personnel shall be located in Massachusetts:

Executive Positions:

1) **Chief Executive Officer (CEO):** An individual who provides overall direction for the Contractor, is responsible for the Contract in its entirety, and who ensures that there is coordination and integration, as appropriate, of functions across the activities related to BH services, administrative services related to the PCC Plan, the full range of Care Management activities, and Specialty Services managed by the Contractor;

2) **Chief Financial Officer:** A professional who shall be responsible for seeing all financial provisions and requirements of this Contract, including but not limited to:

a) Serving as the Contractor's liaison to EOHHS's financial representatives on all financial matters, including payments, reconciliations, and financial forecasting; and

b) Validating the accuracy and completeness of all financial reports required under this Contract under the penalty of perjury;

3) **Chief Operating Officer:** A professional designated to oversee day-to-day business activities conducted pursuant to this Contract;

4) **Chief Information Officer:** A professional who oversees information technology and systems to support the Contractor's operations, including submission of accurate and timely Covered Individual encounter data;

5) **Chief Medical Officer:** A physician who shall be board-certified in psychiatry and/or internal medicine, be in compliance with all professional licensing requirements, and have at least two years of experience in managed BH care, peer review, or both;

6) **Associate Medical Directors:** Three full-time equivalent physicians who meet the following criteria:

   a) One shall be board-certified or board-eligible in child and adolescent psychiatry.

   b) One shall be board-eligible in internal medicine, with experience in integration of care across medical and Behavioral Health Providers and shall be responsible for the oversight of the Care Management Program described in **Section 2.5**.

   c) One shall be responsible for the oversight of the Quality Management program described in **Section 2.13**.

   d) If the full-time Chief Medical Officer is not a board-certified adult psychiatrist, then an additional full-time equivalent Associate Medical Director must be a board-certified adult psychiatrist.

7) **Health Equity Director:** A full-time employee who chairs the Health Equity Committee and provides leadership in the design and implementation of Contractor's strategies and programs to ensure Health Equity is prioritized and addressed; and is the primary liaison between the Contractor, EOHHS, and other MassHealth plans regarding efforts to achieve Health Equity.

8) **Behavioral Health Plan Network Management Director:** An individual dedicated to the Contract, who is responsible for all BHP Network Management activities, as described in **Section 2.8**.

9) **Contract Officer:** A full-time designated individual dedicated solely to the Contract and who shall act as the liaison between the Contractor and EOHHS. The Contract Officer shall hold an executive-level key personnel position in the Contractor's organization, except that the Contractor may propose for EOHHS's prior review and approval an alternate structure for the Contract Officer position; and

Administrative Positions:

10) **PCC Plan Support Services Director:** An individual dedicated to the Contract, who is responsible for all applicable PCC Plan Support Services activities as described in **Section 2.19**;

11) **PCC Plan Support Managers:** At least two full-time individuals dedicated solely to the Contract, with appropriate provider relations, quality management and relevant background and experience, who are responsible for conducting activities on behalf of EOHHS as described in **Section 2.19**.

12) **Quality Management Director:** A senior manager, dedicated solely to the Contract and with demonstrated expertise in quality improvement processes, who is responsible for overseeing all quality management activities related to the Contract, including but not limited to staff training for the successful performance and execution of such activities. The Quality Management Director will be accountable to the Contractor's appropriate clinical leadership, such as the Associate Medical Director for Quality Management.

13) **PCACO Support Manager:** An individual who is responsible for ensuring collaboration with all PCACOs to ensure coordination of care delivery for Covered Individuals.

14) **Youth State Agency Support Manager:** An individual who is responsible for oversight of the Contractor's activities to support youth in the care and custody of the Commonwealth or youth involved with state agencies.

15) **Ombudsman Liaison:** An individual who shall liaise with EOHHS' Ombudsman to resolve issues raised by Covered Individuals.

b. The Contractor's designated Contract Officer shall be authorized and empowered to represent the Contractor in all matters pertaining to the Contract and shall have responsibility for:

1) Ensuring the Contractor's compliance with the terms of the Contract, including securing and coordinating resources necessary for such compliance;

2) Overseeing the Contractor's implementation of all EOHHS-approved plans, policies and timelines;

3) Overseeing all Contract-related activities by the Contractor, each Material Subcontractor and all other subcontractors, including

coordinating with the Contractor's key personnel as described in **Section 2.3.A**;

4) Receiving and responding to all inquiries and requests made by EOHHS related to the Contract, in the time frames and formats specified by EOHHS;

5) Meeting with EOHHS's Contract Manager(s) on a routine basis as agreed upon by the parties, to discuss issues of mutual interest or concern;

6) Coordinating requests and activities among the Contractor, all subcontractors, and MassHealth and other state agency staff (including but not limited to DMH, DPH, BSAS, DCF and DYS);

7) Working to promptly resolve any Contract-related issues identified by the Contractor or EOHHS; and

8) Tracking the compliance of all Contract requirements and deliverables and maintaining records of all compliance activities and compliance dates using an electronic software tool or other similar mechanism such as a spreadsheet. Tracking of Contract compliance shall be in a format that can be shared with EOHHS upon request or an agreed-upon reporting schedule. All deliverables, reports, contracts, subcontracts, agreements and any other documents subject to EOHHS approval shall be provided to EOHHS in accordance with Contract requirements.

c. Key executive positions cannot be vacant for more than 90 calendar days. The Contractor must notify EOHHS within 5 business days of learning that any key position is vacant or anticipated to be vacant.

d. Prior to diverting any of the specified key personnel for any reason, the Contractor must notify EOHHS in writing, and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the delivery of BH Covered Services and performance of core functions under this Contract. These changes are to be reported to EOHHS when individuals either leave or are added to these key positions.

4. Staff Training and Licensure

a. The Contractor shall ensure that all staff members, including Subcontractors, have met any applicable state or federal licensure requirements and have received appropriate training, education, experience, and orientation to fulfill the requirements of their position. EOHHS may require additional staffing if the Contractor substantially fails to maintain compliance with any provision of the Contract.

b. The Contractor shall provide initial and ongoing staff training that includes an overview of contractual, state, and federal requirements specific to individual job functions. The Contractor shall ensure that all staff members having contact with Covered Individuals or Providers receive initial and ongoing training on health equity and social determinants of health, and with regard to the appropriate identification and handling of quality of care concerns.

c. The Contractor shall educate all staff members about its policies and procedures on advance directives.

d. The Contractor shall educate all staff members about Health Equity and related topics in accordance with **Section 2.20**.

5. Physical Presence in Massachusetts

The Contractor shall not be located outside of the United States and no operations, including that of a Material Subcontractor, may be conducted outside of the United States without prior written consent of EOHHS. The Contractor shall have an Administrative Office located in the Boston, Massachusetts metropolitan area.

B. Advisory Committees and Councils

The Contractor shall establish the advisory committees and councils for the exchange of stakeholder ideas related to this Contract, discussion of relevant topics, and the solicitation of advice, recommendations or concerns. The structure and purpose of the committees and councils must be consistent with NCQA protocols. The goal of these committees and councils shall be to foster improved quality, integrated care and Covered Individual, Provider and PCC satisfaction. The committees and councils shall follow standard rules of order and maintain a written record or minutes of each meeting. All committees and councils must meet at least once during the first six months of Contract Year One, and on a regular schedule thereafter. The committees and councils described in this Section shall not be the only venue for the Contractor to solicit input from stakeholders.

1. BH Clinical Advisory Committee

The Contractor shall establish and facilitate a BH Clinical Advisory Committee whose main objective is to support and promote improvement in the quality of BH Covered Services provided to Covered Individuals, including the integration of medical and Behavioral Health services to the benefit of the Covered Individual. The BH Clinical Advisory meetings shall be held at least three times a year and shall include refreshments (food and non-alcoholic beverages) as part of the event.

a. The membership of the BH Clinical Advisory Committee shall be subject to EOHHS's approval, and shall consist of:

1) from eight to 14 Network Providers who represent different types of Network Providers (e.g., mental health clinics, hospitals, individual practitioners) and different BH specialties from diverse geographic areas of the Commonwealth;

2) at least one PCC; and,

3) at least one PCACO.

b. EOHHS may recommend to the Contractor Network Providers to be invited to serve on the committee.

c. EOHHS, DMH, DPH's Bureau of Substance Addiction Services (BSAS) and other state agencies and major stakeholders identified by EOHHS shall be invited to participate in the committee's meetings.

d. The activities of the BH Clinical Advisory Committee shall include:

1) establishing bylaws that include designating a term of duty for committee members;

2) meeting jointly with the PCC Clinical Advisory Committee (see **Section 2.3.B.1**, above), at least one time per Contract Year; and

3) developing agendas that promote and support the QM activities of the BHP, including the integration of medical and Behavioral Health care services to the benefit of Covered Individuals and Enrollees.

2. PCC Clinical Advisory Council

The Contractor shall establish and facilitate a PCC Clinical Advisory Council whose main objective is to support and promote improvement in the quality of clinical services provided to Enrollees. The meetings shall be held at least two times a year and may be held in-person or virtually.

a. The attendees of the PCC Clinical Advisory Council shall be subject to EOHHS's approval, and shall consist of:

1) all enrolled PCCs;

2) non-physician providers affiliated with PCC practices, by invitation only, as determined by EOHHS; and

3) other MassHealth providers acting as specialists, by invitation only as determined by EOHHS.

b. The activities of the PCC Clinical Advisory Council shall include:

1) Meeting at the discretion of EOHHS. The meetings may be a joint meeting with the BH Clinical Advisory Committee (see **Section 2.3.B.1**, above);

2) Developing agendas with the PCC Plan Director and Medical Director that promote and support the improvement in quality of clinical services provided to Enrollees including but not limited to topics pertinent to provider practice and care quality;

3) Engage speakers who present on salient topics in collaboration with the PCC Plan; and

4) Report on minutes to the meeting and provide follow-up on action items established.

3. Patient and Family Advisory Committee (PFAC)

a. Duties of the PFAC include but are not limited to:

1) Providing regular feedback to the Governing Board on issues of Covered Individuals' care and services;

2) Identifying and advocating for preventive care practices to be utilized by the Contractor;

3) Being involved with the development and updating of cultural and linguistic policies and procedures, including those related to Quality Improvement, education, and operational and cultural competency issues affecting groups who speak a primary language other than English;

4) Advising on the cultural appropriateness and member-centeredness of necessary member or provider targeted services, programs, and trainings; Contractor Marketing Materials and campaigns; and Contractor partnerships; and

5) Providing input and advice on member experience survey results and other appropriate data and assessments.

b. The PFAC shall be exclusively made up of Covered Individuals and family members of Covered Individuals.

c. The composition of the PFAC shall, to the extent possible, reflect the diversity of the MassHealth member population, and shall:

1) Consider cultural, linguistic, racial, disability, sexual orientation, and gender identities, among others; and

2) Include representatives from parents or guardians of pediatric Covered Individuals.

d. The Contactor shall ensure:

1) Reasonable accommodations include interpreter services, as well as other resources that may be needed to support participation by Covered Individuals and their family members in the PFAC; and

2) That the process and opportunity for joining the PFAC is publicized such that any Covered Individual (or their family members as applicable) may have the opportunity to apply to join or otherwise participate.

e. The Contractor shall report on the PFAC as part of its Health Quality and Equity Strategic Plan report as set forth in **Appendix E-1.**

4. Other Advisory Committees

As directed by EOHHS during the term of the Contract, the Contractor shall facilitate and convene additional advisory committees, which EOHHS shall chair.

5. A Health Quality and Equity Committee as described in **Section 2.20.A**.

C. Contract Management and Responsiveness to EOHHS

1. Performance Reviews

a. The Contractor shall attend regular performance review meetings held by EOHHS, virtually, at EOHHS' offices, or at another location determined by EOHHS, each month or more frequently at EOHHS' discretion;

b. Contractor shall ensure that Key Personnel and other staff with appropriate expertise are present in person at such meetings, as requested by EOHHS, including but not limited to, the Contractor's CEO;

c. The Contractor shall prepare materials and information for such meetings as further directed by EOHHS, including but not limited to, measures such as:

1) Costs of care and utilization for Covered Individuals by types of service;

2) Performance reporting information;

3) Quality measure performance and variation and trends in such performance measures, including progress in reducing health disparities;

4) Opportunities the Contractor identifies to improve performance and plans to improve such performance, including plans proposed to be implemented by the Contractor for Network Providers;

5) Changes in Contractor's staffing and organizational development;

6) Performance of Material Subcontractors, including but not limited to, any changes in or additions to Material Subcontractor relationships; and

7) Any other measures deemed relevant by Contractor or requested by EOHHS.

d. The Contractor shall, within two business days following each performance review meeting, prepare and submit to EOHHS for review and approval a list of any action items, requested follow-ups for the next meeting, and estimated timelines for delivery, in a form and format specified by EOHHS.

2. Timely Response to EOHHS Requests

a. Contractor shall respond to any EOHHS requests for review, analysis, information, or other materials related to Contractor's performance of this Contract by the deadlines specified by EOHHS, including but not limited to, for most requests such as those described in this Section, providing a sufficient response within one week of receiving the request. Such requests may include but are not limited to requests for:

1) Records from Contractor's Health Information System, claims processing system, Encounter Data submission process, or other sources, to assist Contractor and EOHHS in identifying and resolving issues and inconsistencies in Contractor's data submissions to EOHHS;

2) Analysis of utilization, patterns of care, cost, and other characteristics to identify opportunities to improve Contractor's performance on any cost or quality measures related to this Contract;

3) Financial and data analytics, such as the Contractor's payment rates to Network Providers as a percent of MassHealth's fee schedules;

4) Documentation and information related to Contractor's care delivery, Care Management, or Community Partners responsibilities, to assist EOHHS with understanding Contractor's activities pursuant to these requirements;

5) Information about Contractor's member protections activities, such as Grievances and Appeals;

6) Documentation and information related to Contractor's Program Integrity activities as described in **Section 2.3.D.3;**

7) Documentation, analysis, and detail on the metrics evaluated in the Contractor's Quality Improvement performance and programming; and

8) Cooperation and coordination with EOHHS, the Massachusetts Office of the Attorney General, and the Massachusetts Office of the State Auditor in any Fraud detection and control activities, or other activities as requested by EOHHS.

b. If the Contractor fails to satisfactorily respond within the time requested by EOHHS without prior approval from EOHHS for a late response, EOHHS may take corrective action or impose sanctions in accordance with this Contract.

D. Other Contract Management Requirements

1. Policies and Procedures for Core Functions

The Contractor shall develop, maintain, and provide to EOHHS upon request policies and procedures for all core functions necessary to effectively and efficiently meet the requirements outlined in this Contract. All policies and procedures requiring EOHHS approval shall be documented and shall include the dates of approval by EOHHS. These policies and procedures shall include, but are not limited to, the following:

a. Response to violations of Covered Individuals' privacy rights by staff, Providers, or Subcontractors;

b. Non-discrimination of Covered Individuals;

c. Non-restriction of Providers advising or advocating on a Covered Individual's behalf;

d. Appeal rights for certain minors who under the law may consent to medical procedures without parental consent;

e. Covered Individual's cooperation with those providing health care services;

f. Marketing activities that apply to the BH Contractor, Providers, and Subcontractors, as well as Contractor's procedures for monitoring these activities;

g. Cost-sharing by Covered Individuals;

h. Advance directives;

i. Assisting Covered Individuals in understanding their benefits and how to access them;

j. Access and availability standards;

k. Covered Individual's right to be free from restraint or seclusion used as a means of coercion or retaliation;

l. The provision of Culturally and Linguistically Appropriate Services;

m. Practice guidelines in quality measurement and improvement activities;

n. Compliance with Emergency Services and Post-stabilization Care Services requirements as identified in 42 C.F.R. 438.114(b);

o. Procedures for tracking Appeals when Covered Individuals become aware of the Adverse Action, in the event that no notice had been sent;

p. Handling of Complaints/Grievances;

q. Process used to monitor Subcontractor performance;

r. Claims processing;

s. Engagement and coordination with PCACOs, BH CPs, and other state agencies; and

t. Retention of medical records.

2. Material Subcontracts/Subcontractors

a. Prior to contracting with a Material Subcontractor, the Contractor shall evaluate the prospective Material Subcontractor's ability to perform the activities to be subcontracted.

b. All Material Subcontracts must be prior approved by EOHHS. To obtain such approval, the Contractor shall make a request in writing and submit with that request a completed Material Subcontractor checklist using the template provided by EOHHS and attached hereto as **Appendix B-2**, as may be modified by EOHHS from time-to-time, at least 60 days prior to the date the Contractor expects to execute the Material Subcontract. Among other things required in the checklist, the Contractor must describe the process for selecting the Material Subcontractor, including the selection criteria used.

c. The Contractor shall provide EOHHS with any additional information requested by EOHHS in addition to the information required in the checklist.

d. The Material Subcontract shall:

1) Be a written agreement;

2) Specify, and require compliance with, all applicable requirements of this Contract and the activities and reporting responsibilities the Material Subcontractor is obligated to provide;

3) Provide for imposing sanctions, including contract termination, if the Material Subcontractor's performance is inadequate;

4) Require the Material Subcontractor to comply with all applicable Medicaid laws, regulations, and applicable subregulatory guidance; and

5) Comply with the audit and inspection requirements set forth in 42 CFR 438.230(c)(3), such that the Material Subcontract requires the Material Subcontractor to agree as follows.

a) The State, CMS, HHS Inspector General, the Comptroller General, or their designees, have the right to audit, evaluate, and inspect any records or systems that pertain to any activities performed or amounts payable under this Contract. This right exists through 10 years from the final date of the Contract or from the date of completion of any audit, whichever is later; provided, however that if any of the entities above determine that there is a reasonable possibility of fraud or similar risk, they may audit, evaluate, and inspect at any time; and

b) The Material Subcontractor will make its premises, facilities, equipment, records, and systems available for the purposes of any audit, evaluation, or inspection described immediately above;

e. The Contractor shall monitor any Material Subcontractor's performance on an ongoing basis and perform a formal review annually. If any deficiencies or areas for improvement are identified, the Contractor shall require the Material Subcontractor to take corrective action. Upon request, the Contractor shall provide EOHHS with a copy of the annual review and any corrective action plans developed as a result.

f. Upon notifying any Material Subcontractor, or being notified by such Material Subcontractor, of the intention to terminate such subcontract, the Contractor shall notify EOHHS in writing no later than the same day as such notification, and shall otherwise support any necessary member transition or related activities as described in **Section 2.2** and elsewhere in this Contract.

g. In accordance with **Appendix E-1**, the Contractor shall submit to EOHHS an annual list of all Material Subcontractors. Such annual report shall include notification if any of its Material Subcontractors are a business enterprise (for-profit) or nonprofit organization certified by the Commonwealth's Supplier Diversity Office.

h. The Contractor shall submit ad hoc reports, as frequently as necessary or as directed by EOHHS, with any changes to the above-mentioned list and report.

i. The Contractor shall make best efforts to ensure that all Material Subcontracts stipulate that Massachusetts general law or Massachusetts regulation will prevail if there is a conflict between the state law or state regulation where the Material Subcontractor is based.

j. Notwithstanding any relationship the Contractor may have with a subcontractor, including Material subcontractors, the Contractor shall maintain ultimate responsibility for adhering to and otherwise fully complying with all terms and conditions of this Contract.

k. The Contractor shall remain fully responsible for meeting all of the terms and requirements (including all applicable state and federal regulations) of the Contract regardless of whether the Contractor subcontracts for performance of any Contract responsibility. No subcontract will operate to relieve the Contractor of its legal responsibilities under the Contract.

3. Program Integrity Requirements

a. General Provisions

The Contractor shall:

1) Comply with all applicable federal and state program integrity laws and regulations regarding Fraud, waste and Abuse, including but not limited to, the Social Security Act and 42 CFR Parts 438, 455, and 456.

2) Implement and maintain written internal controls, policies and procedures, and administrative and management arrangements or procedures designed to prevent, detect, reduce, investigate, correct

and report known or suspected Fraud, waste and Abuse activities consistent with 42 CFR 438.608(a) and as further specified in this Contract.

3) In accordance with federal law, including but not limited to Section 6032 of the federal Deficit Reduction Act of 2005, make available written Fraud and Abuse policies to all employees. If the Contractor has an employee handbook, the Contractor shall include specific information about such Section 6032, the Contractor's policies, and the rights of employees to be protected as whistleblowers.

4) Meet with EOHHS regularly and upon request to discuss Fraud, waste and Abuse, audits, overpayment issues, reporting issues, and best practices for program integrity requirements.

5) At EOHHS' discretion, implement certain program integrity requirements for Providers, as specified by EOHHS, including but not limited to implementing National Correct Coding Initiative edits or other CMS claims processing/provider reimbursement manuals, and mutually agreed upon best practices for program integrity requirements.

b. Compliance Plan

1) The Contractor shall, in accordance with 42 CFR 438.608(a)(1), have a compliance plan designed to guard against Fraud, waste and Abuse.

2) At a minimum, the Contractor's compliance plan shall include the following:

a) Written policies, procedures, and standards of conduct that articulate the Contractor's commitment to comply with all applicable federal and state laws regarding Fraud, waste and Abuse;

b) The designation of a compliance officer and a compliance committee, as described in 42 CFR 438.608, that is accountable to senior management;

c) Adequate Massachusetts-based staffing and resources to investigate incidents and develop and implement plans to assist the Contractor in preventing and detecting potential Fraud, waste, and Abuse activities. Staff conducting program integrity activities for the Contractor shall be familiar with MassHealth and state and federal regulations

on Fraud, waste and Abuse;

d) Effective training and education for the Contractor's employees, including but not limited to the Contractor's compliance officer and senior management;

e) Effective lines of communication between the compliance officer and the Contractor's employees, as well as between the compliance officer and EOHHS;

f) Enforcement of standards through well-publicized disciplinary guidelines;

g) Provision for internal monitoring and auditing as described in 42 CFR 438.608;

h) Provision for prompt response to detected offenses, and for development of corrective action initiatives, as well as the reporting of said offenses and corrective actions to EOHHS as stated in this Contract and as further directed by EOHHS; and

i) Communication of suspected violations of state and federal law to EOHHS, consistent with the requirements of this Section;

3) The Contractor's compliance plan shall be in place by the Contract Operational Start Date and in a form and format specified by EOHHS. The Contractor shall provide EOHHS with its compliance plan in accordance with **Appendix E-1**, annually, and when otherwise requested. The Contractor shall make any modifications requested by EOHHS within thirty (30) calendar days of a request.

c. Anti-Fraud, Waste, and Abuse Plan

1) The Contractor shall have an anti-Fraud, waste, and Abuse plan.

2) The Contractor's anti-Fraud, waste, and Abuse plan shall, at a minimum:

a) Require that the reporting of suspected and confirmed Fraud, waste, and Abuse be performed as required by this Contract;

b) Include a risk assessment of the Contractor's various Fraud, waste, and Abuse and program integrity processes, a listing of the Contractor's top three vulnerable areas, and an

outline of action plans in mitigating such risks.

(i) The Contractor shall submit to EOHHS this risk assessment quarterly at EOHHS' request and immediately after a program integrity related action, including financial-related actions (such as overpayment, repayment and fines).

(ii) With such submission, the Contractor shall provide details of such action and outline activities for employee education of federal and state laws and regulations related to Medicaid program integrity and the prevention of Fraud, Abuse, and waste, to ensure that all of its officers, directors, managers and employees know and understand the provisions of the Contractor's compliance plan and anti-Fraud, waste, and Abuse plan;

c) Outline activities for Provider education of federal and state laws and regulations related to Medicaid program integrity and the prevention of Fraud, waste, and Abuse, specifically related to identifying and educating targeted Providers with patterns of incorrect billing practices or overpayments;

d) Contain procedures designed to prevent and detect Fraud, waste, and Abuse in the administration and delivery of services under this Contract; and

e) Include a description of the specific controls in place for prevention and detection of potential or suspected Fraud, waste, and Abuse, such as:

(i) A list of automated pre-payment claims edits;

(ii) A list of automated post-payment claims edits;

(iii) A description of desk and onsite audits performed on post-processing review of claims;

(iv) A list of reports of Provider profiling and credentialing used to aid program and payment integrity reviews;

(v) A list of surveillance and/or utilization management protocols used to safeguard against unnecessary or inappropriate use of Medicaid services;

(vi) A list of provisions in the Subcontractor and Provider

agreements that ensure the integrity of Provider credentials;

f) The Contractor shall have its anti-Fraud, waste, and Abuse plan in place by the Contract Operational Start Date and in a form and format specified by EOHHS. The Contractor shall provide EOHHS with its anti-Fraud, waste, and Abuse plan in accordance with **Appendix E-1**, annually, and when otherwise requested. The Contractor shall make any modifications requested by EOHHS within thirty (30) calendar days of a request.

d. Overpayments

1) Reporting Overpayments to EOHHS

a) The Contractor shall report overpayments to EOHHS using the following reports as specified in this section and **Appendix E-1**:

(i) Notification of Provider Overpayments Report;

(ii) Fraud and Abuse Notification Report;

(iii) Summary of Provider Overpayments Report; and

(iv) Self-Reported Disclosures Report.

b) In accordance with **Appendix E-1**, the Contractor shall submit to EOHHS the Notification of Provider Overpayments Report and Fraud and Abuse Notification Report no later than five business days after the identification of the overpayment.

c) In accordance with **Appendix E-1**, the Contractor shall submit to EOHHS the Summary of Provider Overpayments Report as follows:

(i) The Contractor shall report all overpayments identified, including but not limited to those resulting from potential Fraud, as further specified by EOHHS.

(ii) The Contractor shall, as further specified by EOHHS, report all overpayments identified during the Contract Year, regardless of dates of service, and all investigatory and recovery activity related to those overpayments. This report shall reflect all cumulative activity for the entire Contract Year plus six months

after the end of the Contract Year.

(iii) For any overpayments that remain unrecovered for more than six months after the end of the Contract Year, the Contractor shall continue to report all cumulative activity on such overpayments until all collection activity is completed.

2) Identifying and Recovering Overpayments

a) If the Contractor identifies an overpayment prior to EOHHS:

(i) The Contractor shall recover the overpayment and may retain any overpayments collected.

(ii) In the event the Contractor does not recover an overpayment first identified by the Contractor within one hundred and eighty (180) days after such identification, the Contractor shall provide justification in the Summary of Provider Overpayments report for any initial overpayment amounts identified but not recovered. EOHHS may, at its sole discretion, apply a Capitation Payment deduction equal to the amount of the overpayment identified but not collected in accordance with **Section 5.3.L.10.**

b) If EOHHS identifies an overpayment prior to the Contractor (such that the Contractor did not identify and report to EOHHS the overpayment in accordance with all applicable Contract requirements, including but not limited to the Summary of Provider Overpayments Report, within 180 days of the date(s) of service associated with any claim(s) included in the overpayment):

(i) Within 90 days of EOHHS' notification of the overpayment, the Contractor shall investigate the associated claims and notify EOHHS as to whether the Contractor agrees with or disputes EOHHS's findings, in the Response to Overpayments Identified by EOHHS Report as specified in **Appendix E-1**.

(ii) If the Contractor disputes EOHHS's finding, the Contractor's response shall provide a detailed description of the reasons for the dispute, listing the

claim(s) and amount of each overpayment in dispute.

(iii) If the Contractor agrees with EOHHS's finding:

(a) The Contractor's response shall provide the amount of each overpayment agreed to.

(b) The Contractor shall complete collections of such agreed-upon overpayments. The Contractor shall submit a report to EOHHS of such collections within 90 days of the Contractor's response to EOHHS's notification, in the Agreed Upon Overpayments Collection Report as specified in **Appendix E-1**.

(iv) In the event the Contractor recovers an agreed-upon overpayment first identified by EOHHS within 90 days of the Contractor's response to EOHHS's notification, EOHHS may, at its sole discretion, apply a Capitation Payment deduction equal to 80% of the agreed-upon overpayment amount in accordance with **Section 5.3.L.10**. The Contractor shall retain the remaining 20% of the agreed-upon overpayment amount collected. In the event EOHHS determines that there is a valid justification for any agreed-upon overpayment amounts that cannot be collected (e.g., MFD hold), this Capitation Payment deduction shall be calculated based on the amount collected instead of the initial agreed-upon overpayment amount.

(v) In the event the Contractor does not recover an overpayment first identified by EOHHS within 90 days of the Contractor's response to EOHHS's notification, without providing sufficient justification for any initial overpayment amounts identified but not recovered as determined by EOHHS, EOHHS may, at its sole discretion, apply a Capitation Payment deduction equal to the amount of the overpayment identified but not collected in accordance with **Section 5.3.L.10.**

(vi) No Capitation Payment deductions shall apply to any amount of a recovery to be retained under the False Claims Act cases or through other investigations.

(vii) EOHHS shall calculate, following the end of the

Contract Year, any and all Capitation Payment deductions for any prior Contract Year pursuant to this Section.

(viii) In the alternative to the above process, EOHHS may, in its discretion, recover the overpayment and may retain any overpayments collected.

3) Other Requirements Regarding Overpayments

a) The Contractor shall maintain and require its Providers to use a mechanism for the Provider to report when it has received an overpayment, to return the overpayment to the Contractor within 60 calendar days of the identification of the overpayment, and to notify the Contractor in writing of the reason for the overpayment. The Contractor shall report any such notifications by its Providers To EOHHS in the Self-Reported Disclosures report.

b) The Contractor may not act to recoup improperly paid funds or withhold funds potentially due to a Provider when the issues, services or claims upon which the recoupment or withhold is based on the following:

(i) The improperly paid funds were recovered from the Provider by EOHHS, the federal government, or their designees, as part of a criminal prosecution where the plan had no right of participation, or

(ii) The improperly paid funds currently being investigated by EOHHS are the subject of pending federal or state litigation or investigation, or are being audited by EOHHS, the Office of the State Auditor, CMS, Office of the Inspector General, or any of their agents.

e. Suspected Fraud

1) General Obligations

The Contractor shall:

a) Report, within five business days, in accordance with **Appendix E-1** and all other Contract requirements, any allegation of Fraud, waste, or Abuse regarding a Covered Individual or subcontractor, or EOHHS contractor, consistent with 42 CFR 455.2 or other applicable law to

EOHHS;

b) Notify EOHHS, and receive EOHHS approval to make such contact, prior to initiating contact with a Provider suspected of Fraud about the suspected activity;

c) Take no action on any claims which form the basis of a Fraud referral to EOHHS, including voiding or denying such claims and attempting to collect overpayments on such claims;

d) Provide to EOHHS an annual certification, in a form and format specified by EOHHS, attesting that the Contractor satisfies all Contract requirements regarding suspected Fraud including, but not limited to, the requirement to report any allegation of fraud to EOHHS;

e) Suspend payments to Providers for which EOHHS determines there is a credible allegation of Fraud pursuant to 42 CFR 455.23, and **Section 2.8.G** or as further directed by EOHHS, unless EOHHS identifies or approves the Contractor's request for a good cause exception as set forth in **Section 2.8.G.2.d**.

(i) As further directed by EOHHS, after the conclusion of a Fraud investigation that results in a verdict or settlement obtained by the Office of the Attorney General (AGO) Medicaid Fraud Division the Contractor shall disburse to EOHHS any money the Contractor held in a payment suspension account connected to the investigation to account for the verdict or settlement. For any payment suspensions initiated prior to April 1, 2023, the Contractor shall disburse 40% of such money to EOHHS.

(ii) As further directed by EOHHS, if the amount of money the Contractor held in the payment suspension account exceeds the Provider's liability under the verdict or settlement, the Contractor shall release to the Provider the amount of money that exceeds the Provider's liability under the verdict or settlement.

(iii) As further directed by EOHHS, if EOHHS determines the Contractor may receive a finders' fee performance incentive as described in **Section**

2.3.D.3.e.ii below, the Contractor may retain any money in a payment suspension account necessary to satisfy all or part of the amount of such finders' fee performance incentive. If the Contractor is entitled to a finder's fee performance incentive in an amount greater than the amount held in a payment suspension account, EOHHS will pay the Contractor the difference between the amount of the performance incentive and the amount in the payment suspension account.

f) The Contractor and subcontractors shall cooperate, as reasonably requested in writing, with the Office of the Attorney General's Medicaid Fraud Division, the Office of the State Auditor's Bureau of Special Investigations (BSI), or other applicable enforcement agency. Such cooperation shall include, but not be limited to, providing at no charge, prompt access and copies of any documents and other available information determined necessary by such agencies to carry out their responsibilities regarding fraud and abuse, maintaining the confidentiality of any such investigations, and making knowledgeable staff available at no charge to support any investigation, court, or administrative proceeding.

2) Monetary Recoveries by the Office of the Attorney General's Medicaid Fraud Division

a) Except as otherwise provided within this section, EOHHS shall retain all monetary recoveries made by MFD arising out of a verdict or settlement with Providers.

b) The Contractor shall receive a finders' fee performance incentive as follows:

(i) To receive the finders' fee performance incentive, the Contractor shall satisfy, in EOHHS' determination, the following requirements as they relate to MFD's case against a Provider:

(a) The Contractor made a Fraud referral to EOHHS pursuant to **Section 2.3.D.3.e**

(b) The Contractor's Fraud referral provided sufficient details regarding the Provider(s)', conduct, and time period of the allegation(s)

of Fraud at issue;

(c) The Contractor attests, in a form and format specified by EOHHS, that the fraud referral arose out of the Contractor's own investigatory activity that led to the identification of the allegation(s) of Fraud at issue;

(d) The Contractor complies with all other obligations in **Section 2.3.D.3.e**;

(e) The Contractor made its Fraud referral to EOHHS prior to MFD's investigation becoming public knowledge; and

(f) The basis of the Contractor's Fraud referral – the specific Provider and allegedly fraudulent conduct – is the subject of a verdict or settlement achieved by MFD with a Provider that requires the Provider to pay EOHHS.

(ii) The amount of the finders' fee performance incentive, as determined by EOHHS, shall be as set forth in **Section 4.6.D**.

3) The Contractor shall abide by and adhere to any release of liability regarding a Provider in any verdict or settlement signed by MFD or EOHHS.

f. Other Program Integrity Requirements

The Contractor shall:

1) Prior to initiating an audit, investigation, review, recoupment, or withhold, or involuntarily termination of a Network Provider, the Contractor shall request from EOHHS deconfliction, cease all activity, and wait to receive permission from EOHHS to proceed. The Contractor shall wait until EOHHS either grants the deconfliction request or notifies the Contractor to continue to cease activity so as not to interfere in a law enforcement investigation or other law enforcement activities.

2) Notify EOHHS within two business days after contact by the Medicaid Fraud Division, the Bureau of Special Investigations or any other investigative authorities conducting Fraud and Abuse investigations, unless specifically directed by the investigative authorities not to notify EOHHS. The Contractor, and where

applicable any Material Subcontractors or subcontractors, shall cooperate fully with the Medical Fraud Division, Bureau of Special Investigations, and other agencies that conduct investigations; full cooperation includes, but is not limited to, timely exchange of information and strategies for addressing Fraud and Abuse, as well as allowing prompt and direct access to information, free copies of documents, and other available information related to program violations, while maintaining the confidentiality of any investigation. The Contractor shall make knowledgeable employees available at no charge to support any investigation, court, or administrative proceeding;

3) Report promptly to EOHHS, in accordance with **Appendix E-1** and all other Contract requirements, when it receives information about a Covered Individual's circumstances that may affect their MassHealth eligibility, including but not limited to a change in the Covered Individual's residence and the death of the Covered Individual;

4) Report no later than five business days to EOHHS, in accordance with **Appendix E-1** and all other Contract requirements, when it receives information about a Provider's circumstances that may affect its ability to participate in the Contractor's network or in MassHealth, including but not limited to the termination of the Provider's contract with the Contractor;

5) Verify, in accordance with other Contract requirements, through sampling, whether Covered Services that were represented to be delivered by Providers were received by Covered Individuals. The Contractor shall report the identification of any overpayments related to Covered Services that were represented to be delivered by Providers but not received by Covered Individuals in the following reports as set forth in **Appendix E-1**: Fraud and Abuse Notification, Notification of Provider Overpayments, and Summary of Provider Overpayments report;

6) Provide employees, as well as Material Subcontractors and agents, detailed information about the False Claims Act and other federal and state laws described in section 1902(a)(68) of the Social Security Act, including whistleblower protections.

   a) The Contractor shall comply with all federal requirements for employee education about false claims laws under 42 U.S.C. §1396a(a)(68) if the Contractor received or made Medicaid payments in the amount of at least $5 million

during the prior federal fiscal year.

b) If the Contractor is subject to such federal requirements, the Contractor shall:

(i) On or before April 30th of each Contract Year, or such other date as specified by EOHHS, provide written certification, in accordance with **Appendix E-1** or in another form acceptable to EOHHS, and signed under the pains and penalties of perjury, of compliance with such federal requirements;

(ii) Make available to EOHHS, upon request, a copy of all written policies implemented in accordance with 42 U.S.C. §1396a(a)(68), any employee handbook, and such other information as EOHHS may deem necessary to determine compliance; and

c) Failure to comply with this Section may result in intermediate sanctions in accordance with **Section 5.3.L.**

7) Designate a Fraud and Abuse prevention coordinator responsible for the following activities. Such coordinator may be the Contractor's compliance officer. The Fraud and Abuse prevention coordinator shall:

a) Assess and strengthen internal controls to ensure claims are submitted and payments properly made;

b) Develop and implement an automated reporting protocol within the claims processing system to identify billing patterns that may suggest Provider and Covered Individual Fraud and shall, at a minimum, monitor for under-utilization or over-utilization of services;

c) Conduct regular reviews and audits of operations to guard against Fraud and Abuse;

d) Receive all referrals from employees, Covered Individuals, or Providers involving cases of suspected Fraud and Abuse and developing protocols to triage all referrals involving suspected Fraud and Abuse;

e) Educate employees, Providers, and Covered Individuals about Fraud and how to report it, including informing employees of their protections when reporting fraudulent activities per Mass. Gen. Laws Ch. 12, section 5J; and

f) Establish mechanisms to receive, process, and effectively respond to complaints of suspected Fraud and Abuse from employees, Providers, and Covered Individuals, and report such information to EOHHS.

8) In accordance with Mass. Gen. Laws. Ch. 12, section 5J, not discriminate against an employee for reporting a fraudulent activity or for cooperating in any government or law enforcement authority's investigation or prosecution;

9) Upon a complaint of Fraud, waste, or Abuse from any source or upon identifying any questionable practices, report the matter in writing to EOHHS within five business days;

10) Make diligent efforts to recover improper payments or funds misspent due to fraudulent, wasteful or abusive actions by the Contractor, its parent organization, its Providers, or its Material Subcontractors;

11) Require Providers to implement timely corrective actions related to program integrity matters as approved by EOHHS or terminate Provider Contracts, as appropriate;

12) In accordance with **Appendix E-1**, submit a Summary of Provider Overpayments report in a form and format and at times specified by EOHHS, and submit ad hoc reports related to program integrity matters as needed or as requested by EOHHS;

13) In accordance with **Appendix E-1**, have the CEO or CFO certify in writing to EOHHS that after a diligent inquiry, to the best of their knowledge and belief, the Contractor is in compliance with this Contract as it relates to program integrity requirements and has not been made aware of any instances of Fraud and Abuse other than those that have been reported by the Contractor in writing to EOHHS.

g. Screening Employees and Subcontractors

In addition to the requirements set forth in **Section 2.8.G**, the Contractor shall screen employees and subcontractors by searching the Office of the Inspector General List of Excluded Individuals Entities and exclusion databases, including but not limited to those listed in **Appendix J** to determine if any such individuals or entities are excluded from participation in federal health care programs.

1) The Contractor shall conduct such screening upon initial hiring or contracting and on an ongoing monthly basis, or other frequency

specified at **Appendix J**.

2) The Contractor shall notify EOHHS of any discovered exclusion of an employee or subcontractor within two business days of discovery.

3) The Contractor shall require its Providers to also comply with the requirements of this section with respect to its own employees and subcontractors.

h. Screening Providers

The Contractor shall screen Providers in accordance with the requirements set forth in **Section 2.8.G**.

4. Continuity of Operations Plan

The Contractor shall maintain a continuity of operations plan that addresses how the Contractor's, Material Subcontractors', and other subcontractors' operations shall be maintained in the event of a natural disaster, terrorist attack, pandemic or other event which leads to a significant disruption in operations due to staff absence and/or loss of utilities. The Contractor shall provide copies of such plan with EOHHS upon request and shall inform EOHHS whenever such plan shall be implemented.

Section 2.4 Enrollment and Education Activities

A. Eligibility Verification

The Contractor shall instruct and assist the Contractor's Providers in the process and need for verifying a Covered Individual's MassHealth eligibility and enrollment prior to providing any service at each point of service, through the use of a platform or portal maintained by the Contractor that utilizes real time EOHHS eligibility data (e.g., 834 files); provided, however, the Contractor and its Providers shall not require such verification prior to providing Emergency Services.

B. Enrollment and Disenrollment

The Contractor shall:

1. Provide EOHHS, upon EOHHS request, with sufficient enrollment packages and Marketing Materials to use as training materials and reference guides for EOHHS's enrollment vendor staff and to be distributed by EOHHS's enrollment vendor to Covered Individuals upon request.

2. On each business day, obtain from EOHHS, via the HIPAA 834 Enrollment File, and process information pertaining to all enrollments in the Contractor's Plan including the Effective Date of Enrollment;

3. Accept for enrollment all Members, as described in **Section 4.1**, identified by EOHHS in the order in which they are referred without restriction;

4. Accept for enrollment all Members identified by EOHHS at any time without regard to income status, physical or mental condition (such as cognitive, intellectual, mobility, psychiatric, and sensory disabilities as further defined by EOHHS), age, gender, sexual orientation, religion, creed, race, color, physical or mental disability, national origin, ancestry, status as a Member, pre-existing conditions, expected health status, or need for health care services;

5. Not request the disenrollment of any Covered Individual due to an adverse change in the Covered Individual's health status or because of the Covered Individual's utilization of medical services, diminished mental capacity, or uncooperative or disruptive behavior resulting from the Covered Individual's special needs. The Contractor, however, may submit a written request, accompanied by supporting documentation, to EOHHS to disenroll a Covered Individual, for cause, for the following reason:

    a. After reasonable efforts, the Contractor has attempted to provide Medically Necessary BH Covered Services to the particular Covered Individual through at least three Network Providers that:

        1) Meet the access requirements specified in **Section 2.9.B** for the relevant provider type; and

        2) Are critical for providing ongoing or acute BH Covered Services to meet the Covered Individual's needs;

    b. Where reasonable efforts include attempting to provide all resources routinely used by the Contractor to meet Covered Individuals' needs, including but not limited to, Behavioral Health Services and Care Management; and

    c. Despite such efforts, the continued enrollment of the Covered Individual with the Contractor seriously impairs the Contractor's ability to furnish services to either this particular Covered Individual or other Covered Individuals.

6. EOHHS reserves the right, at its sole discretion, to determine when and if the Contractor's request to terminate the enrollment of a Covered Individual will be granted based on the criteria in **Section 2.4.B.3** above. In addition, if EOHHS determines that the Contractor too frequently requests termination of enrollment for Covered Individuals, EOHHS reserves the right to deny such requests and require the Contractor to initiate corrective action to improve the Contractor's ability to serve such Covered Individuals.

7. The Contractor, upon EOHHS request, shall be able to verify if a Covered

Individual resides in an intermediate care facility for persons with intellectual disability, a state psychiatric hospital, or a locked DYS facility; such verification shall include the date of admission to such facility and shall be in a form and format approved by EOHHS.

C. Enrollee Outreach, Orientation, and Education

The Contractor shall:

1. For each new Enrollee who enrolls in the PCC Plan after the Contract Operational Start Date, but who has not been enrolled in the PCC Plan in the past six months, offer and make best efforts to provide to the Enrollee an orientation, by telephone or in person, within 30 days of the Enrollee's Effective Date of Enrollment in the PCC Plan. The Contractor shall submit to EOHHS for review and approval its orientation and outreach materials and phone scripts. Such orientation shall include, at a minimum:

    a. How the PCC Plan operates, including the role of the PCC;

    b. A description of MassHealth Covered Services and service limitations;

    c. Information on participating PCC Plan Providers and how to access the provider directory either via the internet or in writing;

    d. The value of screening and preventive care;

    e. How to obtain MassHealth Covered Services; and

    f. Information about the availability of and access to Ombudsman's services.

2. The Contractor shall also provide the orientation described in **Section 2.4.C.1** above to parents or guardians of newborns that are enrolled in the PCC Plan, to the extent applicable. As part of such orientation, the Contractor shall confirm the selection or assignment to a pediatrician within the newborn's geographic area as an appropriate PCC.

3. The Contractor must provide a range of health promotion and Wellness information and activities for Enrollees in formats that meet the needs of all Enrollees. The Contractor shall:

    a. Work with EOHHS to implement innovative Enrollee education strategies for Wellness care and immunizations, as well as general health promotion;

    b. Work with PCCs and specialists, as appropriate, to integrate health education, Wellness and prevention training into the care of each Enrollee;

    c. Participate in any EOHHS-led joint planning activities with MassHealth-contracted MCOs and ACOs to develop and implement statewide or regional approaches to Covered Individual health and Wellness education;

d. Provide condition- and disease-specific information and educational materials to Covered Individuals, including information on its Care Management Program described in **Section 2.5**; and

e. Provide condition- and disease-specific information and educational materials to Enrollees.

4. Ensure, in accordance with 42 U.S.C. § 1396u-2(a)(5), that all written information for use by Enrollees and potential Enrollees is prepared in a format and manner that is easily readable, comprehensible to its intended audience, well designed, and includes a card or other notice instructing the Enrollee in multiple languages that the information affects their health benefit, and to contact EOHHS for assistance with translation.

5. Make best efforts to obtain updated contact information whenever the Contractor has been unable to contact an Enrollee as a result of undeliverable mail or an incorrect telephone number. On a monthly basis, notify EOHHS of all Enrollees whom the Contractor has been unable to contact. Such notification shall be in the format and process specified by EOHHS in consultation with the Contractor.

Section 2.5 Care Management, Care Coordination and Supporting Dispositions from the ED

A. The Contractor is responsible for providing care management or care coordination support for Covered Individuals as follows:

1. The Contractor shall operate a Care Management Program for PCC Plan Enrollees as set forth in this Section, consistent with **Section 2.19**, and as further specified by EOHHS, to serve Enrollees with complex medical, mental health or substance use disorders. The Care Management Program shall consist of an Integrated Care Management Program (ICMP) and a Practice Based Care Management (PBCM) program, as set forth in **Section 2.5.B-H**. The Contractor shall identify Enrollees for both PBCM and the ICMP based on medical risks, behavioral risks and social determinants of health.

2. The Contractor shall offer to collaborate with PCACOs and Behavioral Health Community Partners (BHCPs) for Covered Individuals that are members of PCACOs, as described in **Section 2.5.I.**

3. The Contractor shall offer care coordination support to Covered Individuals not enrolled in the PCC Plan or PCACO as described in **Section 2.5.J**.

4. The Contractor shall support all Covered Individuals that are awaiting disposition in the ED as described in **Section 2.5.K**.

B. Care Management Program for PCC Plan Enrollees

1. Practice Based Care Management (PBCM)

The Contractor shall:

a. Operate Practice Based Care Management (PBCM) in all regions to PCCs and BH Providers serving Enrollees. Expanding PBCM includes providing technical assistance on topics such as approaches to population health management for the high risk/complex Enrollees and strategies to engage Enrollees into care management, as well as support for the provision of care management as needed by the participating practice.

b. Monitor each practice's compliance with the PBCM contract.

c. Submit to EOHHS a plan to promote and increase the number of PCC service locations enrolled in PBCM.

d. The Contractor shall provide direct-to-Provider practice transformation support services for established and expanded PBCMs, including but not limited to, Behavioral Health consultation, Enrollee engagement strategies and supports, population health management strategies, state agency resources, and care management tools.

e. As directed by EOHHS, the Contractor shall enter into a provider arrangement with a specialized provider or organization to provide intensive PBCM to up to 33 Covered Individuals identified by EOHHS with complex and acute medical needs in a fully integrated setting, at a rate to be specified by EOHHS.

2. Integrated Care Management Program (ICMP)

a. The Contractor shall operate an enhanced care management program known as the Integrated Care Management Program (ICMP) for Enrollees with complex medical, mental health and/or substance use disorders.

b. The Contractor shall also identify pregnant and postpartum Enrollees with the following high-risk conditions for outreach and engagement in the ICMP:

1) any history of complex or severe Behavioral Health diagnosis;

2) any history of substance use disorder, including opioids, alcohol, tobacco, or other substances;

3) any current chronic physical health diagnosis which may complicate pregnancy or postpartum (i.e., hypertension, diabetes, HIV, etc.);

4) any history of adverse maternal or neonatal outcomes in previous pregnancies, including any instances of severe maternal morbidity; and/or

5) any current complex social conditions which could impact outcomes during pregnancy or postpartum (i.e., unsafe living environment, significantly late prenatal care initiation, food or housing insecurity, etc.).

c. The Contractor shall identify Enrollees for outreach and engagement in the ICMP through predictive modeling using Behavioral Health, Medical and Pharmacy claim data (historical and current), acceptance of referrals from PCCs, EOHHS staff, Enrollees or other providers for participation in the ICMP, and communication with Enrollees and Providers about ICMP.

d. The Contractor shall provide monthly reports as further specified by EOHHS for Enrollees identified by the Contractor as eligible for ICMP, as well as the methodology by which these members are identified.

e. For each Enrollee in the ICMP, the Contractor shall:

1) Provide Care Management (which are clinical care related services rendered to the member directly either in person or via telephone as per the individual care plan) and Care Coordination (which are care activities rendered by the Contractor on behalf of the Enrollee) to identified Enrollees who have complex medical or Behavioral Health needs and whose overall health care may benefit from the assistance of a Care Manager.

2) provide holistic coordinated health care, social supports, and wellness and recovery tools, and shall assist Enrollees with identifying and using their medical home for treatment of Behavioral Health and medical conditions.

C. Integrated Design for Care Management

1. The Contractor shall submit to EOHHS a work plan for the Contract Year, including timelines, for providing ongoing support for PBCM programs and providing integrated care management for Enrollees served in ICMP. The work plan shall include the supports offered by the Contractor's care management staff related to care management activities provided by PBCMs.

2. The work plan shall be submitted, for review and approval, within two months of the first day of the current Contract Year. This work plan shall:

a. Prioritize direct real-time referrals to ICMP for high risk Enrollees not served by PBCM programs;

b. Describe the process of referring Enrollees from ICMP to PBCMs, where appropriate;

c. Include a description and process for Care Coordination activities within ICMP for those Enrollees in need of primary complex Care Coordination;

d. Address care management services for those Enrollees transitioning to the community from long term support services;

e. Address the expansion of PBCM and plan-based programs throughout the Commonwealth to provide care management for Enrollees identified by the Contractor as high risk and eligible for care management, including ICMP among members for whom PBCM is not available;

f. Include the supports and services offered by the Contractor to Providers who request support from the Contractor for their care management program;

g. Include an ICMP staffing plan with that includes professional licensed staff, Certified Mental Health Peer Specialists, Peer Recovery Coaches, and community health workers, including the functions to be performed by para-professional staff under the clinical supervision of licensed clinical staff. Licensed staff includes Behavioral Health clinicians and nurses. All ICMP para-professional staff shall be employed directly by the Contractor;

h. Include the functions of the PCC Support Managers as an ICMP team member; and

i. Include proposals to provide ICMP to high risk populations other than Enrollees who are pregnant or postpartum.

3. Within three months of the first day of the current Contract Year, the Contractor shall submit to EOHHS any updates in the policies and procedures for daily operation of the care management program.

4. The Contractor shall specifically tailor the care management provided to improve the health outcomes of each Participant, including such items as the frequency and intensity of interventions, and ensuring that the staff assigned to the Participant is appropriate based on each Participant particular needs.

a. The Contractor shall include in each Participant's plan a range of care management activities that may vary in frequency or intensity depending on the Participant's clinical needs.

b. The Contractor shall assign a registered nurse, or a Behavioral Health licensed care manager who shall oversee their assigned caseload, perform

direct clinical activities and oversee all Care Coordination or support activities performed by para-professional staff.

5. The Contractor shall educate all Participants in self-care strategies, illness prevention and Wellness Program activities, and ensure that staff assigned to the Participant have knowledge of community-based services and supports.

6. Within six (6) months of the beginning of each Contract Year, the Contractor shall evaluate the current ICMP electronic system for tracking, profiling and managing Participants, including but not limited to face-to-face, telephonic, home visits, e-mail, texts, and mail encounter(s) between the care manager and the Participant and submit to EOHHS the results of the evaluation, including data to demonstrate the performance of the current ICMP electronic system and details of improvements that will be pursued.

D. Identification and Engagement of Enrollees for Care Management

1. The Contractor shall use a predictive modeling tool that incorporates health claims data in its algorithm to stratify high risk Enrollees for Enrollment into a PBCM or ICMP. EOHHS may in its sole discretion instruct the Contractor to use EOHHS's risk stratification of the PCC Plan for the Care Management Program. EOHHS may also request from the Contractor its risk stratification data on Enrollees. The Contractor shall work with the PBCM programs to determine sites in need of population-based stratification of high-risk members.

2. The Contractor shall use the Health Needs Assessment (HNA) tool to identify Enrollees who may want to participate in care management.

3. The ICMP shall accept referrals of Enrollees who might be appropriate for care management or who may want to participate in care management from EOHHS, the Contractor's staff, PCCs, state agencies, Enrollees, other Providers, hospital discharge planners, Network Providers, or other knowledgeable sources.

4. The Contractor shall provide each practice offering the PBCM program a monthly list of Enrollees affiliated with the PBCM eligible for care management.

5. The Contractor shall serve high-risk, complex, and specialty populations of Enrollees referred to CMP and not associated with PBCM, unless otherwise requested.

6. The Contractor shall document CMP Engagement activities in-person or telephonic encounters with or on behalf of an Enrollee for the purposes of completing a comprehensive health assessment, creating an Individual Care Plan (ICP), and implementing the Participant's ICP. These care management activities including in-person or telephonic voice-to-voice contact with the Participant must occur no less than once each month while the Participant is enrolled in the Care Management Program. When the Contractor's documented attempts to contact the

Participant within thirty (30) days are unsuccessful, the Contractor shall ensure that face-to-face or telephonic voice-to-voice contact with the Participant is made within sixty (60) days.

7. The Contractor shall ensure that Enrollees, PCCs, and Behavioral Health Network Providers are informed about the plan-based Care Management Program in sufficient detail so that Enrollees, PCCs, and Behavioral Health Network Providers understand the program and how to participate.

8. The Contractor shall submit to EOHHS for approval within three (3) months of the beginning of each Contract Year a work plan for informing Enrollees, PCC's and Behavioral Health Network Providers of the plan-based Care Management Program. The work plan shall include a plan for outreach to and Engagement of identified or referred Enrollees.

9. The Contractor shall document the Participant's verbal consent to participate in the Care Management Program, noting the date consent was given, the care management staff to whom the consent was given, and, to the extent that the person giving consent is not the Participant, document the name of the person giving consent and the authority of that person to do so (e.g., "parent" or "guardian"). Additionally, the Contractor shall send a letter to the Participant explaining the Care Management Program in sufficient detail so that the Participant understands the program for which the verbal consent was given and provide sufficient information so that the Participant may opt out.

10. The Contractor shall make available to EOHHS the Contractor's contract with the PBCMs and the outreach, Enrollment and reporting processes expected of PBCMs.

11. On a quarterly basis the Contractor shall provide monthly rosters to EOHHS of all members enrolled and engaged in ICMP or PBCM.

12. At the discretion of EOHHS, the Contractor shall utilize other reports provided by EOHHS (e.g. Community Partner Enrollment roster for PCC Plan members and/or the CARES Enrollment Report) to determine member eligibility for Care Management.

E. Assessment of an Enrollee for Care Management

1. Prior to an assessment for the ICMP, the Contractor shall ensure that Enrollees eligible for participation in PBCM will not be assessed for ICMP.

2. The Contractor shall ensure that an assessment by appropriate health care professionals is conducted for Enrollees identified for care management. The care management assessment shall include the following components:

a. Assessment of an Enrollee's physical and Behavioral Health status including cognitive functioning and condition-specific issues, including the Enrollee's understanding of their condition-specific issues;

b. Enrollee's history, needs, and preferences with regard to race, ethnicity, language, culture, literacy, gender identity, sexual orientation, income, housing status, recent incarceration, food insecurity and other social characteristics;

c. Assessment of the Enrollee's health care utilization patterns, including ED visits, types and variety of Providers who have treated the Enrollee and the Enrollee's diagnoses, if any;

d. Documentation of clinical history, including medications and response to treatment;

e. Assessment of risk for violence, suicide, substance use;

f. Assessment of activities of daily living;

g. Assessment of life planning activities; and

h. Evaluation of caregiver resources and natural community supports.

3. A licensed Behavioral Health clinician or a nurse supervisor will determine the type of support an Enrollee needs, including whether the Enrollee requires intensive Care Coordination activities without significant additional care management support. All Care Coordination activities will be documented in an electronic system.

F. Development, Implementation and Monitoring of an Individual Care Plan (ICP) for Care Management

The Contractor shall:

1. Develop required ICPs for, and with, Participants receiving ICMP care management and ensure that an ICP is developed by PBCMs for their Participants.

2. Ensure that the ICMP care manager coordinates a Participant's care across the Contractor's staff, including BH service authorization and BH Utilization Management, and utilizes a multidisciplinary Care Team that includes the Participant, the PCC, and others who are stakeholders in the Participant's care (e.g., family members, Peer Support, BH Providers or other specialists, state agency case managers and/or service providers, and other community supports), as agreed to by the Participant;

3. Ensure that the ICP addresses the Participant's specific medical and BH care needs and includes the following components:

a. Long- and short-term goals identified by the Participant and care management team that seek to reduce the risk and help manage the complexity of the Participant's health conditions;

b. Identification of Barriers to meeting goals and consideration of the Participant's ability to adhere to treatment plans;

c. Development of a schedule for follow-up and ongoing Participant assessment and communication;

d. Development and communication of self-management, health promotion, and Wellness Programs for Participant;

e. Assessment of progress toward meeting goals established in the ICP; and

f. Behavioral Health Crisis Prevention/Response Plans and Safety and Wellness Action Plan as appropriate.

4. Initiate activities, as indicated in the ICP, related to care management to ensure:

a. Medication review and reconciliation;

b. Communication with other treating Providers and other supports identified by the Enrollee;

c. Comprehensive care transition planning;

d. Education on self-management of chronic conditions; and

e. Education and empowerment of Participants and their family support system.

5. Initiate activities, as indicated in the ICP, to ensure Participants' timely and coordinated access to Primary, medical specialty and BH care, such as:

a. Ensuring access to necessary translation/interpretation services and any other accommodations necessary to assure accessibility of services;

b. Reinforcement of PCC, specialists or other Network Provider instructions;

c. Guidance and assistance with obtaining a PCC/medical home for Enrollees when needed;

d. Assistance in scheduling appointments;

e. Well-visit and preventive care self-management reminders;

f. Medical and BH appointments reminders and confirmation with the Participant that appointments have been kept;

g. Wellness activities (e.g., smoking cessation, weight loss);

h. Confirming with Participants that they are adhering to medication recommendations;

i. Ensuring certified Mental Health Peer Specialists are available to individuals recommended to receive such services as part of their care plan; and

j. Facilitating communities of social supports available for Participants.

6. Provide the Participant with the opportunity to sign off on or verbally agree to the ICP goals and treatment plan prior to the implementation of such plan. Such plan shall be signed or otherwise approved by the Participant. The Contractor shall establish and maintain policies and procedures to ensure a Participant can sign or otherwise convey approval of his or her ICP when it is developed or subsequently modified. Such policies and procedures shall include:

a. Informing a Participant of his or her right to approve the ICP;

b. Providing the Participant with a copy of the ICP;

c. Providing mechanisms for the Participants to sign or otherwise convey approval of the ICP. Such mechanisms shall meet the Participants accessibility needs;

d. Informing the Participant of his or her right to an appeal for any Adverse Action related to services included in the ICP; and

e. Informing the Participant of the availability of Ombudsman services.

7. On at least a monthly basis, assess and monitor each Participant's ICP to ensure that the goals set forth in the ICP are met, the Participant's compliance is monitored, and recommendations for follow-up and all ICP activities are documented in the Participant's ICP.

G. Care Management Activities

The Contractor shall:

1. Assist Providers and Participants in the development of an appropriate ICMP discharge plan when the Enrollee changes treatment settings or is admitted to an in-patient treatment program. The development of a discharge plan shall occur prior to a Participant's hospital or long term care setting discharge or change in treatment setting, in coordination with appropriate staff, including but not limited to discharge planners, care managers, staff, the Participant's PCC, and other Network Providers. Where possible, the care manager should be present at Discharge Planning meetings for Enrollees within their caseload;

2. Ensure that PBCM providers develop appropriate discharge plans for their Participants transitioning between treatment settings. Complete discharge plans

for continuity of care for Participants who transition from ICMP to PBCM or ACO or MCO care management programs;

3. Provide on-going ICMP clinical updates and Care Coordination activities to PCCs and BH Providers for ICMP Participants with complex conditions. The Contractor shall document any clinical information received from the PCC or BH Provider in the ICMP record. The Contractor shall ensure via record review that PBCM providers provide and document clinical updates and Care Coordination activities for their Participants;

4. As necessary for successful Participant Enrollment and tenure, ensure face-to-face contact occurs in home visits, community, inpatient, or emergency department settings, as necessary and appropriate;

5. Facilitate communication among the ICMP Participant, the PCC, the Network Provider and other specialty Providers, and the Participant's support network, as identified by the Participant, who are involved in the Participant's health care, to promote service delivery coordination and improved outcomes;

6. Ensure PBCM programs facilitate communication and service delivery coordination to improve outcomes for their Participants;

7. Monitor medical and pharmacy utilization for ICMP Participants through claims data obtained from EOHHS and appropriately update the ICP and coordinate follow-up care as indicated through data received;

8. Educate and provide to the ICMP Participant and Provider, as appropriate, EOHHS-approved informational materials created by the Contractor or obtained from external sources, about the ICMP Participant's medical or BH condition;

9. Document activities related to the provision of Care Management to ICMP Enrollees and share progress reports with care team members, with written consent from the Enrollees, if required by law; and

10. Prior to any disclosures regarding a Participant made during the provision of care management services, obtain written consent if required by law, and maintain a copy of it in each individual Participant’s files at the Contractor's principal place of business, to the extent required by law.

H. ICMP and Transition to Practice-Based Care Management Programs

The Contractor shall provide either a transition or discharge summary when a Participant transitions to a PBCM from ICMP to encourage a seamless transition and continuity of care. Such transition or discharge summary shall include but not be limited to a summary of the Participant’s care plan, care goals and Barriers to completing care goals. This transition plan can be facilitated face-to-face, telephonically, or through the ICMP clinical meeting.

I. Collaboration with PCACOs and Behavioral Health Community Partners (BHCPs)

1. The Contractor shall collaborate with the PCACOs, as further specified by EOHHS, to support Covered Individuals that are PCACO members. Collaboration shall include but not be limited to:

    a. Care coordination;

    b. Event notification and utilization monitoring;

    c. Quality management and improvement;

    d. Integration of primary care and Behavioral Health;

    e. Risk stratification;

    f. Data collection, analytics, management, and reporting;

    g. Network development and management; and

    h. Other tasks as directed by EOHHS.

2. The Contractor shall collaborate with PCACO-contracted BHCPs, as further specified by EOHHS. Collaboration shall include but not be limited to:

    a. Referring PCACO-enrolled Covered Individuals who may benefit from BHCP support to BHCP, via such systems and processes determined by PCACOs;

    b. Care coordination;

    c. Data collection, analytics, management, and reporting; and

    d. Other tasks as directed by EOHHS.

J. Coordination for Covered Individuals not enrolled in the PCC Plan or a PCACO, including children in care and custody of DCF and DYS

1. The Contractor shall establish clinical protocols for providing Care Coordination to a Covered Individual who is not an Enrollee when:

    a. The Covered Individual presents with a pattern or history of:

        1) high inpatient utilization;

        2) ongoing active involvement with other state agency services and programs;

        3) frequent AMCI/YMCI utilization;

        4) inconsistent pattern of follow through with outpatient BH treatment;

5) utilization of both psychiatric inpatient and detoxification services; or

6) co-existing medical and BH problems; or

b. The Covered Individual presents to a Network Provider with complex child custody and placement issues that are adversely affecting the provision of Behavioral Health and medical services, inclusive of youth in in the care and custody of the Commonwealth.

2. The Contractor shall accept referrals from EOHHS, PCPs, state agencies, Network Providers, or other knowledgeable sources identifying Covered Individuals who may be appropriate for Care Coordination as described in this **Section 2.5.J**.

3. Within thirty days of the first day of the Contract Year, the Contractor shall submit to EOHHS a work plan for Contract Year One, for the Clinical Service Coordination programs as described in this **Section 2.5.J**, for EOHHS review and approval.

4. The Contractor shall provide Care Coordination for Covered Individuals as follows by:

a. Ensuring that each Covered Individual has a specifically assigned Care Coordinator:

1) With the authority to authorize Covered Services pursuant to the Covered Individual's plan;

2) Who shall convene an interdisciplinary team for service planning meetings; and

3) Who shall work directly with state agency representatives in coordinating care to expedite a timely community placement as part of the Discharge Planning activities described in **Section 2.5.C.5.c**.

b. Ensuring that each Covered Individual has a service plan that addresses the Covered Individual's specific BH care needs, including short-term and long-term service needs and, as applicable, medical services the Covered Individual may require and that coordinates BH services with services provided by other state agencies involved with the Covered Individual;

c. Ensuring that the service plan is sent to the Covered Individual's Primary Care Practitioner after receiving consent, if such consent is required;

d. Facilitating a schedule of home visits and face-to-face contacts with the Covered Individual, if appropriate;

e. Facilitating communication among the Covered Individual, Primary Care Practitioner, Network Providers and other specialty providers involved in the Covered Individual's health care, to promote service delivery coordination and improved outcomes;

f. Providing linkages with staff in other state agencies and community service organizations that may be able to provide services the Covered Individual needs;

g. Assisting the Covered Individual to access Primary Care and medical specialty care;

h. Ensuring that each Covered Individual receives his or her Care Coordinator's contact information;

i. Implementing procedures to coordinate the services that the Contractor furnishes to the Covered Individual:

1) between settings of care, including appropriate discharge planning for short- and long-term hospital and institutional stays;

2) with the services the Covered Individual receives in fee-for-service Medicaid; and

3) with the services the Covered Individual receives from community and social support providers.

K. Reduction in Covered Individuals Awaiting Disposition in the Emergency Department (ED)

The Contractor shall make best efforts to minimize Covered Individuals awaiting disposition in EDs as follows:

1. The Contractor shall develop a plan to support EOHHS' efforts to reduce Covered Individuals waiting in EDs for disposition to Behavioral Health care. The plan shall include the specific strategies the Contractor shall engage in to reduce transition times from the ED to other services, with a focus on hard to place individuals.

2. The Contractor shall provide timely access to medically necessary, clinically appropriate BH Covered Services for populations determined by EOHHS to be disproportionately boarded in EDs, including but limited to individuals with:

a. Autism Spectrum Disorder-Intellectual Disability (ASD-ID);

b. Developmental and Intellectual Disabilities;

c. Dual Diagnosis for mental health and substance use disorder;

d. Co-morbid Medical Condition; and

e. Assaultive or combative presentation resulting in the need for special accommodation in an inpatient psychiatric setting.

3. When directed and as further specified by EOHHS, the Contractor shall contract with Acute Outpatient Hospital (AOH) EDs to deliver Behavioral Health crisis services to Covered Individuals. When directed and as further specified by EOHHS, create and sustain a network management structure to oversee the provision of Behavioral Health crisis services in AOH EDs.

4. The Contractor shall work in collaboration with PCACOs, PCCs and EDs to facilitate transitions from the ED to other care settings, including supporting providers in identifying appropriate placements.

5. The Contractor shall report to EOHHS on any Covered Individuals awaiting placements in a 24-hour level of Behavioral Health care who remain in an ED for 24 hours or longer, through the Behavioral Health Treatment and Referral Platform and the activities the Contractor will take to assist in identifying an appropriate location, in a form and format and at a frequency to be determined by EOHHS.

Section 2.6 Covered Services

A. BH Covered Services and Other Benefits

The Contractor shall:

1. Authorize, arrange, coordinate, and provide to Covered Individuals all Medically Necessary BH Covered Services listed in **Appendix A-1**, in accordance with the requirements of this Contract, and in an amount, duration, and scope that is no less than the amount, duration, and scope for the same services furnished to Members under MassHealth fee-for-service as set forth in 42 CFR 440.230, and, for Covered Individuals under the age of 21, as set forth in 42 CFR subpart B.

2. Inform Covered Individuals of the MassHealth-established access standards for and the availability of Medically Necessary Behavioral Health Covered Services and how to obtain such services.

3. Incorporate the provisions of 130 CMR 450.204 into all criteria for BH Covered Services.

4. Provide all BH Covered Services that are Medically Necessary, including but not limited to those BH Covered Services that:

   a. Prevent, diagnose, or treat the Covered Individual's disease, condition, and/or disorder that results in health impairments and/or disability;

   b. Assist the Covered Individual to achieve age-appropriate growth and development; and

c. Allow the Covered Individual to attain, maintain, or regain functional capacity.

5. Not arbitrarily deny or reduce the amount, duration, or scope of a required BH Covered Service solely because of diagnosis, type of illness, or condition of the Covered Individual.

6. Coordinate with PCCs and PCACOs to support the provision of other MassHealth covered services included in 130 CMR 450.105 for Covered Individuals.

7. Not be responsible for providing to Covered Individuals or coordinating any Excluded Services as described in **Appendix A-1**.

8. Offer and provide to all Covered Individuals any and all Non-Medical Programs and Services specific to Covered Individuals for which the Contractor has received EOHHS approval.

9. For items or services provided under this Contract, the Contractor shall not cover such services outside the U.S and its territories and shall not provide any payments for such items or services to any entity or financial institution located outside the U.S.

10. Ensure that criminal justice involved Covered Individuals have access to medically necessary BH Covered Services, and Care Management and care coordination as appropriate, as otherwise provided in this Contract.

11. Not impose on a Covered Individual:

    a. An annual dollar limit or an aggregate lifetime dollar limit on Behavioral Health Covered Services; and

    b. Any QTL, as defined in 42 C.F.R. 438.900, on Behavioral Health Covered Services.

12. In accordance with 42 CFR 457.1201(p), not avoid costs of providing BH Covered Services by referring Covered Individuals to publicly supported Behavioral Health care resources.

13. Effective September 23, 2025, develop policies and procedures to pay for annual Behavioral Health Wellness (BH wellness) exams provided to any Covered Individual in any care setting by a licensed mental health professional or PCP, as specified in Managed Care Entity Bulletin 136. The annual BH wellness exam shall identify undiagnosed behavioral or mental health needs and appropriate resources for treatment, in accordance with M.G.L. Ch. 118E, s. 10Q, as added by Chapter 177 of the Acts of 2022. The Contractor shall allow, if appropriate, for additional diagnosis codes on the claim, should a condition be discovered during the exam, as specified in Managed Care Entity Bulletin 136 and any superseding bulletins. Such policies and procedures shall not impose prior authorization on the

annual BH wellness exam, shall not require a member to have pre-existing clinical conditions, and shall not require a provider to conduct a CANS assessment prior to providing the annual BH wellness exam.

B. Services to the Uninsured and Individuals without Mobile Crisis Coverage

1. The Contractor shall provide Individuals without Mobile Crisis Coverage who are experiencing a behavioral health crisis with AMCI/YMCI including follow-up, Community Crisis Stabilization, and up to three units of outpatient CBHC bundle without regard to enrollment with the Contractor.

2. The Contractor shall provide Uninsured Individuals and persons covered by Medicare only who are experiencing a behavioral health crisis with Medically Necessary Behavioral Health crisis services, including AMCI/YMCI including follow-up, Community Crisis Stabilization and up to three units of outpatient CBHC bundle without regard to enrollment with the Contractor.

3. The Contractor shall provide Uninsured Individuals and persons covered by Medicare only with Medically Necessary Behavioral Health initial crisis evaluation services in the emergency department without regard to enrollment with the Contractor.

C. Utilization Management and Authorization of Services

1. General Requirements

a. The Contractor may place appropriate limits on a BH Covered Service based on Medical Necessity, or for the purpose of utilization control, provided that the furnished services can reasonably be expected to achieve their purpose. The Contractor's Medical Necessity guidelines must, at a minimum, be:

1) Developed with input from practicing physicians in the Contractor's Provider Network and experts who are familiar with standards and practices of mental health and substance use treatment for adults, children and adolescents in Massachusetts, including the state substance abuse and mental health authorities (BSAS and DMH);

2) Developed in accordance with standards adopted by national accreditation organizations;

3) Developed in accordance with the definition of Medical Necessity in **Section 1.1** of this Contract and therefore no more restrictive than MassHealth Medical Necessity guidelines, quantitative treatment limitations (QTLs) and non-quantitative treatment limitations (NQTLs);

4) Evidence-based, if practicable; and

5) Applied in a manner that considers the individual health care needs of the Covered Individual, including but not limited to the ongoing need for services of Covered Individuals with ongoing or chronic conditions;

b. The Contractor shall:

1) Submit the proposed Clinical Criteria to EOHHS for review and approval; and

2) Annually review, and update as necessary, the Clinical Criteria and any other clinical protocols that have been developed, and submit any proposed changes to EOHHS for prior review and approval no less than 60 days prior to any change.

2. Service Authorizations, Utilization Review, Clinical Service Coordination, and Clinical Referral

a. UM Policies and Procedures

1) The Contractor shall develop and maintain UM policies and procedures that ensure Covered Individuals receive the care that is Medically Necessary, and that BH Covered Services are not over-utilized or provided without a determination of Medical Necessity. Such policies and procedures shall include but not be limited to service authorizations that are consistent with the EOHHS-approved Clinical Criteria the Contractor has developed, and shall adhere to the requirements set forth in this **Section 2.6**.

2) The Contractor shall:

a) Initially, submit the UM policies and procedures to EOHHS for approval at least one month prior to the Operational Start Date.

b) Participate in any EOHHS efforts to standardize UM policies and procedures across EOHHS and its MassHealth managed care entities and fee-for-service programs, including workgroups, task forces, and meetings related to Utilization Management and best practices, as requested by EOHHS.

c) Annually review, and update as necessary and as directed by EOHHS, the UM policies and procedures and submit any proposed changes to EOHHS for prior review and approval no less than 60 days prior to any change.

b. Standards for Clinicians

The Contractor shall ensure the following standards for clinicians who authorize services, unless otherwise approved by EOHHS:

1) The clinician(s) coordinating services and making service authorization decisions must have training and experience in the specific area of service for which they are coordinating and authorizing services.

2) The clinician(s) coordinating and authorizing services for a Covered Individual with a coexisting medical and BH diagnosis must be a registered nurse, psychiatrist, or other licensed clinician with experience and training in services with a coexisting medical and BH diagnosis.

3) In the event a clinician with experience in the specific area of service is unavailable to authorize a service, appropriate clinical consultation must be provided.

c. Service Authorization Procedures

The Contractor shall process requests for initial and continuing authorizations of services which shall:

1) Require that any decision to deny a service authorization request or to authorize a service in an amount, duration, or scope that is less than requested be made by a board-certified or board-eligible psychiatrist or health care professional who has appropriate expertise addressing the Covered Individual's Behavioral Health needs, except as provided in **Section 2.6.C.2.c.2** below;

2) In cases of denials of services for psychological testing, require that the denials be rendered by a qualified psychologist;

3) Have in effect mechanisms to ensure consistent application of review criteria for authorization decisions;

4) Consult with the requesting Network Provider when appropriate;

5) Make authorization decisions and provide notice as follows:

a) For standard authorization decisions, make a decision and provide notice of any denial or decision to authorize services in an amount, duration, or scope that is less than requested as expeditiously as the Covered Individual's health condition requires and within the following timeframes:

(i) For Outpatient Services, Outpatient Day Services, and non-24-hour Diversionary Services, the Contractor shall make a decision no later than 7 calendar days following receipt of the request, and shall mail a written notice to both the Covered Individuals and the Network Provider on the next business day after the decision is made; or provide an electronic notification if allowed; and

(ii) For Inpatient Services and 24-hour Diversionary Services, the Contractor shall make a decision within 72 hours of the request, notify the Network Provider orally within 72 hours, and notify both the Covered Individual and the Network Provider in writing within three days;

b) For expedited service authorization decisions, where the Network Provider indicates or the Contractor determines that following the standard timeframe in **Section 2.6.C.2.c.5.a** above could seriously jeopardize the Covered Individual's life or health or ability to attain, maintain, or regain maximum function, the Contractor shall make a decision and provide notice as follows:

(i) The Contractor shall make a decision as expeditiously as the Covered Individual's health condition requires and within 72 hours after receipt of the request for service, with a possible extension not to exceed an additional 14 calendar days. Such extension shall be allowed only if:

(a) the Covered Individual or the Network Provider requests an extension; or

(b) the Contractor can justify (to EOHHS upon request) that (a) the extension is in the Covered Individual's interest, and (b) there is a need for additional information where there is a reasonable likelihood that receipt of such information would lead to approval of the request, if received; and such outstanding information is reasonably expected to be received within 14 calendar days.

(ii) The Contractor shall notify the Network Provider orally and notify both the Covered Individual and the Network Provider in writing of any denial or decision to authorize services in an amount, duration, or scope that is less than requested on the day that the decision is made.

6) In accordance with 42 CFR 438.3(i) and 422.208, ensure that compensation to individuals or entities that conduct Utilization Management activities for the Contractor are not structured so as to provide incentives for the individual or entity to deny, limit, or discontinue Medically Necessary services to any Covered Individual.

7) Require the Contractor to conduct monthly reviews of a random sample of no fewer than 50 Covered Individuals per month to ensure that such Covered Individuals received the services for which Network Providers billed with respect to such Covered Individuals.

8) Specify that prior authorization shall not be required for the following services as defined in **Appendix A-1**:

a) Inpatient Substance Use Disorder Services (Level 4);

b) Inpatient Mental Health Services. The Contractor must require hospitals to notify the Contractor of the admission of a Covered Individual for inpatient mental health services and the Covered Individual's initial treatment plan within 72 hours of admission;

c) Community Based Acute Treatment (CBAT) and Intensive Community-Based Acute Treatment (ICBAT). The Contractor must require CBAT and ICBAT programs to notify the Contractor of the admission of a Covered Individual and the Covered Individual's initial treatment plan within 72 hours of admission;

d) Acute Treatment Services (ATS) for Substance Use Disorders (Level 3.7). Medical necessity shall be determined by the treating clinician in consultation with the Covered Individual;

e) Clinical Stabilization Services for Substance Use Disorders (Level 3.5). Medical necessity shall be determined by the

treating clinician in consultation with the Covered Individual;

f) Youth Withdrawal Management and Stabilization Services;

g) Structured Outpatient Addiction Program (SOAP);

h) Intensive Outpatient Program (IOP);

i) Partial Hospitalization (PHP) with short-term day mental health programming available seven days per week;

j) All types of Residential Rehabilitation Services (RRS) (Level 3.1);

k) Youth Community Crisis Stabilization (YCCS);

l) Enhanced Structured Outpatient Addiction Program (ESOAP);

m) All types of Peer Recovery Coach Services; and

n) All types of Recovery Support Navigator Services.

9) Require that Providers providing CSS and ATS shall provide the Contractor, within 48 hours of a Covered Individual's admission, with notification of admission of a Covered Individual and an initial treatment plan for such Covered Individual. The Contractor may establish the manner and method of such notification but may not require the provider to submit any information other than the name of the Covered Individual, information regarding the Covered Individual's coverage with the Contractor, and the provider's initial treatment plan. The Contractor may not use failure to provide such notice as the basis for denying claims for services provided.

10) Specify that concurrent review will not be imposed and coverage for ATS will not be denied based on such review. However, the Contractor may contact providers of ATS to discuss coordination of care, treatment plans, and after care.

11) If utilization management review activities are performed for CSS, specify that such activities may be performed no earlier than day 7 of the provision of such services, including but not limited to discussions about coordination of care and discussions of treatment plans. The Contractor may not make any utilization management review decisions that impose any restriction or deny any future Medically Necessary Clinical Stabilization Services for Substance

Use Disorders (Level 3.5) unless a Covered Individual has received at least 14 consecutive days of Clinical Stabilization Services for Substance Use Disorders (Level 3.5). Any such decisions must follow the requirements regarding Adverse Action notifications to Covered Individuals and clinicians, as specified in **Section 2.12.B.2**, and processes for Internal and BOH Appeals of the Adverse Action, as specified in **Section 2.12.C**.

12) Allow for at least the first 90 days of Residential Rehabilitation Services for a Covered Individual to occur without prior approval, provided however that the Contractor may establish notification or registration procedures during the first 90 days of Residential Rehabilitation Services. The Contractor shall submit for EOHHS's approval the Contractor's authorization and concurrent review procedures for Residential Rehabilitation Services.

13) Contractor may require YCCS providers, within 5 days of a Covered Individual's admission, to notify the Contractor of the admission.

d. Notwithstanding any other provision of this Contract, the Contractor shall not authorize services or treatment plans for services to be rendered after the termination of this Contract without EOHHS's prior review and approval, or unless otherwise directed by EOHHS.

e. The Contractor shall, in a form and format specified by EOHHS, post on its website service authorization metrics and other information in accordance with 42 CFR 438.210(f). Such data may include, but shall not be limited to, information collected in accordance with **Section 2.14.L** and **Appendix E-1**.

3. Clinical Referral and Service Authorization Functions

a. Clinical Referrals Function

To assist Providers and Covered Individuals in identifying Network Providers who can provide BH Covered Services in accordance with this Contract, the Contractor shall operate and maintain a toll-free Clinical Referral Line that is staffed 24 hours a day, seven days a week by, at a minimum, bachelor's-level staff who are trained and knowledgeable about Contractor referral resources and who can make appropriate referral suggestions.

b. Service Authorization Function

1) To authorize delivery of Behavioral Health Covered Services, if appropriate, and to assist Providers and Covered Individuals in

identifying Network Providers who can provide Covered Services in accordance with this Contract, the Contractor shall operate and maintain a toll-free Service Authorization Line that is staffed 24 hours a day, seven days a week by staff with qualifications as described in **Section 2.6.C.2.b**. Such clinical staff shall have access to Covered Individuals' clinical and service authorization information.

2) The Contractor shall ensure that supervisory staff is available to assist staff clinicians with handling calls to the Service Authorization Line.

3) The Contractor may propose for EOHHS review and approval a plan to adopt an alternative to the Service Authorization Line and/or additional method for Network Providers to request and receive authorization for services.

4) The Contractor shall coordinate service authorization functions with the Care Management Program described in **Section 2.5**, as appropriate.

4. Service Authorization for Specific BH Covered Services

a. Inpatient Service Authorization

The Contractor shall develop Inpatient Service authorization policies and procedures that shall include, at a minimum, the following:

1) A plan and system in place to direct Covered Individuals to the least intensive clinically appropriate service;

2) A system for ensuring, to the extent possible permitted by law, prior to admissions for inpatient Behavioral Health services, the admitting Provider will:

(a) Ensure that a behavioral health clinical assessment is completed for the Covered Individual, including a full biopsychosocial, medical necessity assessment and diversionary considerations. This assessment must be completed by a qualified behavioral health professional. For youth under the age of 18 years old, the qualified behavioral health provider must have child-specific expertise or certification;

(b) Document the above assessment in the Covered Individual's medical record; and

(c) Use the above assessment to determine that the admission of the Covered Individual is Medically Necessary.

3) Processes to ensure placement for Covered Individuals who require Behavioral Health Inpatient Services when no inpatient beds are available, as described in **Section 2.5.K**;

4) A system for authorizing and assigning an initial length of stay for all admissions, and communicating information on the assigned length of stay to the Covered Individual, facility and attending physician, as specified in **Section 2.6.C.2.c**;

5) A system for ensuring that Inpatient Services are authorized for 24 hours for all Covered Individuals ordered hospitalized by a judge pursuant to M.G.L. c. 123 § 12(e); and that Inpatient Services for such individuals are authorized for more than 24 hours only if the Contractor determines that such services are Medically Necessary;

6) A system of concurrent review for Inpatient Services to monitor the Medical Necessity of the need for continued stay and achievement of Behavioral Health Inpatient treatment goals;

7) A system for addressing Discharge Planning during initial authorization and concurrent review;

8) A system for conducting retrospective reviews of the medical records of selected inpatient authorizations, to assess the Medical Necessity, clinical appropriateness, and appropriateness of the Level of Care and duration of the stay; and

9) A system for ensuring that the Inpatient Services Network Provider asks for the Covered Individual's consent to notify the Covered Individual's PCP that the Covered Individual has been hospitalized.

b. Diversionary Service Authorization

The Contractor shall develop Diversionary Service authorization policies and procedures that shall include, at a minimum, the following:

1) A system that operates 24 hours a day, seven days a week, for authorizing admissions of Covered Individuals to 24-hour Diversionary Services, utilizing the Contractor's Clinical and Medical Necessity Criteria;

2) A system for making clinically appropriate referrals for children and adolescents in need of Community-Based Acute Treatment Services for Children and Adolescents when such Providers have no available beds;

3) A system for authorizing and assigning an initial length of stay for all admissions to 24-hour Diversionary Services, and communicating information on the assigned length of stay to the Covered Individual, facility and attending physician, as specified in **Section 2.6.C.2.c**;

4) A system for authorizing non-24-hour Diversionary Services based on Medical Necessity Criteria;

5) A system of concurrent review for 24-hour Diversionary Services to monitor justification and appropriateness of the length of stay, need for continued stay, and achievement of treatment goals;

6) A system for addressing Discharge Planning during initial authorization and concurrent review;

7) A system for ensuring that Network Providers of 24-hour Diversionary Services ask for the Covered Individual's consent to notify the Covered Individual's PCP that the Covered Individual has been admitted; and

8) A system for conducting retrospective reviews of the medical records of selected Diversionary Services cases, to assess the Medical Necessity, clinical appropriateness, and appropriateness of Level of Care and duration of the stay.

c. Outpatient Service Authorization

The Contractor shall develop Outpatient Service authorization policies and procedures that shall include, at a minimum, the following:

1) A system that operates 24 hours a day, seven days a week;

2) A policy and system for automatically authorizing at least 12 outpatient sessions per Covered Individual per Contract Year;

3) A policy and system, secure from unauthorized access, for authorizing outpatient sessions beyond 12 sessions;

4) A policy and system for authorizing Outpatient Services and lengths of treatment based on the Contractor's Clinical Criteria;

5) A policy and system for generally informing Network Providers of the Contractor's protocols for approving Outpatient Services, such as including such protocols in the Provider Manual; and

6) A policy and system to ensure that the provision of outpatient BH Services is based on the individual clinical needs of each Covered Individual, and that the BH Covered Service(s) provided are the least intensive clinically appropriate service(s).

5. Assessment, Treatment Planning and Discharge Planning

a. Assessments

The Contractor shall:

1) Ensure that all Network Providers prepare an individualized written assessment for any Covered Individual entering treatment, regardless of treatment setting.

2) Ensure that assessments are conducted by Network Providers and include but are not limited to:

a) history of presenting problem;

b) chief complaints and symptoms;

c) past BH history;

d) past medical history, including but not limited to Primary Care, specialty care, treatment for chronic conditions, and use of prescription drugs;

e) the Covered Individual's family history, social history and linguistic and cultural background, with an assessment of the Covered Individual's identified supports in each of these domains;

f) for Children in the Care and/or Custody of the Commonwealth, history of placements outside the home;

g) current or previous substance use;

h) mental status exam including assessment of suicide and violence risk using industry recognized evidence-based tools (e.g., CSSRS);

i) current or historical service in the military and/or family of a service member;

j) current or historical exposure to violence including domestic violence

k) current or historical exposure to trauma;

l) previous medication trials, current medications and any allergies;

m) diagnosis, clinical formulation, rationale for treatment, and recommendations;

n) level of functioning;

o) the Covered Individual's strengths and, for children and adolescents, family strengths;

p) name of PCP and other key Providers; and

q) the Covered Individual's housing status, including if the Covered Individual is homeless or at risk of homelessness.

3) Ensure that when assessments are completed, a multidisciplinary treatment team has been assigned to each Covered Individual. The multidisciplinary treatment team shall, with consent from the Covered Individual, include the following Providers and community supports, as appropriate for the Covered Individual's clinical needs: the PCP current community-based BH Network Providers, other specialists, state agency case managers and/or service providers, Peer Supports identified by the Covered Individual, and others recommended by a team member or requested by the Covered Individual. For children under 18, a parent or legal guardian must be an active participant in the team. The treatment team shall meet to review the assessment and initial treatment plan within the following time frames:

a) For Inpatient Services: within 24 hours of admission;

b) For Diversionary Services: within 48 hours of admission; and

c) For Outpatient Services, for clinics, group practices and solo practitioners, the timeline specified in DPH regulation 105 CMR 140.540.

4) Make best efforts to ensure that the assessments are conducted by Network Providers who have training and experience that match the Covered Individual's clinical needs based on the Covered Individual's presenting problem(s) and diagnosis.

5) Require the clinicians who provide Behavioral Health services described in **Section 2.7.5** to use the CANS Tool and the information gathered from its use to inform treatment planning and Discharge Planning when: providing initial Behavioral Health Clinical Assessments; as part of the Discharge Planning process from Inpatient Psychiatric Hospitalizations, and Community-Based Acute Treatment Services; and, at a minimum, every 180 days during treatment provided to Covered Individuals who are under age 21.

b. Treatment Planning

The Contractor shall ensure that its Network Providers:

1) Utilize the individualized written assessment, including the clinical formulation, to develop a treatment plan;

2) Develop initial treatment plans that are in writing, dated and signed, and include, at a minimum:

a) a description of all services needed during the course of treatment;

b) goals, expected outcomes and time frames for achieving the goals;

c) indication of the strengths of the individual and his/her family as identified in the assessment;

d) links to Primary Care and specialty care, especially when there is an active co-occurring medical condition;

e) when appropriate, the plan to involve a case manager from a state agency, such as DCF, DMH, DYS or DDS; and

f) treatment recommendations consistent with the service plan of the relevant state agency for Covered Individuals who are also DMH Clients, Children in the Care and/or Custody of the Commonwealth, DYS youth, or DDS clients.

3) Periodically review initial treatment plans and modify them as necessary;

4) Receive Covered Individual medical and pharmaceutical profiles on a regular basis and use these profiles as part of its periodic review of the Covered Individual's treatment plan;

5) Invite and encourage the following persons to participate in the development and modification of the Covered Individual's

treatment plan, the treatment itself, and to attend all treatment plan meetings:

a) In the case of an individual over age 16 or an emancipated minor, the Covered Individual, the Covered Individual's family members, guardians, the PCP, Network Providers of BH Outpatient Services, key specialists and other identified supports, but only when the consent of the Covered Individual to such involvement(s) has been obtained, unless the individual has a legal guardian, in which case the consent of the legal guardian is required.

b) In the case of an individual under age 16 who is not an emancipated minor, with the consent of a parent or guardian, the Covered Individual, if appropriate, family members, the PCP, Network Providers of BH Outpatient Services, Family Partners, Care Coordinators, key specialists, and other identified supports.

c) For Covered Individuals who are also DMH Clients, DYS-involved youth, DDS clients or Children in the Care and/or Custody of the Commonwealth, the designated staff from the relevant state agencies.

d) For Covered Individuals who are participating in Care Management through the Contract, the Contractor's assigned care manager.

6) Make best efforts to schedule treatment planning meetings concerning children and adolescents at a time when their family members or guardians are available;

7) Encourage Covered Individuals over the age of 18 to consent to the participation of guardians and family members in the treatment and treatment planning;

8) Assign a multidisciplinary treatment team to each Covered Individual within 24 hours of admission for Inpatient Services or for 24-hour Diversionary Services.

c. Discharge Planning

The Contractor shall:

1) Ensure that all Network Providers, especially Network Providers of Inpatient and Diversionary Services, upon admission of Covered Individuals:

a) assign appropriate designated staff who are knowledgeable about the continuum of coordinated BH and medical services, services and supports in the community, and Discharge Planning;

b) provide notice to the Covered Individual's PCP within one business day of the admission, include the PCP in current Discharge Planning efforts and schedule a follow-up appointment with the PCP for care, as appropriate;

c) coordinate and collaborate with the Contractor's care manager if the Covered Individual is participating in Care Management under the Contractor;

d) make best efforts to ensure a smooth transition to the next service, if any, or to the community;

e) document all efforts related to these activities, including the Covered Individual's active participation in his or her individualized Discharge Planning and, in the case of Covered Individuals under 18, their parent or legal guardian; and

f) Identify Barriers to aftercare and develop strategies to assist Covered Individuals with aftercare services.

2) Develop, in collaboration with each Covered Individual, prior to the individual's discharge from any Inpatient BH Service or, if appropriate, any other BH Covered Service, a written, individualized person-centered, strength-based discharge plan for the next service or program, anticipating the individual's movement along a continuum of services, including availability of Wraparound services for children under 18 and their families;

3) Include in the discharge plan, at a minimum:

a) Identification of the individual's needs, including but not limited to:

(i) housing;

(ii) finances;

(iii) medical care;

(iv) transportation;

(v) family, employment, and educational concerns;

(vi) natural community and social supports; and

(vii) a Crisis Prevention Plan that follows the principles of recovery and resilience, and which may be a component of a Wellness, Recovery Action Plan (WRAP) model for adults and the Risk, Management, Safety Plan for children and their families.

b) A list of the services and supports that are recommended post-discharge;

c) Identified Providers, PCPs and other community resources available to deliver each recommended service;

d) A list of prescribed medication, dosages and possible side effects; and

e) Treatment recommendations consistent with the service plan of the relevant state agency for Covered Individuals who are also DMH Clients, DCF and DYS Youth in the Care and/or Custody of the Commonwealth, or DDS clients.

4) Invite and encourage the following persons to participate in Discharge Planning meetings:

a) In the case of an individual over age 16 or an emancipated minor, the Covered Individual, the Covered Individual's family members, guardians, PCP, Network Providers of BH Outpatient Services, key specialists, and other identified supports, but only when the consent of the individual to such involvement(s) has been obtained, unless the individual has a legal guardian, in which case consent of the legal guardian is required;

b) In the case of an individual under age 16 who is not an emancipated minor, with the consent of a parent or guardian, the Covered Individual, if appropriate, family members, PCP, Network Providers of BH Outpatient Services, key specialists and other identified supports;

c) For Covered Individuals who are also DMH Clients, DCF and DYS Youth in the Care and/or Custody of the Commonwealth, or DDS clients, designated staff from the relevant state agencies; and

d) For Covered Individuals enrolled in a PCACO, the Covered Individual's CP, care coordinator, and/or clinical care manager, as applicable;

e) For Covered Individuals receiving Care Management services through the Contractor, the Contractor's assigned care manager.

5) Schedule Discharge Planning meetings concerning children and adolescents at a time when their family members or guardians are available;

6) Develop linkages and policies that create a smooth, clinically sound transition of a Covered Individual's care from one service setting or BH Covered Service to the next, including transition to services provided by state agencies;

7) Assist Covered Individuals in obtaining post-discharge appointments as follows: within seven calendar days of discharge for aftercare services, which may include Outpatient Services as well as a broader range of BH Covered Services, including Non-24-Hour Diversionary Services such as partial hospital programs, if necessary; and within 14 calendar days of discharge for Medication Monitoring, if necessary;

8) Require the treatment team staff responsible for implementing the individual's discharge plan to document the discharge plan in the medical record;

9) Ensure that Network Providers of 24-hour Levels of Care furnish, with appropriate consent, written discharge instructions to the Covered Individual, parents, guardians, residential providers, PCPs, PCACOs, CPs, and relevant state agencies or Contractor care managers at the time of the individual's discharge, to include, without limitation:

a) a list of prescribed medications and information about any potential medication side effects;

b) aftercare appointments;

c) recommended behavior management techniques when applicable; and

d) a Crisis Prevention Plan, including the toll-free phone number or contact information for the Covered Individual's local CBHC.

10) Ensure that Network Providers of 24-hour Levels of Care furnish, with appropriate consent, a written discharge summary to the Covered Individual, parents, guardians, PCPs, CPs, Contractor care managers, and the Member's current Behavioral Health Providers within two weeks of discharge, to include a summary of:

a) the course of treatment;

b) the Member's progress;

c) the treatment interventions and behavior management techniques that were effective in supporting the Member's progress;

d) medications prescribed; and

e) treatment recommendations.

11) Ensure that the discharge plans for Covered Individuals who are DMH Clients are coordinated with the DMH Area or Site Office.

d. Additional Discharge Planning Requirements for Homeless Covered Individuals

The Contractor shall:

1) Strongly discourage Network Providers from discharging Homeless Covered Individuals to shelters;

2) Ensure that all Network Providers provide comprehensive Discharge Planning for Homeless Covered Individuals, and that Network Providers exhaust all potential avenues to secure placement or housing resources, with assistance from the Contractor;

3) Ensure that, within two business days of admission, all Network Providers complete and forward to DMH a DMH Service Authorization packet for Homeless Covered Individuals who appear to meet DMH clinical criteria for service eligibility;

4) Identify community resources for the Homeless Covered Individual and ensure that Network Providers are aware of and utilize all such resources to assist with Discharge Planning for Homeless Covered Individuals;

5) Collaborate with DMH to ensure that Network Providers are aware of and utilize all available DMH resources to assist with Discharge Planning for Homeless Covered Individuals; and

6) Maintain and periodically update website links to Homeless services resources on the Contractor's website to assist Network Providers with Discharge Planning for Homeless Enrollees.

e. Additional Discharge Planning Requirements for Covered Individuals experiencing or at risk of homelessness

The Contractor shall:

1) Ensure that Providers notify the Contractor at the time of admission of a Covered Individual experiencing or at risk of homelessness.

2) Require that, at the time of admission and as part of its general discharge planning processes, each Network Provider assess each admitted Covered Individual's current housing situation. At a minimum, the network provider must assess whether such Covered Individual is experiencing or is at risk of homelessness. To aid in this assessment, network providers must ensure that their discharge planning staff screen admission data, including but not limited to age, diagnosis, and housing status, within 24 hours of admission. For any Covered Individual determined by the network provider to be experiencing or at risk of homelessness, the network provider must commence discharge planning activities no later than three calendar days after the Covered Individual's admission unless otherwise required to commence such activities at an earlier time following admission.

3) Require that, to assist in the discharge planning process for each Covered Individual experiencing homelessness or at risk of homelessness, the Network Provider, to the extent consistent with all applicable federal and state privacy laws and regulations, invite and encourage the following persons to participate in such Covered Individual's discharge planning activities: the Covered Individual; the Covered Individual's family members; guardians; primary care providers; Behavioral Health providers; key specialists; case managers or other representatives; emergency shelter outreach or case management staff; care coordinators; and any other supports identified by the Covered Individual. For any such Covered Individual who is a client of the Department of Mental Health (DMH), the Department of Developmental Services (DDS), or the Massachusetts Rehabilitation Commission (MRC), the network provider must, to the extent consistent with all applicable federal and state privacy laws and regulations, invite and encourage

designated staff from each such agency to participate in such Covered Individual's discharge planning activities.

4) Require the Network Provider to determine whether any non-DMH-, non-DDS-, or non-MRC-involved Covered Individual experiencing or at risk of homelessness may be eligible to receive services from some or all of those agencies. For any such Covered Individual, the Network Provider must, within two business days of admission, and to the extent consistent with all applicable federal and state privacy laws and regulations, offer to assist the Covered Individual with completing and submitting an application to receive services from DMH, DDS, or MRC, as appropriate.

5) Require that the Network Provider to determine whether any Covered Individual experiencing or at risk of homelessness has any substance use disorder (SUD). For any such Covered Individual, the Network Provider must contact the Massachusetts Substance Use Helpline (800) 327-5050), the statewide, public resource for finding substance use treatment, recovery options, and assistance with problem gambling, or successor Helplines as identified by EOHHS. The Helpline's trained specialists will help the Covered Individual understand the available treatment services and their options.

6) Require that for any Covered Individual experiencing homelessness who is expected to remain in the Network Provider's facility for fewer than 14 days, the Network Provider contact:

   a) The emergency shelter in which the Covered Individual most recently resided, if known, to discuss the Covered Individual's housing options post discharge; or

   b) The local emergency shelter to discuss the Covered Individual's housing options post discharge if the Covered Individual has not resided in an emergency shelter or if the emergency shelter in which the Covered Individual most recently resided is unknown.

7) Ensure that Providers assess options for discharge as follows:

   a) Network Providers must ensure that their discharge planning staff are aware of and utilize available community resources to assist with discharge planning for Covered Individuals experiencing homelessness or at risk of homelessness;

b) Network Providers must make all reasonable efforts to prevent discharges to emergency shelters and/or the street of Covered Individuals who have skilled care needs, Covered Individuals who need assistance with activities of daily living, and Covered Individuals whose Behavioral Health condition would impact the health and safety of individuals residing in the shelter. For such Covered Individuals, Network Providers should seek placement in more appropriate settings including DMH community-based programs or skilled nursing facilities;

c) For certain Covered Individuals, discharge to an emergency shelter or the streets may be unavoidable. For example, certain Covered Individuals may choose to return to the streets or go to an emergency shelter despite the best efforts of the Network Provider. For these Covered Individuals, the Network Provider shall:

(i) Discharge the Covered Individual only during daytime hours;

(ii) Provide the Covered Individual a meal prior to discharge;

(iii) Ensure that the Covered Individual is wearing weather appropriate clothing and footwear;

(iv) Provide the Covered Individual a physical copy of their health insurance information;

(v) To the extent clinically appropriate and consistent with all applicable laws and regulations, provide the Covered Individual with a written copy of all prescriptions and at least one week's worth of filled prescription medications;

(vi) If the Covered Individual is to be discharged to an emergency shelter:

(a) Provide at least 24 hours advance notice to the shelter prior to discharge;

(b) Provide the Covered Individual with access to paid transportation to the emergency shelter;

(c) Ensure that the shelter has an available bed for the Covered Individual. In the event that

a shelter bed is unavailable on the planned discharge date, but a bed will be available soon, the network provider should delay discharge until a bed is available. In these cases, the hospital may bill the Contractor at the Administratively Necessary Day (AND) rate for each such day on which the Covered Individual remains in the network provider facility.

8) Ensure that Providers adhere to the following discharge planning tracking and reporting activities:

a) Network Providers must document in each Covered Individual's medical record all efforts related to the discharge planning activities described above, including options presented to the Covered Individual and, if applicable, the Covered Individual's refusal of any alternatives to discharge to the streets or emergency shelters.

b) Network Providers must track discharges of Covered Individuals to local emergency shelters or the streets in a form, format, and cadence to be specified by EOHHS.

9) Notify the Contractor at the time of admission of a Covered Individual experiencing or at risk of homelessness.

6. Utilization Management Services for Review of Services to Additional Populations

a. At the direction of and as further specified by EOHHS, the Contractor shall provide utilization management services to EOHHS to assist in the review and management of services to additional populations, including Members enrolled in MassHealth's fee-for-service program and all MassHealth Members receiving services through court-ordered SUD treatment programs as defined in M.G.L. Chapter 123, Section 35.

b. The Contractor shall work collaboratively with EOHHS to develop utilization management strategies and policies, as further specified by EOHHS.

D. Clinical and Other Support Services

1. Pharmacy Support Services

a. General Requirements

The Contractor shall:

1) As directed by EOHHS, support the initiatives of the MassHealth Pharmacy Program, which manages the pharmacy benefit for PCC Plan Enrollees and other Covered Individuals served under this Contract;

2) Establish and maintain the capability to receive and analyze Claims data received from the EOHHS Data Warehouse for all Covered Services, including pharmacy utilization data for all Covered Individuals;

3) Establish a process to ensure that the Contractor determines the need for care management or care coordination for those individuals who are referred to the Contractor by the MassHealth Drug Utilization Review (DUR) and Pharmacy Program. If the Contractor is unable to reach a Covered Individual, or the Covered Individual declines to participate, the Contractor shall follow up with the Covered Individual's PCC or prescriber to ensure coordinated care;

4) Ensure that sufficient clinical staff with an understanding of medications(s) and data analytic staff are available to fulfill the pharmacy requirements of the Contract. The Contractor shall have access to a pharmacist on an episodic basis if needed to assist with pharmacy-related projects;

5) Coordinate pharmacy support activities in collaboration with the MassHealth's DUR, and as directed by EOHHS with DMH;

6) The Contractor shall submit the Pharmacy Quarterly Activities Report to MassHealth on the pharmacy-related activities the Contractor has performed in support of this Contract as specified in **Appendix E-1**. This report shall include but not be limited to the following categories of activities:

    a) A summary report of the number of Covered Individuals in each Pharmacy Program initiative that DUR or Office of Clinical Affairs (OCA) staff have referred to the Contractor's Care Management Program and the results of the referral;

    b) Pediatric Behavioral Health Medication Initiative (PBHMI); and

    c) Any other initiatives currently being worked on.

7) For the purposes of this Section, provide Covered Individual-level information described herein only to Providers who have a record of treating the Covered Individual, or otherwise as directed by EOHHS and consistent with all applicable laws and regulations.

b. Pharmacy Initiatives

The Contractor shall support and collaborate with EOHHS on pharmacy activities and efforts, including but not limited to:

1) Using Covered Individuals' drug utilization data obtained from EOHHS to inform and guide prescribing activity, and to improve collaboration by prescribers.

2) Using criteria developed in collaboration with and agreed to by EOHHS, identifying Covered Individuals under the age of 18 on antipsychotic medication who need metabolic monitoring (diabetes and lipid screening test) and notifying both the Covered Individual's prescribing clinician and the PCC, and as further directed by EOHHS, the Covered Individual's Primary Care ACO, in a form and format and at a frequency specified by EOHHS.

3) At the direction of EOHHS, supporting EOHHS pharmacy initiatives by:

a) Promoting the adoption of MassHealth clinical policy recommendations to PCC Plan Providers, Network Providers and Primary Care ACOs as applicable.

b) Educating PCC Plan Providers and Network Providers regarding the need to coordinate and manage prescribed medication use for BH and medical conditions through an alert, brochure or newsletter.

4) Using criteria developed in collaboration with and agreed to by EOHHS, develop a program to identify prescribers serving Covered Individuals who are currently in the acute stage of opioid therapy and at risk for continued opioid utilization and to develop an early intervention strategy to be used with the identified prescribers.

5) All existing and proposed projects (including all data reports, template letters and notifications) will be reviewed by the Contractor's clinical staff prior to submission to EOHHS. All projects that are implemented need to include an annual QA process to ensure operational soundness and evaluate outcomes.

c. Work Group Participation

1) The Contractor shall assign a pharmacist or other clinician to participate in all appropriate pharmacy work groups as determined necessary by EOHHS, including but not limited to:

a) The DUR Board as well as open DUR workgroups and committees. In the interest of having a multi-disciplinary board, EOHHS prefers that the Contractor sends a Care Manager to these meetings;

b) The Pharmacy Director Meeting Workgroup; and

c) The Pharmacy Advisory Committee Workgroup.

2) The Contractor shall participate in any EOHHS pharmacy strategic planning processes as directed by EOHHS.

d. Obligations of the Contractor to Support Rebate Collection

The Contractor shall take all steps necessary to participate in, and support EOHHS' participation in, federal and supplemental drug rebate programs as directed by EOHHS and as follows:

1) The Contractor shall ensure EOHHS obtains all drug utilization data in accordance with the requirements set forth by EOHHS. The Contractor shall participate and cooperate with EOHHS in activities meant to assist EOHHS with identifying and appropriately including eligible drug claims in the federal drug rebate program.

2) The Contractor shall perform all system and program activities determined necessary to:

a) Collect all of the following information on claims for physician-administered drugs billed separately using a Healthcare Common Procedure Coding System (HCPCS) by Opioid Treatment Programs, and deny any claim for such drugs that does not include all such information:

(i) All information set forth in 42 CFR 447.511 that EOHHS specifies the Contractor needs to provide, including but not limited to National Drug Code (NDC);

(ii) Metric Quantity; and

(iii) NDC Unit of Measure.

b) Validate that all National Drug Codes (NDCs) submitted on physician- administered drugs for rebate match the HCPCS being billed for, and include accurate NDC information (unit of measure and quantity);

c) Properly identify drugs purchased through the Federal 340B Drug Pricing Program by adding the identifier of "UD" to the HCPCS and include this information in the Encounter data;

3) The Contractor shall take all steps necessary, as determined by EOHHS, to enable EOHHS to maximize rebate collection. Such steps shall include:

a) Requiring Opioid Treatment Programs to use the preferred products listed on the MassHealth Drug List or as otherwise specified by EOHHS, and changing such designation as directed by EOHHS;

b) Signing up to receive notifications from EOHHS of changes to the MassHealth drug list;

c) Collecting, managing, and reporting this information in Encounter Data as described in this Section and as further specified by EOHHS in **Section 2.14.E** and **Appendix D-1 and D-2**; and future updates to Encounter Data formats as may be issued by EOHHS; and

d) Taking any other steps that are necessary for EOHHS to maximize rebate collection.

e. The Contractor shall provide outpatient drugs pursuant to this Section in accordance with Section 1927 of the Social Security Act and 42 CFR 438.3(s), including but not limited to complying with all applicable requirements related to coverage, drug utilization data, drug utilization review program activities and prior authorization policies.

2. Massachusetts Child Psychiatry Access Program

The Massachusetts Child Psychiatry Access Program (MCPAP) consists of five psychiatric and behavioral consultation programs. Two programs are part of this Contract, and three are part of the companion contract for DMH Specialty Programs. It is expected that any MCPAP specialty programs covered under this Contract will be delivered seamlessly and contractual oversight will be conducted in close collaboration with DMH for those MCPAP programs covered under the 24/7 BH Help Line and DMH Specialty Service Model Contract. The two programs under this Contract include Early Childhood (EC), a psychiatric and

Behavioral Health consultation with a sole focus on children age 0 to 5 (for the purpose of the MCPAP Program 0-5 means from birth through age 5) and ASD-ID for MCPAP, which consists of a Behavioral Team and a Statewide Physician Consult Team that help AMCI and YMCI Providers and EDs effectively manage Behavioral Health crises in children and young adults up to age 26 with diagnosed or presumed ASD-ID. Through consultation and education, ASD-ID for MCPAP improves AMCI, YMCI, and ED providers and pediatric primary care providers' competencies in behavioral assessment and intervention, parent coaching, and in making effective referrals for patients who need community-based services and provides access to pharmacological consultation on an emergency basis.

The Contractor shall:

a. Maintain a network of ASD-ID for MCPAP providers to provide crisis consultation to AMCI/YMCI providers, emergency department providers and pediatric primary care providers treating children and young adults with ASD-ID.

b. Maintain ASD-ID for MCPAP teams with optimal staffing patterns to ensure effective team functioning and quality services. The team structure of ASD-ID for MCPAP, including FTE allocations for ASD-ID for MCPAP Behavioral Teams and Statewide Physician Consult Team, must be approved by EOHHS.

c. Ensure that ASD-ID for MCPAP services are available statewide.

d. In collaboration with EOHHS, develop, implement, and maintain a continuous quality improvement system capable of systematically collecting and analyzing data and information to ensure ASD-ID for MCPAP services are high quality, efficient, and meeting the needs of providers. This CQI system must include the following elements:

    1) Information systems that collect reliable and accurate data;

    2) Clearly defined quality indicators, metrics, and benchmarks that are guided by a logic model;

    3) Rigorous methods for collecting both quantitative and qualitative data;

    4) Analysis of quality data to inform programmatic improvements; and

    5) Timely reports that have up to date information for quality improvement. This includes both routine monthly, quarterly, and annual reports as well as ad hoc reports which respond to a targeted need as requested by EOHHS.

e. Contract with a sufficient number of ASD-ID for MCPAP Behavioral Team and ASD-ID for MCPAP Statewide Physician Consult Team providers to ensure continuous access for AMCI, YMCI, ED and pediatric primary care providers between 11:00 a.m. to 7:00 p.m., Monday through Saturday, (excluding holidays) including the following:"

1) Immediate advice from the ASD-ID for MCPAP Behavioral Team within 30 minutes of the contact or within the time requested by the AMCI, YMCI or ED provider. Ninety-five percent (95%) of all calls to ASD-ID for MCPAP Behavioral Team should be responded to within this time frame.

2) Immediate advice from the ASD-ID for MCPAP Statewide Physician Consult Team within 30 minutes of the contact or within the time requested by the ASD-ID for MCPAP Behavioral Team. Ninety-five percent (95%) of all calls to ASD-ID for MCPAP Statewide Physician Consult Team should be responded to within this time frame.

3) ASD-ID for MCPAP Behavioral Team available to provide behavioral intervention consultation, including Applied Behavior Analysis (ABA) to the YMCI provider that is providing 7-day follow up to member.

4) ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team available to coordinate follow up activities with the AMCI or YMCI provider that is providing 7-day follow up to member.

5) Schedule a patient face-to-face or telehealth assessment with an ASD-ID for MCPAP Statewide Physician Consult Team provider within 5 business days of the referral date or schedule a face to face or telehealth assessment with an ASD-ID for MCPAP Behavioral Team LABA within 1 business day of the referral date. To assess these standards for timely face-to-face or telehealth assessments, on a monthly basis, the Contractor shall contact the ASD-ID for MCPAP Behavioral Teams and Statewide Physician Consult Teams to receive the prospective wait time for the first available and second available appointment dates from the date of the Contractor's contact with the Teams.

6) Submit to EOHHS and implement a quality improvement plan that describes root causes and identifies corrective action steps by the 30th of the month following the quarter if either of the following occurs:

a) If response time for an ASD-ID for MCPAP Behavioral Team is lower than 95% consistently for a quarter;

b) If response time for ASD-ID for MCPAP Statewide Physician Consult Team is lower than 95% consistently for a quarter.

f. Perform the following ongoing responsibilities, without limitation:

1) Collect Encounter data pursuant to the Contractor's requirements;

2) Conduct outreach to recruit, enroll, and build relationships with AMCIs, YMCIs and ED providers;

3) Inform AMCIs, YMCIs and ED providers in a MCPAP Team's region how to access MCPAP services;

4) Annually survey AMCIs, YMCIs and ED providers regarding satisfaction with MCPAP;

5) Maintain program-specific dedicated websites about the ASD-ID for MCPAP that provide information about the program and information about Behavioral Health topics and resources;

6) Conduct outreach and trainings for AMCI, YMCI, and ED providers and other Behavioral Health first responders to develop their knowledge and skills to treat youth and adults with ASD-ID.

7) Create public awareness campaign about the availability of the ASD-ID for MCPAP service for families of individuals with ASD-ID, staff at Autism Support Centers, pediatric providers, parent resource groups, and other stakeholders as directed by EOHHS.

g. Submit ASD-ID for MCPAP monthly, quarterly, and annual aggregate progress reports to EOHHS identified in and according to the reporting schedule in **Appendix E-1**.

h. Submit annual itemized budgets for the ASD-ID Program by December 31st of each calendar year, and whenever there is a change in the budget.

i. Coordinate all ASD-ID for MCPAP program activities with EOHHS, including but not limited to:

1) Revising program activities as requested by EOHHS and approved by EOHHS; and

2) Participating in any EOHHS-initiated program evaluation activities and accompanied recommendations for future direction.

j. [Reserved]

k. Establish and maintain an Early Childhood (EC) MCPAP team to increase availability of supports and access to treatment for children aged 0 through 5 with Behavioral Health needs and their families. The team will include:

1) The Medical Director, at 0.15 FTE, who will provide supervision to the Early Childhood Mental Health Clinician and Child Psychiatrist. In partnership with DPH, she will develop educational materials and curriculum focused on early childhood mental health and secondary prevention for the ECHO (a professional development model that combines didactic training, case presentation by a participant with feedback and resources provided by the participants and faculty) training and case consultation model to be piloted with pediatric PCPs, and to be used to expand the model to all MCPAP regions.

2) A Child Psychiatrist, at 0.1 FTE, will provide evaluation, using the multi-axial Diagnostic Classification of Mental Health and Developmental Disorders of Infancy and Early Childhood (DC: 0-5), and short-term treatment of children 3-5 years old referred for medication management consideration.

3) A licensed Behavioral Health Clinician with expertise/training in early childhood mental health, at 1.0 FTE, who will respond to phone queues from pediatric PCP referred for phone consultation. This position will provide evaluation, using the multi-axial Diagnostic Classification of Mental Health and Developmental Disorders of Infancy and Early Childhood DC:0-5. The clinician will also provide on an as needed basis short-term treatment of children 0-5 years old (up to age 6) referred for behavioral assessment and management, as well as resource and referral services.

4) A Program Coordinator, at 0.5 FTE, who will respond to phone calls and messages, initiate queues, and manage scheduling. This position will also support coordination of ECHO, a professional development model that combines didactic training, case presentation by a participant with feedback and resources provided by the participants and faculty.

5) An ASD Assessor, at 0.5 FTE, to support PCPs to appropriately diagnose young children with less complex diagnoses, based on assessment reports and other documentation from MCPAP and other collateral partners, and their own medical rule outs. The ASD Assessor will partner with the EC MCPAP team to refine and implement protocols for working with the clinical team; receive

referrals to the service through PCPs; conduct assessments using a screening tool to be determined by EOHHS; and work with the EC MCPAP team, family members, and PCP to share information to support diagnosis and referral to treatment. The ASD Assessor will provide assessment services and consultation in Central/Western Massachusetts. In the event of delays in hiring the ASD Assessor role, unspent funds may be used to support consultant time from Pediatric ASD diagnostic process experts to consult on development of protocols.

l. Oversee the building of the EC MCPAP Team which will be housed and administered in the MCPA Central Hubs. The EC MCPAP services area will include the Central and Western hubs.

m. Provide expanded EC MCPAP telehealth consultation to pediatric Primary Care Practitioners (PCPs), including Primary Care Clinicians (PCCs), treating pediatric Members who may need Behavioral Health services with an initial focus on practices in MCPAP Central and Western hubs. Consultation shall include:

1) An assessment of Behavioral Health needs of children ages 0-5 years for enrolled providers within the Central and Western hubs as specified above. This assessment shall include:

a) Revision of the MCPAP annual survey to providers to add additional questions specific to critical needs of children 0-5 years old with Behavioral Health needs as well as their preferred mechanism for receiving consultation, including any post-pandemic changes; and

b) Specific outreach to providers in the Western and Central hubs to participate in two ECHO programs: one on Early Childhood Behavioral Health and one on the Pyramid in Primary Care, which will be developed with content adapted from the national Pyramid Model for Promoting Social Emotional Competence in Infants and Young Children.

2) Development and implementation of communication process for Pediatric Primary Care Providers (PPCPs) and other stakeholders, utilizing MCPAP's websites, webinars and other communication channels;

3) Adoption of practices to ensure family support and racial health equity with guidance from DPH; and

4) Provision of EC MCPAP telehealth consultation, assessment, referrals, and brief treatment using DC:0-5 assessment of children 0-5 years old.

n. Develop and implement EC MCPAP training, as follows:

1) Develop curriculum, do outreach and recruitment, enroll providers, and implement ECHO virtual clinics for pediatric and other providers; include DPH Early Childhood Systems Coordinator for Family Engagement and Training in planning and implementation;

2) Work with DPH on the creation and implementation of the Pyramid in Primary Care (PiPC) modules, and family engagement training using the ECHO approach and learning communities for integrated primary care teams to support outreach and recruitment of integrated care teams;

3) Work with DPH and family leaders to support development and dissemination of the PiPC Toolkit;

4) Partner with DPH to develop and implement training or webinars on additional topics in response to the annual training needs assessments; and

5) Work with DPH to ensure family voice and a racial equity lens in all online or in-person trainings, including having a person with lived experience as a co-presenter or responder in all training programs.

o. Enhance and expand EC MCPAP referral network and community-based resources, as follows:

1) Coordinate with DPH and partners to expand referral network of early childhood mental health (ECMH) clinicians trained in Evidence Based Treatment models (EBTs) (including DC:0-5); and

2) Expand referral network and listings for IECMH services and other community resources, including Pyramid Model sites and family support resources and groups by coordinating with DPH and partners.

3) The EC MCPAP team will base implementation plans on feedback from the project's Advisory Committee, including qualifications for the ASD Assessor and selection of assessment tool. The ASD Assessor and EC MCPAP team will develop workflows for outreach and referral, assessment, collaboration with collateral

providers, consultation to pediatricians to support diagnosis by pediatricians, and coordinated support to families. The EC MCPAP team will develop and implement approaches to educate PCPs, families, and collaterals about the ASD assessment project and process. The EC MCPAP team will evaluate the ASD assessment efforts, standardize protocols, and determine a plan to sustain and possibly scale the ASD assessment to other regions. The EC MCPAP team will track and report data on these activities to DPH and through DPH, to HRSA.

4) Enhance Autism Spectrum Disorder (ASD) assessment of children under age 6, by including an ASD Assessor at 0.5 FTE on the EC-MCPAP team in Central/Western Massachusetts. The ASD Assessor shall:

a) Support PCPs to appropriately diagnose young children with less complex diagnoses, based on assessment reports and other documentation from MCPAP and other collateral partners, and their own medical rule outs;

b) Conduct assessments using a screening tool to be determined by EOHHS in collaboration with the EC-MCPAP team;

c) As part of the EC-MCPAP team, develop protocols for working with the member's clinical team, ASD consultant, family members, and PCP to share information to support diagnosis and referral to treatment;

d) With the EC-MCPAP team, develop workflows for outreach and referrals; assessment; collaboration with collateral providers; and consultation to pediatricians, to support diagnosis by pediatricians and to coordinate support to families; and

e) With the EC-MCPAP team, evaluate the ASD assessment efforts, standardize protocols, and develop plans to sustain and possibly scale the ASD assessment to other regions.

p. Promote equitable access for children ages 0-5 to EC MCPAP and the IECMH system of care as follows:

1) Build linkage with MCPAP for Moms and other perinatal providers for referrals of infants to EC MCPAP and for training on IECMH;

2) Build capacity of other MCPAP hubs through consultation and training by EC MCPAP and regional PCP champions, focusing on underserved areas; and

3) Increase amount and effectiveness of data collection on race and ethnicity and use of this data in CQI efforts (including use of DPH Racial Equity Data Roadmap), including:

a) Continue CQI project on collecting patient race and ethnicity data; and

b) Track education/training data, including registration, on race and ethnicity of enrolled providers in attendance;

q. Sustain, and integrate EC MCPAP with the early childhood system of care and expand program statewide, as follows:

1) Conduct regular assessment of EC MCPAP capacity to serve, including an annual report with a plan for sustainability;

2) Participate in IEMCH Policy Workgroup, Young Children's Council, and other efforts;

3) Align EC MCPAP with other MCPAP programs; and

4) Disseminate information about the project with DPH at conferences and through publications.

r. As directed by DPH and in conjunction with EOHHS, coordinate with and report to DPH on all EC program activities, including but not limited to:

1) Participating in regular planning meetings and other meetings as required by DPH and project activities;

2) Utilizing feedback from Young Children's Council, the EC MCPAP Advisory Committee, to inform and advise MCPAP and on program improvements and direction;

3) Revising program activities as requested by DPH or EOHHS and approved by EOHHS;

4) Participating in any DPH or EOHHS-initiated program evaluation activities and accompanied recommendations for future direction;

5) Providing data from MCPAP Live to respond to Health Resources and Services Administration (HRSA) performance measures in the reporting template as specified by DPH on a quarterly basis;

6) Making any enhancements to the data base that are needed for the project, e.g., amending the data elements for the provider education segment specific to the 0-5 age group; and

7) Providing quarterly expenditure reports to DPH on spending of the EC MCPAP program in Central Hub submitted to DPH to ensure compliance with HRSA's financial reporting requirements;

s. As further directed by EOHHS, the Contractor will submit an annual report to DPH and EOHHS which meets the HRSA reporting requirements. The track and report on the following performance measures using information reported from the prior year as a baseline:

1) Number of trainings held by topic and mechanism (e.g., in-person, web-based);

2) Number and types of providers training type (e.g., Project ECHO, other distance learning training, in-person training);

3) Number and types of providers enrolled in a statewide or regional pediatric mental health care access program;

4) Percentage of primary care providers enrolled in a statewide or regional pediatric mental health care access program who receive tele-consultation on Behavioral Health conditions;

5) Reasons for provider contact with the pediatric mental health team (e.g., psychiatric consultation and/or care coordination, and suspected or diagnosed Behavioral Health conditions such as depression, anxiety, ADHD, or Autism Spectrum Disorder);

6) Course of action to be taken by provider as result of contact with the pediatric mental health team and number of times each course of action was recommended (e.g., medication evaluation/change, use of screening tool or instrument, referral to community-based support services or resources, referral to Behavioral Health provider);

7) Number of consultations and referrals provided to enrolled providers by the pediatric mental health team, by enrolled provider discipline type, and by telehealth mechanism (e.g., telephone, videoconferencing, email);

8) Number of consultations and referrals provided by each discipline type (e.g., psychiatrist, counselor, care coordinator) of the pediatric mental health team;

9) Number and types of community-based mental health and support service and service providers in the telehealth referral database (e.g., childcare, employment/job-seeking training, food programs, housing support, parenting support, school-based services, Behavioral Health services, inpatient and outpatient treatment programs; inpatient hospitalization or emergency department; all other clinical provider services including medication management; and all other service or service provider types);

10) Types of referrals provided by the pediatric mental health team (e.g., Behavioral Health services, inpatient and outpatient treatment programs; inpatient hospitalization or emergency department; other clinical provider services including medication management; school-based services; parenting support);

11) Number of children and adolescents, age 0–21, and a subset of children 0 through 5 years of age, for whom a provider contacted the pediatric mental health team for consultation or referral during the reporting period;

12) Number of referrals provided to children and adolescents aged 0–21, and a subset of children 0-5 years of age, for whom a primary care provider contacted the pediatric mental health team during the reporting period;

13) Number of children and adolescents, age 0–21 and a subset of children 0 through 5 years of age, for whom a provider contacted the pediatric mental health team, who received at least one screening for a Behavioral Health condition using a standardized validated tool;

14) Percentage of children and adolescents, 0–21 and a subset of children 0 through 5 years of age, for whom providers contacted the pediatric mental health team for consultation or referral during the reporting period, from rural and underserved counties;

15) Number of children and adolescents, 0–21 and a subset of children 0 through 5 years of age, for whom a primary care provider contacted the pediatric mental health team during the reporting period, who were recommended for referral to a behavioral clinician or treatment from the primary care provider; and

16) Number of children and adolescents, age 0–21 and a subset of children 0 through 5 years of age, for whom a primary care provider contacted the pediatric mental health team during the reporting period, who screened positive for a Behavioral Health

condition using a validated tool, and who were recommended for referral to a behavioral clinician or treatment from the primary care provider.

3. Crisis Service Safety Initiative

The Contractor shall administer the Crisis Service Safety Initiative by providing oversight to the Living Room Model as directed by EOHHS and DMH, ensuring that providers receiving these grants:

a. Provide a 24/7 peer supported recovery environment for individuals 18 and older who are experiencing a crisis as an alternative to emergency services or traditional crisis stabilization services, as no cost to the individual for no longer than 24 hours per encounter.

b. Staff the Living Room Model with Certified Peer Specialists who have received training in alternative crisis intervention techniques.

4. Medication for Opioid Use Disorder (MOUD) Access and Pain Management Support

The Contractor shall develop a network of MOUD expert prescribers and pain management specialists to support primary care providers as follows:

a. The Contractor shall develop a virtual consult (phone or video) system to link primary care and other providers requesting consult with MOUD experts and pain management specialists for support or consultation.

b. The Contractor shall maintain a central help desk to connect primary care providers to such experts and specialists.

c. The MOUD experts identified by the Contractor shall provide consultation on MOUD including, but not limited to:

1) MOUD initiation;

2) MOUD management (e.g., titration for existing patients);

3) Dosing;

4) Appropriate prescribing for patients on more than one medication;

5) Prescribing guidance for vulnerable populations with increased risk of diversion; and

6) Support for clinical presentation of complex cases for MOUD medication.

d. The pain management specialists identified by the Contractor shall provide consultations on pain management, including but not limited to:

1) Pain management prescribing (e.g., initial prescription, weaning patient off of or changing prescription);

2) Dosing;

3) Appropriate prescribing for patients on more than one medication;

4) Prescribing guidance for vulnerable populations with increased risk of diversion; and

5) Support clinical presentation of complex cases for pain management.

e. As directed by EOHHS, the Contractor shall develop strategies for increasing provider utilization of the consultations on MOUD and pain management set forth in this **Section 2.6.D.4**, which shall include, but not be limited to:

1) MOUD and Pain Management Specialists to place follow-up calls to training programs to enhance training support resources;

2) MOUD and Pain Management Specialists to place follow-up calls to practices that have requested consultations in the past;

3) MOUD and Pain Management Specialists to present at hospital grand rounds or other hospital presentations;

4) MOUD and Pain Management Specialists to staff and manage monthly "office hours" where clinicians can call in for a group discussion; and

5) Enhancing promotional materials, including but not limited to developing a clinical manual for dissemination.

f. As directed by EOHHS, the Contractor shall provide case management and care navigation support to assist healthcare facilities, individual practitioners and other healthcare providers including, but not limited to, nurse case managers, social workers and recovery coaches in identifying community-based providers to refer patients for treatment of substance use disorder.

g. As directed by EOHHS, the Contractor shall annually submit to EOHHS a comprehensive evaluation of the MOUD and Pain Management Consultation programs, including but not limited to a provider satisfaction survey and member follow-ups to document outcomes.

5. Community Support Program (CSP) Benefits

The Contractor shall provide Community Support Program services (CSP) and

Specialized CSP services, including CSP for Homeless Individuals (CSP-HI), CSP Tenancy Preservation Program (CSP-TPP), and CSP for Individuals with Justice Involvement (CSP-JI) in accordance with 130 CMR 461 and as follows:

a. Arrange, coordinate, and provide to Covered Individuals Medically Necessary CSP and Specialized CSP services as set forth in Appendix A-1 and consistent with MassHealth Medical Necessity guidelines for CSP and Specialized CSP services;

b. Execute and maintain written contracts with a sufficient number of Providers of CSP and Specialized CSP services to ensure Covered Individuals have timely access to such services and as follows:

   1) The Contractor shall ensure Providers of CSP and Specialized CSP meet the respective Provider qualifications and staffing requirements set forth in 130 CMR 461.

   2) The Contractor shall execute and maintain contracts with all Providers of CSP-JI services, as further specified by EOHHS, and shall report to EOHHS about its Network Providers of Specialized CSP in accordance with **Appendix E-1**.

c. Actively communicate with Providers of CSP-HI, CSP-TPP, and CSP-JI regarding the provision of the respective CSP services to Covered Individuals, including coordinating care to ensure that Covered Individuals' needs are met;

d. Develop performance specifications for the delivery of CSP-HI, CSP-TPP, and CSP-JI as specified by EOHHS and submit such performance specifications to EOHHS as well as any updates to the specifications as they occur;

e. Designate a single point of contact to provide information to Providers of specialized CSP and to EOHHS, as further specified by EOHHS. The Contractor shall designate one point of contact for both CSP-HI and CSP-TPP and a separate point of contact for CSP-JI; and

f. Establish Provider rates at or above the rates in accordance with **Appendix L** to the Contract.

6. [Reserved]

7. [Reserved]

8. Preventive Behavioral Health Services

The Contractor shall cover medically necessary preventive Behavioral Health services for members from birth until age 21, or their caregiver, as outlined in

Appendix A-1, and in **MassHealth Managed Care Entity Bulletin 65** or as further specified by EOHHS. The Contractor shall cover up to six sessions of preventive Behavioral Health services without requiring prior authorization or a diagnostic assessment, such as the CANS (Child and Adolescent Strengths and Needs). After six sessions, the Contractor may require the provider to submit documentation to support the clinical appropriateness of ongoing preventive services. The Contractor may require providers to complete a diagnostic assessment, including the CANS, as part of the Contractor's determination of the ongoing need for preventive services. The Contract shall pay providers no less than the rate set forth in **Appendix L** for these services and shall require providers to utilize the code and modifier combination set forth in **Appendix L** when billing for such services.

9. [Reserved]

10. Behavioral Health Urgent Care Program

    a. The Contractor shall manage an attestation process for mental health centers or other providers, as directed by EOHHS, to become designated Behavioral Health Urgent Care providers. The attestations must include assurances that the mental health center meets the following requirements:

        1) Provide same or next day appointment available for diagnostic evaluation for new clients;

        2) Provide same or next day urgent appointments for current clients;

        3) Provide urgent psychopharmacology appointments and MAT or MOUD evaluation access within 72 hours, as needed based on a psychosocial assessment;

        4) Provide other treatment appointments within 14 calendar days;

        5) Provide extended clinical availability outside of the hours of 9am-5pm, including:

            a) Eight (8) hours of extended availability per week during weekdays;

            b) Two 4-hour blocks of availability on weekends per month

        6) Each quarter, the Contractor shall collect the following reports from the designated Behavioral Health Urgent Care providers, stratified by months, or other reporting as required by EOHHS:

            a) Percentage of total quarterly visits provided during extended appointment hours

b) Percentage of total quarterly initial evaluations completed within 1 day of clinic operation following the first contact

c) Percentage of total quarterly initial evaluations completed during extended appointment hours

d) Percentage of total quarterly urgent visits for existing clients completed within 1 day of clinic operation

e) Percentage of total quarterly urgent visits completed within 1 day of clinic operation occurring during extended appointment hours

f) Percentage of total quarterly urgent psychopharmacology appointments that occur within 72 hours of initial diagnostic evaluation

g) Percentage of total quarterly Medication for Addiction Treatment appointments that occur within 72 hours of initial diagnostic evaluation

h) Percentage of total quarterly routine or follow-up visits completed within 14 calendar days of initial contact; and

i) Percentage of total quarterly routine or follow-up visits completed within 14 calendar days of initial contact that occur during extended appointment hours.

7) Other attestation requirements as directed by EOHHS.

b. The Contractor shall conduct an annual analysis and summary of the Behavioral Health Urgent Care Program Member Experience Survey

c. The Contractor shall pay Behavioral Health Urgent Care providers designated by EOHHS in accordance with **Section 2.7.F.3**.

d. The Contractor shall work with EOHHS to strategize and implement payment and program innovation for BHUC providers.

e. The Contractor shall develop Performance Specifications for the delivery of Behavioral Health Urgent Care services as specified by EOHHS and submit such Performance Specifications to EOHHS when directed by EOHHS. The contractor shall update EOHHS within 30 days if there are any updates to the Performance Specifications.

11. Behavioral Health Crisis Evaluation and Management Services

a. [Reserved]

b. Behavioral Health Crisis Management

1) The Contractor shall pay hospitals for behavioral health crisis management in medical or surgical inpatient and emergency department settings set forth in **Appendix A-1** as set forth in **Section 2.7.F.3.t**. Hospitals may sub-contract these services out to behavioral health providers, including crisis teams, but hospitals shall be solely responsible for billing the Contractor unless otherwise directed by EOHHS.

2) Once all hospitals have established procedures for behavioral health crisis evaluations in acute medical settings, as determined by EOHHS, the Contractor shall not make payments to Emergency Service Programs and Mobile Crisis Intervention teams for ED-based behavioral health crisis evaluations provided in the Emergency Department.

c. The Contractor shall pay community-based AMCI and YMCI teams for a day of Adult or Youth Mobile Crisis Intervention services performed on the same day as a behavioral health crisis evaluation provided in a medical or surgical inpatient or emergency department setting as set forth in **Appendix A-1**, in accordance with **Section 2.7.F.3** and **Appendix L**.

12. Health Related Social Needs (HRSN) Supplemental Services for Covered Individuals Enrolled in a PCACO

The Contractor shall work with each PCACO to provide HRSN Supplemental Services as follows and as further specified by EOHHS, including but not limited to the HRSN Service Manual:

a. The Contractor shall provide the HRSN Supplemental Services selected by each PCACO in accordance with the requirements in this section. Each PCACO's selection shall be reflected in **Appendix O, Exhibit 2** and described in **Appendix O, Exhibit 1**.

b. Providing HRSN Supplemental Services

The Contractor shall:

1) Arrange, coordinate, and provide to Covered Individuals enrolled in a PCACO the HRSN Supplemental Services selected by each PCACO, specified in Appendix O, Exhibit 2 and described in Appendix O, Exhibit 1, in accordance with the requirements of this Contract, the HRSN Service Manual, and as otherwise specified by EOHHS.

2) Coordinate with each PCACO to:

a) Ensure that a Covered Individual enrolled in a PCACO

receives only one HRSN Category 1 Supplemental Nutrition Service at any given time.

b) Provide HRSN Category 2 Supplemental Nutrition Services only to a Covered Individual enrolled in a PCACO who is also receiving a HRSN Category 1 Supplemental Nutrition Service.

3) Coordinate with the PCACO to require Providers of HRSN Supplemental Services to request and receive service registration from the Contractor, or the PCACO, prior to providing HRSN Supplemental Services. This service registration is not an authorization and therefore is not subject to the authorization and utilization management requirements set forth in Section 2.6.C. The Contractor shall work with each PCACO to:

a) Respond to Provider service registration requests no later than seven (7) business days after receipt of the request; and

b) Require Providers of HRSN Supplemental Services to include, at minimum, the following information when submitting a service registration request:

(i) The MassHealth identification number of the Covered Individual enrolled in a PCACO;

(ii) National Provider Identifier;

(iii) HRSN Supplemental Service for which the service registration request is being submitted; and

(iv) Anticipated service duration.

c. Contracting with Providers of HRSN Supplemental Services

1) The Contractor shall coordinate with each PCACO to execute and maintain written contracts with a sufficient number of Providers, as determined by each PCACO, of the HRSN Supplemental Services for each PCACO as set forth in Appendix O, Exhibit 2, to ensure Covered Individuals enrolled in a PCACO have timely access to such services. The Contractor shall work with each PCACO to establish contracting protocols to allow information sharing and coordination between the three entities. The Contractor shall execute and maintain contracts with those Providers of HRSN Supplemental Services identified by each PCACO.

a) If there are an insufficient number of qualified providers

located in Massachusetts who are able to provide Covered Individuals enrolled in a PCACO with appropriate access to HRSN Supplemental Services, the Contractor shall contract with out-of-state providers meeting all requirements in the Contract and the HRSN Service Manual, as determined by the PCACO.

b) The Contractor shall work with each PCACO to screen, credential, and enroll Providers of HRSN Supplemental Services in accordance with Section 2.8.G provided, however, that the Contractor shall establish processes accounting for the fact that these providers are not subject to NCQA standards and certain traditional licensing requirements.

c) The Contractor shall work with each PCACO to ensure Providers of HRSN Supplemental Services meet the Provider qualifications set forth in the HRSN Service Manual and as further specified by EOHHS.

2) The Contractor shall coordinate with each PCACO to ensure that all Providers of HRSN Supplemental Services establish, maintain, and implement written policies and procedures for working with the Contractor and the PCACO, including but not limited to addressing:

a) Referrals and their disposition;

b) Information exchange;

c) Start and end dates of HRSN Supplemental Services;

d) Timing and outcomes of determinations for whether a Covered Individual enrolled in a PCACO meets the criteria to receive HRSN Supplemental Services; and

e) Coordination with the Contractor and the PCACO.

3) The Contractor shall ensure that staff of Providers of HRSN Supplemental Services receive documented training to enhance the quality and cultural competence of services delivered and to broaden their skills related to the provision of HRSN Supplemental Services.

4) [Reserved]

5) [Reserved]

d. Administrative, Customer Service for Covered Individuals enrolled in a PCACO Services, and Reporting Requirements

1) The Contractor shall update key personnel to appoint an HRSN Point of Contact consistent with **Section 2.3.A.3**.

2) As further specified by EOHHS, the Contractor shall include information about HRSN Supplemental Services in the Contractor's Covered Individuals handbook. Such information shall be consistent with the HRSN Service Manual when applicable, and shall include, in addition to all other Covered Individuals handbook requirements, the following information:

a) A list of HRSN Supplemental Services the Contractor provides consistent with **Appendix O, Exhibit 2** and a description of such services;

b) Description of who may receive HRSN Supplemental Services;

c) How Covered Individuals enrolled in a PCACO may access such services.

3) In accordance with **Section 2.7.G**, the Contractor shall include Providers of HRSN Supplemental Services in its Provider Directory.

4) The Contractor shall collaborate with each PCACO to develop, implement, and maintain processes for collecting, sharing, and reporting data related to HRSN Supplemental Services as further specified by EOHHS.

5) The Contractor shall ensure that information about consent, screening, and referrals is documented in the Covered Individual enrolled in a PCACO's medical records.

e. Determining Whether a Covered Individual enrolled in a PCACO Meets the Criteria for Receiving HRSN Supplemental Services

The Contractor shall coordinate with the PCACO to ensure Covered Individuals enrolled in a PCACO meet the criteria for receiving HRSN Supplemental Services in accordance with the requirements set forth in the HRSN Service Manual as follows:

1) The Contractor shall work with each PCACO to ensure the Covered Individual enrolled in a PCACO meets the criteria for receiving HRSN Supplemental Services at all of the following times:

a) Prior to the start date of a Covered Individual enrolled in a PCACO receiving HRSN Supplemental Services;

b) No less than:

(i) For HRSN Supplemental Housing Services, every 12 months.

(ii) For HRSN Category 1 Supplemental Nutrition Services, every 6 months. If the Covered Individual enrolled in a PCACO is pregnant or postpartum, they may alternately be assessed at 2 months postpartum if they were first assessed during the pregnancy, resulting in a timing interval between assessments that is longer than 6 months.

(iii) For HRSN Category 2 Supplemental Nutrition Services, every 12 months.

c) Whenever a Covered Individual enrolled in a PCACO experiences a major change that may impact whether the Covered Individual enrolled in a PCACO meets the criteria to receive HRSN Supplemental Services.

2) Determinations for whether a Covered Individual enrolled in a PCACO meets the criteria to receive HRSN Supplemental Services may be determined by the Contractor, the PCACO, a BH or LTSS CP, or a Provider, including a Provider of HRSN Supplemental Services.

3) The Contractor shall ensure that information about whether and how the Covered Individual enrolled in a PCACO meets the criteria for receiving a HRSN Supplemental Service is:

a) Made available to the Provider providing the HRSN Supplemental Service(s) and the PCACO; and

b) Documented in the Covered Individual enrolled in a PCACO's medical record.

4) [Reserved]

5) For any determination that a Covered Individual enrolled in a PCACO does not meet the criteria to receive HRSN Supplemental Services, the Contractor shall work with each PCACO to:

a) Make best efforts to work with the Covered Individual enrolled in a PCACO and their care team, as appropriate, to

ensure the Covered Individual enrolled in a PCACO's needs are met (e.g. coordinating care in accordance with **Section 2.5.I**)

b) Ensure the Covered Individual enrolled in a PCACO is made aware of their rights to file a grievance, in accordance with **Section 2.12**.

f. HRSN Supplemental Services Service Plan

The Contractor shall coordinate with the PCACO to ensure that Providers of HRSN Supplemental Services develop and maintain a service plan for all Covered Individuals enrolled in a PCACO receiving HRSN Supplemental Services as follows:

1) Service plans shall:

a) Be person-centered;

b) Identify the service(s) provided and responsible parties;

c) Identify ways to support the Covered Individuals enrolled in a PCACO in mitigating barriers to accessing and utilizing services;

d) Identify the Covered Individual enrolled in a PCACO's needs and individualized strategies and interventions for meeting those needs;

e) As appropriate, be developed in consultation with the Covered Individual enrolled in a PCACO and Covered Individual enrolled in a PCACO's chosen support network including family and other natural or community supports; and

f) Subject to consent by the Covered Individual enrolled in a PCACO and as appropriate, incorporate available records from referring and existing providers and agencies, including any bio-psychosocial assessment, reasons for referral, goal, and discharge recommendations.

2) The Contractor shall work with the PCACO to ensure Providers of HRSN Supplemental Services:

a) Collect or have access to all the information necessary to create, review, and update a service plan.

b) Review and update service plans:

(i) No less than every 12 months;

(ii) Whenever a Covered Individual enrolled in a PCACO experiences a major change that may impact their HRSNs; and

(iii) Upon the request of the Covered Individual enrolled in a PCACO.

g. Provider Payments for HRSN Supplemental Services

The Contractor shall pay Providers the rates equal to those established by each PCACO in accordance with the MassHealth HRSN Supplemental Services Fee Schedule and shall use procedure codes as directed by EOHHS to provide payment for such services.

h. Suspension of HRSN Supplemental Services

The Contractor shall suspend the provision of an HRSN Supplemental Service upon EOHHS' notification that overall funding levels for that HRSN Supplemental Service (or for all HRSN Supplemental Services) has been reached for the Contract Year and, as further directed by EOHHS, shall provide Covered Individuals enrolled in a PCACO notice of such suspension.

i. Additional Terms and Conditions

1) The Contractor shall ensure that receiving HRSN Supplemental Services remains the choice of the Covered Individual enrolled in a PCACO, and that the Covered Individual enrolled in a PCACO may opt out at any time.

2) The Contractor shall not apply requirements related to continuity of care in **Section 2.2.C** or related to out-of-network access in **Section 2.8.B.19** to HRSN Supplemental Services.

3) The Contractor shall ensure all Providers of HRSN Supplemental Services have appropriate policies and procedures in place to address potential conflicts of interest between service planning and service delivery.

E. [Reserved]

F. Mental Health Services in IMDs

1. The Contractor shall cover the Inpatient Mental Health Services (including Observation/Holding Beds and Administratively Necessary Day Services) for Covered Individuals ages 21-64, Youth and Adult Community Crisis Stabilization, and Community Based Acute Treatment for Children and

Adolescents (CBAT) set forth in **Appendix A-1** delivered in Institutions for Mental Disease (IMD), as defined in Section 1905(i) of the Act, for stays of no more than 60 consecutive days.

2. For any Covered Individual who received Inpatient Mental Health Services (including Observation/Holding Beds and Administratively Necessary Day Services) for Covered Individuals ages 21-64, Youth and Adult Community Crisis Stabilization, and Community Based Acute Treatment for Children and Adolescents (CBAT) set forth in **Appendix A-1** in an IMD for more than 60 consecutive days, the Contractor shall:

   a. Report to EOHHS, in a form and format and at a frequency to be determined by EOHHS:

      1) The Covered Individual's rating category;

      2) The length of stay in the IMD; and

      3) Any other information requested by EOHHS.

   b. As further specified and directed by EOHHS, accept EOHHS' reconciliation of the capitation payments received by the Contractor pursuant to **Section 4** and **Appendix H-1** for period in which the Covered Individual received the Inpatient Mental Health Services (including Observation/Holding Beds and Administratively Necessary Day Services) for Covered Individuals ages 21-64, Youth and Adult Community Crisis Stabilization, and Community Based Acute Treatment for Children and Adolescents (CBAT) set forth in **Appendix A-1** in an IMD for more than 60 consecutive days.

Section 2.7 BH Provider Contracts and Related Responsibilities

A. BH Provider Contracts General Requirements

The Contractor shall:

1. Maintain all Provider Contracts and other agreements and subcontracts relating to this Contract, including single case agreements with out of network providers, in writing.

   a. All such agreements and subcontracts shall fulfill all applicable requirements of 42 CFR Part 438 and shall contain all relevant provisions of this Contract appropriate to the subcontracted service or activity. Without limiting the generality of the foregoing, the Contractor shall ensure that all Provider Contracts and contracts with out of network providers include the following provision: *"Providers shall not seek or accept payment from any Covered Individual for any BH Covered Service*

rendered, nor shall Providers have any claim against or seek payment from EOHHS for any BH Covered Service rendered to a Covered Individual. Instead, Providers shall look solely to the (Contractor's name) for payment with respect to BH Covered Services rendered to Covered Individuals. Furthermore, Providers shall not maintain any action at law or in equity against any Covered Individual or EOHHS."

b. The Contractor shall not acquire established networks without executing a Provider Contract with each Provider that complies with all of the provisions of this Contract and contacting each Provider to ensure that the Provider understands the requirements of this Contract and agrees to fulfill all terms of the Provider Contract. In Provider organizations where the organization represents the Provider in business decisions, a Provider Contract with the Provider organization shall be sufficient to satisfy this requirement.

2. Require a National Provider Identifier on all claims and provider applications;

3. Not include in its Provider Contracts any provision that directly prohibits or indirectly, through incentives or other means, limits or discourages Network Providers from participating as Network or non-network Providers in any provider network other than the Contractor's Provider Network(s), and

4. With respect to all Provider Contracts, comply with 42 CFR 438.214 Provider selection, including complying with any additional requirements as specified by EOHHS;

5. Require all Providers to provide a Covered Individual's clinical information to other Providers, as necessary, to ensure proper coordination and BH treatment of Covered Individuals who express suicidal or homicidal ideation or intent, consistent with state law;

6. Require Behavioral Health Providers to submit to the Contractor a written report of all Reportable Adverse Incidents in accordance with **Appendix E-1**, or in another form and format acceptable to EOHHS;

7. Require the use of any standardized clinical assessment tools by substance use disorder treatment providers as directed by EOHHS;

8. Ensure that all Provider Contracts prohibit Providers from:

   a. Billing Covered Individuals for missed appointments or refusing to provide services to Covered Individuals who have missed appointments. Such Provider Contracts shall require Providers to work with Covered Individuals and the Contractor to assist Covered Individuals in keeping their appointments;

b. Billing patients for charges for BH or non-BH Covered Services;

c. Refusing to provide services to a Covered Individual because the Covered Individual has an outstanding debt with the Provider from a time prior to the Covered Individual becoming a MassHealth Member;

d. Closing or otherwise limiting their acceptance of Covered Individuals as patients unless the same limitations apply to all commercially insured enrollees.

9. Ensure that all Provider Contracts specify that:

a. No payment shall be made by the Contractor to a Provider for a Provider Preventable Condition;

b. As a condition of payment, the Provider shall comply with the reporting requirements as set forth in 42 CFR 447.26(d) and as may be specified by the Contractor. The Provider shall comply with such reporting requirements to the extent the Provider directly furnishes services;

c. The Contractor shall not refuse to contract with or pay an otherwise eligible health care provider for the provision of BH Covered Services solely because such Provider has in good faith:

1) Communicated with or advocated on behalf of one or more prospective, current or former patients regarding the provisions, terms or requirements of the Contractor's BHP as they relate to the needs of such Provider's patients; or

2) Communicated with one or more prospective, current or former patients with respect to the method by which such Provider is compensated by the Contractor for services provided to the patient;

d. No contract between the Contractor and a Provider may contain any incentive plan that includes a specific payment to a Provider as an inducement to deny, reduce, delay or limit specific, Medically Necessary Services;

e. A Provider is not required to indemnify the Contractor for any expenses and liabilities, including, without limitation, judgments, settlements, attorneys' fees, court costs and any associated charges, incurred in connection with any claim or action brought against the Contractor based on the Contractor's management decisions, utilization review provisions or other policies, guidelines or actions;

f. When a Provider contract is terminated for any reason, a Provider must assist with transitioning Covered Individuals to new Providers, including sharing the Covered Individual's medical record and other relevant

Covered Individual information as directed by the Contractor or Covered Individual;

g. The Contractor shall provide a written statement to a Provider of the reason or reasons for termination with cause;

h. Providers shall participate in Contractor's continuity of care policies and procedures as described in **Section 2.2.C**;

i. Contracts between the Contractor and Providers shall require Providers to comply with the Contractor's requirements for utilization review, quality management and improvement, credentialing and access and availability of services, and

j. Contracts between the Contractor and Providers shall require Providers to comply with the accessibility standards as described in **Section 2.9**.

10. Maintain, for all Providers with whom it has a Provider Contract, a payment rate schedule for all BH Covered Services each Provider is contracted to provide. The Contractor shall establish policies and procedures to ensure:

a. Compliance with the Provider payment requirements set forth in **Section 2.7**, as updated by EOHHS from time to time;

b. Any modifications to the Contractor's payment rates to Providers are communicated to Providers and reflected in the payment rate schedule in a timely manner;

c. The payment rate schedule is made available, upon request, to Providers; and

d. The Contractor's Material Subcontractors, as applicable, adhere to the requirements of this **Section 2.7.A.10**.

B. Additional Responsibilities for BH Providers that Serve Covered Individuals under Age 21

For Network Providers that serve Covered Individuals under age 21, the Contractor shall enter into and oversee Provider Contracts with Network Providers who provide Behavioral Health Services that include the following requirements:

1. The Contractor shall ensure that such Provider Contracts shall require that clinicians, including psychiatrists, psychiatric residents, psychiatric nurse mental health clinical specialists, psychologists, Licensed Independent Clinical Social Workers (LICSWs), Licensed Alcohol and Drug Counselors 1 (LADC1), Licensed Mental Health Counselors (LMHCs), Licensed Marriage and Family Therapists, (LMFTs), Licensed Clinical Social Workers (LCSWs), and unlicensed Master's level clinicians working under the supervision of a licensed clinician,

who provide Behavioral Health Services to Covered Individuals under the age of 21 in certain levels of care, including Diagnostic Evaluation for Outpatient Therapy (individual Counseling, Group Counseling, and Couples/Family Counseling), In-Home Therapy, Inpatient Psychiatric Services, and Community Based Acute Treatment Services (CBAT):

a. Participate in CANS training sponsored by EOHHS;

b. Become certified in the use of the CANS Tool and recertified every two years;

c. Use the CANS Tool whenever they deliver a Behavioral Health Clinical Assessment for a Covered Individual under the age of 21, including the initial Behavioral Health Clinical Assessment and, at a minimum, every 180 days thereafter during ongoing treatment;

d. Use the CANS Tool as part of the Discharge Planning process from Inpatient Psychiatric Hospitalizations and Community Based Acute Treatment Services; and

e. Subject to consent by the Covered Individual, parent, guardian, custodian, or other authorized individual, as applicable, input into the CANS IT system the information gathered using the CANS Tool and the determination whether or not the assessed Covered Individual is suffering from a Serious Emotional Disturbance (SED);

2. The Contractor shall ensure that such Provider Contracts with Community Service Agencies require that intensive care coordinators of all levels:

a. Become certified in the use of the CANS Tool and re-certified every two years;

b. Use the CANS Tool during the comprehensive home-based assessment that is part of the initial phase of Intensive Care Coordination (ICC), at least every 180 days thereafter during ongoing care coordination, and as part of Discharge Planning from ICC services; and

c. Subject to consent by the Covered Individual, parent, guardian, custodian, or other authorized individual, as applicable, input into the CANS IT System the information gathered using the CANS Tool and a determination as to whether or not the Covered Individual meets the definition of an SED;

3. The Contractor shall ensure that such Provider Contracts require all Behavioral Health Providers who have clinicians who are required to provide Behavioral Health Clinical Assessments and perform the Discharge Planning process from Inpatient Psychiatric Hospitalizations and Community Based Acute Treatment

Services using the CANS Tool in accordance with **Section 2.7.B**, have Virtual Gateway accounts and a high speed internet or satellite internet connection to access the CANS IT System, provided that the Contractor may have policies and procedures approved by EOHHS to grant temporary waivers for these requirements on a case by case basis;

4. The Contractor shall establish policies and procedures that:

   a. Require Behavioral Health Providers who are required to provide Behavioral Health Clinical Assessments and perform the Discharge Planning process from Inpatient Psychiatric Hospitalizations and Community Based Acute Treatment Services using the CANS Tool in accordance with **Section 2.7.C.5.a** to seek consent from the Covered Individual, parent, guardian, custodian, or other authorized individual, as applicable, before entering CANS assessments into the CANS IT System using the form of consent approved by EOHHS;

   b. Require Behavioral Health Network Providers who obtain such Covered Individual consent to enter the information gathered using the CANS Tool and the determination whether or not the assessed Covered Individual is suffering from an SED into the CANS IT System; and

   c. Require Behavioral Health Network Providers who do not obtain such Covered Individual consent to enter only the determination of whether or not the assessed Covered Individual is suffering from a Serious Emotional Disturbance into the CANS IT System.

5. As directed by EOHHS, the Contractor shall:

   a. Pay Pay no less than EOHHS approved rates for CPT code 90791 with modifier HA for initial Behavioral Health Clinical Assessments using the CANS Tool for Covered Individuals under the age of 21. Further:

      1) The Contractor shall ensure that any failure to include an "HA" modifier using CPT Service Code 90791 will result in a denial of the claim for members under 21 if billed without the HA modifier.

      2) For members under 21, the Contractor shall allow Network Providers up to two 90791 "HA" claims per member per site in a 90-day period. The Contractor shall also allow a new set of 90791 "HA" claims when the member experiences a lapse in service of six month or more with the original provider;

   b. Only pay a Provider for providing Behavioral Health Clinical Assessments using the CANS Tool if such Provider's servicing clinicians are certified in the CANS Tool;

c. Ensure that Providers of Behavioral Health Clinical Assessments using the CANS Tool bill for these assessments and do not bill as a separately billable service the review and updating of the assessment that is required every 180 days for Covered Individuals in ongoing, individual, group, or family therapy since such review and updating is part of treatment planning and documentation; and

d. Ensure that its Providers have the ability to access and use the CANS IT System and data contained therein, and shall, as further directed by EOHHS, participate in any testing or development processes as necessary for EOHHS to build the CANS IT System.

C. BH Inpatient and 24-hour Diversionary Services

The Contractor shall:

1. Ensure that all BH Inpatient and 24-Hour Diversionary Services Provider Contracts require the BH Inpatient and 24-Hour Diversionary Services Provider accept for admission or treatment all Covered Individuals for whom the Contractor has determined admission or treatment is Medically Necessary, regardless of clinical presentation, as long as a bed is available in an age appropriate unit;

2. Promote continuity of care for Covered Individuals who are readmitted to BH Inpatient and 24-Hour Diversionary Services by offering them readmission to the same Provider when there is a bed available in that facility;

3. Require BH Inpatient and 24-Hour Diversionary Services Providers to coordinate treatment and Discharge Planning with the state agencies (e.g., DCF, DMH, DYS, DDS) with which the Covered Individual has an affiliation, and that in no case shall Providers discharge patients who are homeless or who have unstable housing without a plan for housing as detailed in **Section 2.7.C.5.c.12**;

4. Ensure that all BH Inpatient and 24-Hour Diversionary Services Providers have:

   a. Human rights and restraint and seclusion protocols that are consistent with the DMH's Human Rights and Restraint Seclusion Policy and regulations and include training of the Provider's staff and education for Covered Individuals regarding human rights; and

   b. A human rights officer, who shall be overseen by a human rights committee, and who shall provide written materials to Covered Individuals Covered Individuals regarding their human rights, in accordance with applicable DMH regulations and requirements;

5. Require that BH Inpatient and 24-hour Diversionary Services Providers coordinate with designated CBHCs, including procedures to credential and grant admitting privileges to said provider psychiatrists; and

6. Convene regular meetings and conduct ad hoc communication on clinical and administrative issues with designated CBHCs to enhance the continuity of care for Covered Individuals.

D. Medication for Opioid Use Disorder (MOUD) Services

1. The Contractor shall ensure that Covered Individuals have access to MOUD Services, including initiation and continuation of MOUD, and ensure that Covered Individuals receive assistance in accessing such services.

2. The Contractor shall include in its Provider Network, qualified providers to deliver MOUD Services, by at a minimum, as further directed by EOHHS, and in accordance with all other applicable Contract requirements, offering Network Provider agreements at a reasonable rate of payment to:

   a. All Office Based Opioid Treatment (OBOT) providers as specified by EOHHS;

   b. All Opioid Treatment Program (OTP) providers as specified by EOHHS;

3. The Contractor shall ensure that all such Providers of MOUD Services coordinate and integrate care with Covered Individuals' PCPs and other providers in response to Covered Individuals' needs.

4. The Contractor shall not require an authorization or referral for MOUD Services, unless otherwise directed by EOHHS.

E. Additional Responsibilities for Certain Providers

1. At EOHHS' direction, the Contractor shall incorporate DMH's Infection Control Competencies/Standards, as set forth in Attachments A and B to DMH Licensing Bulletin 20-05R, or successor guidance, in its contracts with DMH-licensed providers of Inpatient Mental Health Services. The Contractor shall review such facility's compliance with the applicable DMH requirements as part of the Contractor's program integrity efforts pursuant to **Section 2.3.D.3**. The Contractor shall promptly report any noncompliance with the applicable DMH standards to EOHHS and shall treat such noncompliance in accordance with the Contractor's program integrity activities pursuant to **Section 2.3.D.3**.

2. As directed by EOHHS, the Contractor shall contract with the network of Community Services Agencies (CSAs) to provide Intensive Care Coordination, Family Support and Training Services, and Family-based Intensive Treatment. For each of these services, the Contractor shall establish Provider rates at or above the rate floor set by EOHHS in 101 CMR 352, unless otherwise directed by

EOHHS, and shall, as directed by EOHHS, use the procedure codes specified by EOHHS to provide payment for such services.

3. As directed by EOHHS, the Contractor shall establish provider rates at or above the rate floor set by EOHHS in 101 CMR 352, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for the following services:

   a. Family Support and Training Services;

   b. In-Home Behavioral Services (including Behavior Management Therapy and Behavior Management Monitoring) and Therapeutic Mentoring Services; and

   c. In-Home Therapy Services (including Therapeutic Clinical Intervention and Ongoing Therapeutic Training and Support).

4. In collaboration with and as further directed by EOHHS, the Contractor shall support the implementation of Behavioral Health Inpatient Services payment methodologies which may include, but is not limited to: updating claims systems and working with EOHHS and Providers on testing system updates; developing training materials and providing education and training for Providers; and developing and implementing procedures to address Provider escalations.

F. Provider Payments

The Contractor's payments to Network Providers shall be consistent with the provisions of this Section:

1. Timely Payment to Providers

   The Contractor shall make payment on a timely basis to Providers for BH Covered Services furnished to Covered Individuals, in accordance with 42 USC 1396u-2(f) and 42 CFR 447.46. Unless otherwise provided for and mutually agreed to in a contract between the Contractor and a Provider that has been reviewed and approved by EOHHS, the Contractor shall:

   a. Pay 90% of all Clean Claims for BH Covered Services from Providers within 30 days from the date the Contractor receives the Clean Claim;

   b. Pay 99% of all Clean Claims from Providers within 60 days from the date the Contractor receives the Clean Claim;

   c. Submit a Claims Processing report in accordance with **Appendix E-1**; and

   d. For the purposes of this Section, the day the Contractor receives the Clean Claim is the date indicated by the date stamp on the claim and the day the Contractor pays the Clean Claim is the date of the check or other form of payment.

e. Not require a Network Provider to pay a claims processing fee.

2. The Contractor shall not implement any incentive plan that includes a specific payment to a Provider as an inducement to deny, reduce, delay or limit specific, Medically Necessary Services.

   a. The Provider shall not profit from provision of BH Covered Services that are not Medically Necessary or medically appropriate.

   b. The Contractor shall not profit from denial or withholding of BH Covered Services that are Medically Necessary or medically appropriate.

   c. Nothing in this Section shall be construed to prohibit Contracts that contain incentive plans that involve general payments such as capitation payments or shared risk agreements that are made with respect to physicians or physician groups or which are made with respect to groups of Covered Individuals if such agreements, which impose risk on such physicians or physician groups for the costs of medical care, services and equipment provided or authorized by another physician or health care provider.

3. Minimum payment rates for Certain Behavioral Health Services

   a. The Contractor shall provide specialized inpatient psychiatric services to Covered Individuals under the age of 21 with Autism Spectrum Disorder-Intellectual Disability (ASD-ID) in specialized ASD-ID inpatient psychiatric treatment settings, as directed by EOHHS:

      1) The Contractor shall report claims paid for psychiatric Inpatient Services delivered to Covered Individuals under the age of 21 in specialized ASD-ID inpatient psychiatric treatment settings to EOHHS in a form and format and at a frequency to be determined by EOHHS;

      2) The Contractor shall pay Providers no less than the rate specified by EOHHS for inpatient psychiatric services delivered to Covered Individuals under the age of 21 with ASD-ID in specialized ASD-ID inpatient psychiatric treatment settings, and shall use procedure codes as directed by EOHHS to provide payment for such services;

   b. For Case Consultation, Family Consultation, and Collateral Contact services delivered to Covered Individuals under the age of 21, the Contractor shall:

      1) Establish a 15-minute rate at or above one quarter of the 60 minute rate the Contractor sets for providers for outpatient Individual Treatment, or the amount set forth in **Appendix L Exhibit 1 and**

Exhibit 2, whichever is higher, and shall use procedure codes as directed by EOHHS to provide payment for such services.

c. For Acute Treatment Services for Substance Use Disorders (Level 3.7), the Contractor shall establish provider rates at or above the rate floor as specified by EOHHS in 101 CMR 346,unless otherwise directed by EOHHS, including but not limited to, accounting for the publicly assisted client mix factor, and shall use procedure codes as directed by EOHHS to provide payment for such services.

d. For Clinical Stabilization Services for Substance Use Disorders (Level 3.5) the Contractor shall establish provider rates or above the rate floor as specified by EOHHS in 101 CMR 346, unless otherwise directed by EOHHS, including but not limited to, accounting for the publicly assisted client mix factor, and shall use procedure codes as directed by EOHHS to provide payment for such services.

e. For Individualized Treatment Services the Contractor shall establish Provider rates at or above the rate floor set by EOHHS in 101 CMR 444, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

f. For Youth Withdrawal Management and Stabilization Services the Contractor shall establish Provider rates at or above the rate floor set by EOHHS in 101 CMR 418, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

g. For Applied Behavior Analysis (ABA Services), the Contractor shall establish provider rates at or above the rate floor set by EOHHS in 101 CMR 358.00, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

h. For all types of and enhancements to Residential Rehabilitation Services for Substance Use Disorders (ASAM Level 3.1) (RRS) set forth in **Appendix A-1**, the Contractor shall establish Provider rates at or above the rate floor set by EOHHS in 101 CMR 346, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

i. For Program of Assertive Community Treatment services (PACT), the Contractor shall establish provider rates at or above the rate floor as specified in 101 CMR 430.03, and shall use procedure codes as directed by EOHHS to provide payment for such services.

j. For inpatient substance use disorder services provided by freestanding substance use disorder hospitals, the Contractor shall establish provider rates at or above the rates under Appendix A of the MassHealth Program Provider Agreement: Special Conditions for Substance Abuse Treatment Hospitals, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

k. For Youth Community Crisis Stabilization services, the Contractor shall establish provider rates at or above the rates specified in 101 CMR 305.000, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

l. For Opioid Treatment Program services, the Contractor shall establish provider rates at or above the rate floor, set by EOHHS in 101 CMR 444, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

m. The Contractor's payment rates to inpatient psychiatric hospitals for Covered Individuals placed on AND status shall be adequate to maintain the ongoing provision of appropriate clinical care until date of discharge.

n. For inpatient mental health services, the Contractor shall establish provider rates at or above the rates under Section 5.B.4 of the MassHealth Acute Hospital Request for Application and Section 4.2 of Attachment A to the MassHealth Psychiatric Hospital Request for Application, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

o. The Contractor shall:

1) In accordance with **Section 2.7.F.3.n** increase its payment rates to in-state acute hospitals for:

a) adjudicated inpatient discharge by a uniform dollar amount specified by EOHHS; and

b) adjudicated outpatient episodes by a uniform dollar amount specified by EOHHS.

2) The increased payment rates shall be a uniform dollar amount through lump sum payments as directed by EOHHS and consistent with the uniform dollar amount increase payment methodology set forth in the MassHealth Acute Hospital RFA. If directed by EOHHS, the Contractor shall pay in-state acute hospitals an additional uniform dollar amount based on the reconciliation set forth in **Section 4.5** by a date specified by EOHHS.

p. For CBHI Services other than YMCI, the Contractor shall establish Network Provider rates at or above the rate floor specified in 101 CMR 352.00 and procedure codes as set forth in **Section 2.7.K.3**, unless otherwise directed by EOHHS.

q. For YMCI Services, the Contractor shall establish Network Provider rates for CBHCs at or above the rates specified in 101 CMR 305.00 unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

r. The Contractor shall provide specialized inpatient psychiatric services to Covered Individuals with an eating disorder diagnosis in specialized eating disorder inpatient psychiatric treatment settings, as directed by EOHHS:

1) The Contractor shall report claims paid for psychiatric inpatient services delivered to Enrollees with an eating disorder diagnosis and severe associated psychiatric and medical needs in specialized eating disorder inpatient psychiatric treatment settings to EOHHS in a form and format and at a frequency to be determined by EOHHS;

2) The Contractor shall pay Providers no less than the rate specified by EOHHS in the MassHealth Psychiatric Hospital RFA as further specified by EOHHS, for inpatient psychiatric services delivered to Enrollees with an eating disorder diagnosis and severe associated psychiatric and medical needs in specialized eating disorder inpatient psychiatric treatment settings;

s. For behavioral health crisis evaluation services in medical or surgical inpatient and emergency department settings, the Contractor shall establish Provider rates at or above the rate specified in the MassHealth Acute Hospital Request for Application (RFA) unless otherwise directed by EOHHS and shall use procedure codes as directed by EOHHS to provide payment for such services.

t. For behavioral health crisis management services in medical or surgical inpatient and emergency department settings, the Contractor shall establish Provider rates at or above the rate specified in in the MassHealth Acute Hospital Request for Application (RFA) unless otherwise directed by EOHHS and shall use procedure codes as directed by EOHHS to provide payment for such services.

u. For evaluation of Enrollees for opioid use disorder and initiation of Medications for Opioid Use Disorder (MOUD) in the Emergency Department, the Contractor shall establish Provider rates at or above the

rate set by EOHHS in 101 CMR 317, unless otherwise directed by EOHHS, and shall use procedure codes as directed by EOHHS to provide payment for such services.

v. Effective September 1, 2025, for mental health centers designated as Behavioral Health Urgent Care Provider sites, the Contractor shall pay no less than the rate set forth in **Appendix L, Exhibit 3** for these services and shall require providers to utilize the code and modifier combination set forth in **Appendix L, Exhibit 3** when billing for such services rendered by Behavioral Health Urgent Care Provider sites.

w. Effective September 1, 2025, for services rendered by mental health centers that have not been designated as a Behavioral Health Urgent Care Provider site, the Contractor shall pay no less than the rate set forth in **Appendix L, Exhibit 2** and shall use procedure codes as directed by EOHHS to provide payment for such services.

4. Behavioral Health Quality Incentive Payment

The Contractor shall:

a. For each Contract Year, collect the following information, in a form and format and at times specified by EOHHS, from all non-federal, non-state public hospitals in the Contractor's Network:

1) At the time of the midpoint evaluation specified by EOHHS:

a) Progress on certain behavioral health quality measures and related performance goals specified by EOHHS; and

b) Additional information as specified by EOHHS.

2) At the time of the year end evaluation specified by EOHHS:

a) Performance information on certain behavioral health quality measures specified by EOHHS; and

b) Additional information as specified by EOHHS.

b. Submit to EOHHS, at a time and in a manner specified by EOHHS:

1) The information the Contractor collected in accordance with **Section 2.7.F.4** above; and

2) A certification notifying EOHHS that, to the Contractor's knowledge, such information is accurate and complete.

c. Make value-based payments specified by EOHHS, pursuant to 42 CFR 438.6(c) and as specified by EOHHS, to such non-federal, non-state public hospitals. The Contractor shall make such payments to such providers

within 3 business days of receiving payment from EOHHS.

5. Clinical Quality Incentive for Acute Hospitals

The Contractor shall:

a. For each Contract Year, collect the following information, in a form and format and at times specified by EOHHS, from acute care hospitals that have executed the MassHealth Acute Care Hospital RFA (RFA):

1) At the time of the midpoint evaluation specified by EOHHS:

a) Progress on certain measures targeting clinical quality and related performance goals specified by EOHHS; and

b) Additional information as specified by EOHHS.

2) At the time of year end evaluation specified by EOHHS:

a) Performance information on measures targeting clinical quality specified by EOHHS; and

b) Additional information as specified by EOHHS.

b. Submit to EOHHS, at a time and manner specified by EOHHS:

1) The information the Contractor collected in accordance with **Section 2.7.F.5** above; and

2) A certification notifying EOHHS that, to the Contractor's knowledge, such information is accurate and complete.

c. Make value-based payments at a frequency specified by EOHHS, pursuant to 42 CFR 438.6(c) and as specified by EOHHS, to acute care hospitals that have executed the RFA. The Contractor shall make such payments to such providers within 14 calendar days of receiving payment from EOHHS.

6. Value-Based Payment (VBP)

a. The Contractor shall develop for EOHHS review and shall implement a multi-year VBP strategy with its Behavioral Health Network Providers focused on increasing its use of VBP methodologies aimed at meaningfully incentivizing providers to improve performance, resulting in enhanced experience of care for Covered Individuals and improved outcomes.

b. The Contractor shall implement a Pay for Reporting (HCP-LAN Category 2B) methodology during CY2023 to support provider reporting of identified Behavioral Health performance measures, including but not

limited to performance measures that EOHHS requires the Contractor to report. At a minimum, the Contractor shall establish these Pay For Reporting contracts in CY2023 with CBHCs and high-volume ATS and CSS treatment providers.

c. The Contractor shall utilize initial performance measure reporting results from providers received in CY2023 to identify benchmarks for specific measures to implement Pay for Performance (HCP-LAN Category 2C) as part of its provider contracts during CY2024.

d. The Contractor shall also encourage Behavioral Health providers to participate in VBP methodologies in which providers have the opportunity to share in savings based on improving health care quality and reducing costs. The Contractor shall work towards having an increasing amount of its provider contracts in a VBP model that falls within the HCP-LAN Category 3 or 4 models. At EOHHS' direction, Contractor shall implement specific VBP models.

e. The Contractor shall report on its progress in implementing VBP models with Network Providers on an annual basis, including reporting on numbers and types of providers with which the Contractor has entered into a VBP arrangement, the types of VBP models used according to the HCP-LAN APM Framework and how the Contractor has facilitated providers' ability to successfully meet VBP requirements including with timely, actionable data and other tools to support care delivery.

7. Non-Payment and Reporting

a. Non-Payment and Reporting of Serious Reportable Events (SREs)

1) The Contractor shall develop and implement a process for ensuring non-payment or recovery of payment for services when SREs occur. The Contractor's standards for non-payment or recovery of payment shall be, to the extent feasible, consistent with the minimum standards for non-payment for such events developed by EOHHS;

2) The Contractor shall notify EOHHS of SREs, in accordance with **Appendix E-1** and guidelines issued by the Department of Public Health (DPH); and

3) The Contractor shall provide, at a frequency and format specified by EOHHS, a summary of SREs in accordance with **Appendix E-1**. Such summary shall include the resolution of each SRE, if any, and any next steps to be taken with respect to each SRE;

b. Non-Payment and Reporting of Provider Preventable Conditions

1) The Contractor shall take such action as is necessary in order for EOHHS to comply with and implement all federal and state laws, regulations, policy guidance, and MassHealth policies and procedures relating to the identification, reporting, and non-payment of provider preventable conditions, including Section 2702 of the Patient Protection and Affordable Care Act and regulations promulgated thereunder;

2) In accordance with 42 CFR 438.3(g), the Contractor shall:

   a) As a condition of payment, comply with the requirements mandating Provider identification of Provider Preventable Conditions, as well as the prohibition against payment for Provider Preventable Conditions as set forth in 42 CFR 434.6(a)(12) and 447.26;

   b) Report all identified Provider Preventable Conditions in a form and format and frequency specified by EOHHS, including but not limited to any reporting requirements specified in accordance with **Appendix E-1**.

3) The Contractor shall develop and implement policies and procedures for the identification, reporting, and non-payment of Provider Preventable Conditions. Such policies and procedures shall be consistent with federal law, including but not limited to 42 CFR 434.6(a)(12), 42 CFR 438.3(g), and 42 CFR 447.26, and guidance and be consistent with EOHHS policies, procedures, and guidance on Provider Preventable Conditions. The Contractor's policies and procedures shall also be consistent with the following:

   a) The Contractor shall not pay a Provider for a Provider Preventable Condition;

   b) The Contractor shall require all Providers to comply with all instructions set forth in All Provider Manuals Appendix V: MassHealth Billing Instructions for Provider Preventable Conditions;

   c) The Contractor shall require, as a condition of payment from the Contractor, that all Providers comply with reporting requirements on Provider Preventable Conditions as described at 42 CFR 447.26(d) and as may be specified by the Contractor and/or EOHHS;

   d) The Contractor shall not impose any reduction in payment for a Provider-Preventable Condition when the condition

defined as a Provider-Preventable Condition for a particular Enrollee existed prior to the Provider's initiation of treatment for that Enrollee;

e) A Contractor may limit reductions in Provider payments to the extent that the following apply:

(i) The identified Provider-Preventable Condition would otherwise result in an increase in payment; and

(ii) The Contractor can reasonably isolate for nonpayment the portion of the payment directly related to treatment for, and related to, the Provider-Preventable Condition;

f) The Contractor shall ensure that its non-payment for Provider- Preventable Conditions does not prevent Enrollee access to services;

c. Non-Payment and Reporting of Preventable Hospital Readmissions

As directed by EOHHS, the Contractor shall develop and implement a process for ensuring non-payment or recovery of payment for preventable hospital readmissions. Such process shall be, to the extent feasible, consistent with minimum standards and processes developed by EOHHS.

G. Provider Directory and Other Information

1. The Contractor shall maintain a BH Provider directory (or directories) as further specified by EOHHS. Such directory (or directories) shall include Behavioral Health Providers, hospitals, specialists, sub-specialists, and ancillary service Providers, including a listing of statewide emergency rooms and CBHCs, that is made available in Prevalent Languages and Alternative Formats, upon request, and includes, at a minimum, the following information:

a. Alphabetical Provider list, including any specialty and group affiliation as appropriate;

b. Geographic list of Providers by town;

c. Office address and telephone numbers for each Provider, as well as website URL as appropriate;

d. Office hours for each Provider;

e. The Provider's Cultural and Linguistic Competence and capabilities, including languages spoken by Provider or by skilled medical interpreter at site, including ASL, and whether the Provider has completed cultural competence training;

f. Which accommodations the Provider's office or facility has for people with physical disabilities, including offices, exam rooms, and equipment;

g. Qualifications and licensing information, and special experience, skills, and training (i.e., trauma, child welfare, substance use); and

h. For ancillary services Providers: 1) Alphabetical Provider list; and 2) Geographic list of Providers by town.

i. Whether the Provider is accepting new patients.

j. Whether the Provider offers services via telehealth.

2. The Contractor shall provide EOHHS with an updated electronic submission of its Provider directory (or directories) on a semi-annual basis, if updated, and an electronic submission of changes to the Provider Network monthly.

3. The Contractor shall provide the Provider directory to its Covered Individuals as follows:

a. The Contractor shall provide a copy in paper form to Covered Individuals upon request. The Contractor shall update its paper-version of its Provider directory monthly if the Contractor does not have a mobile-enabled, electronic directory as further specified by EOHHS and quarterly if the Contractor has such mobile-enabled electronic directory as further specified by EOHHS;

b. The Contractor shall include written and oral offers of such Provider directory in its outreach and orientation sessions for New Covered Individuals; and

c. The Contractor shall include an electronic copy of its Provider directory on the Contractor's website in a searchable machine-readable file and format. The Contractor shall update its electronic version of its Provider directory no later than 30 calendar days after being made aware of any change in information.

4. As requested by EOHHS, the Contractor shall, in a form and format specified by EOHHS, report to EOHHS its Network Providers and whether each provider is enrolled as a MassHealth provider;

5. The Contractor shall develop, maintain and update information about Behavioral Health Providers with areas of special experience, skills, and training including, but not limited to, Providers with expertise in treating: children, adolescents, people with HIV, homeless persons, people with disabilities, people with Autism Spectrum Disorder, people with early psychosis, people who are deaf or hard-of hearing, people who are blind or visually impaired, and children in the care or custody of DCF or youth affiliated with DYS (either detained or committed). The

Contractor shall make available to EOHHS and Covered Individuals such information upon request.

6. The Contractor shall provide to a Covered Individual directly, or through referral, publicly available information maintained by the Massachusetts Board of Registration in Medicine (BORIM) and the National Practitioner Databank on the malpractice history of any Provider(s), upon a Covered Individual's request;

7. The Contractor shall demonstrate to EOHHS, by reporting annually in accordance with **Appendix E-1**, that all Providers within the Contractor's Provider Network are credentialed according to **Section 2.8.G**. of the Contract;

8. Provider Network Changes

   a. The Contractor shall provide notice to EOHHS of significant changes (additions or deletions) in the operations of the Provider Network and significant to the Provider Network itself, that will affect the adequacy and capacity of services. At the time of any change that (a) prevents the Contractor from complying with **Sections 2.7.A. and B**; or (b) is considered significant pursuant to **Section 2.8.H.8.b** below, the Contractor shall provide immediate written notice to EOHHS, with the goal of providing notice to EOHHS at least 60 days prior to the effective date of any such change. Such notice shall be in the form and format specified by EOHHS and the Contractor shall provide EOHHS will all requested information about the significant change;

   b. Significant changes requiring notification include, but are not limited to, the following:

      1) Changes in the operations of the Provider Network that result from EOHHS changes in BH Covered Services, and Provider or Material Subcontractor payment methodology;

      2) Enrollment of a new population in the Contractor's Plan;

      3) Any termination or non-renewal of a hospital, community health center or community mental health center contract;

      4) Any termination or non- renewal of a Behavioral Health Provider or specialist contract that results in there being no other, or a limited number of, Behavioral Health Providers or specialists available in a particular part of the Region; or

      5) Any termination or non-renewal of a Behavioral Health Provider or specialist contract that results in there being no other, or a limited number of Behavioral Health Providers or specialists available within a service area.

c. The Contractor shall provide any information requested by EOHHS pertaining to any such significant change within seven calendar days of the request;

d. For Behavioral Health Provider Network significant changes, the Contractor shall notify EOHHS of the number of affected Covered Individuals, and the specific steps the Contractor is taking to assure that such Covered Individuals continue to have access to Medically Necessary Services;

e. The Contractor shall provide to EOHHS a written summary of all significant change(s) with its next Annual Summary of Access and Availability report set forth in **Appendix E-1**, and in the timeframes specified in **Appendix E-1**, that describes the issues, the steps taken to date to assure that Covered Individuals have access to Medically Necessary services, and any relevant next steps; and

f. In the event that a Provider leaves or is terminated from the Contractor's Network, the Contractor shall follow the process set forth by EOHHS for communicating with and, as appropriate, transitioning Covered Individuals affected by the termination. Such process shall include developing a member communication and outreach plan and a provider communication and outreach plan, and performing other activities EOHHS determines necessary;

9. The Contractor shall establish and sustain a publicly accessible, standards-based Provider directory application programming interface (API) in accordance with federal law, including but not limited to the Consolidated Appropriations Act, 2023 and the CMS Interoperability and Patient Access final rule.

H. Community Behavioral Health Center (CBHC) Program

1. CBHC Implementation and Operations

The Contractor shall, as directed by EOHHS, take all steps and perform all activities necessary to support the successful implementation and ongoing operations of the CBHC program, which shall include, without limitation, participation in meetings and workgroups, including joint workgroups with all MassHealth-contracted managed care entities to develop coordinated network management and quality improvement strategies for all payers and other tasks as directed.

2. Contracting with CBHCs

The Contractor shall execute and maintain contracts with CBHCs identified in **Appendix A-2, Exhibit 1,** and pay CBHCs no less than the payment rates

established by EOHHS in 101 CMR 305.000 and shall use procedure codes as directed by EOHHS to provide payment for services rendered by CBHCs.

3. CBHC Service Authorization

The Contractor shall not require prior authorization for any services provided under the CBHC program.

4. Management of CBHC Network

The Contractor shall:

a. Ensure that CBHCs provide services in accordance with all EOHHS-approved performance specifications and Medical Necessity criteria.

b. Ensure that appropriate members of the CBHCs' staff participate in CBHC training, coaching, and mentoring as approved by EOHHS for CBHC training. The Contractor shall ensure that such members of CBHCs' staffs utilize evidence-based practice in service delivery.

c. Develop operational manuals for selected CBHC services, including but not limited to AMCI and YMCI.

d. Perform quality assurance and training activities for CBHCs as directed by EOHHS.

e. Work collaboratively with all MassHealth payers to manage the network of all CBHCs by:

1) Coordinating regional and statewide meetings for all CBHC components that include all MassHealth-contracted payers, at a frequency agreed to annually by EOHHS. The Contractor shall coordinate and pay for administrative costs associated with such meetings; and

2) Coordinating with all MassHealth-contracted payers to provide joint technical assistance and network management to specific CBHC providers as necessary to address quality improvement and ensure full program implementation, and to monitor ongoing program operations and outcomes.

f. Assign a point of contact for management for each CBHC to provide technical assistance to CBHCs as needed and to monitor individual CBHC performance.

g. Require CBHCs to track and report monthly to the Contractor on each component service. The reported data shall include information for all MassHealth Members using these services, regardless of the member's managed care enrollment.

h. In collaboration with, and as further directed by EOHHS, develop a plan to ensure the quality of CBHC component services, including but not limited to access and availability.

5. CBHC Policies and Procedures

For CBHC providers under contract with the Contractor, the Contractor shall:

a. Ensure that CBHCs provide Covered Individuals with unrestricted statewide access, and that Uninsured Individuals, persons covered by Medicare only, and Individuals without Mobile Crisis Coverage who are experiencing a behavioral health crisis are provided with unrestricted state-wide access to AMCI and YMCI services, Community Crisis Stabilization, and up to three units of outpatient CBHC bundle services immediately in response to a Behavioral Health crisis, on a 24-hour basis, seven days a week;

b. Share with MassHealth-contracted managed care entities and PCC Plan Providers any changes and/or updates to the CBHC provider network prior to disseminating that information to all Covered Individuals.

c. Ensure that all CBHC providers set forth in **Appendix A-2, Exhibit 1** provide all components of the CBHC program in accordance with the Contract and in a manner that is consistent with the Contractor's performance specifications and maximizes utilization of community-based diversion strategies.

d. The Contractor shall require CBHCs to implement the CBHC program to meet EOHHS' vision, including providing readily available outpatient Behavioral Health evaluation and treatment in community-based locations.

e. Ensure that CBHC services are available on site at all community-based locations for minimum of 12 hours per day on weekdays and 8 hours per day on weekends;

f. Ensure that the response time for face-to-face community crisis evaluations does not exceed one hour from notification of the need, or, in the case of referrals from hospital emergency departments, does not exceed the time set forth in the applicable agreement between the CBHC and the hospital, as approved by EOHHS;

g. Ensure that CBHCs provide Covered Individuals with 24-hour-a-day access to clinicians who have special training or experience in providing Behavioral Health services for:

1) the full array of Behavioral Health conditions;

2) children and adolescents (clinicians providing Youth CI must be child-trained clinicians who meet competency standards as defined in the Contractor's performance specifications);

3) individuals with substance use conditions or a Dual Diagnosis;

4) individuals with intellectual disabilities, developmental disabilities, or autism spectrum disorders; and

5) older adults;

h. Ensure that CBHCs include Recovery Coaches as part of their team to provide non-judgmental, non-clinical recovery support to individuals in a SUD crisis.

i. At the direction of EOHHS, identify and implement strategies to maximize utilization of community-based diversion services and reduce unnecessary psychiatric hospitalization, in a manner that is consistent with medical necessity criteria. Such strategies shall support providers in shifting the volume from hospital EDs to community-based settings.

j. Establish policies and procedures to ensure that all Covered Individuals receive AMCI or YMCI provided by a CBHC or a crisis evaluation provided at a hospital prior to hospital admissions for Inpatient Mental Health Services to ensure that the Covered Individuals have been evaluated for diversion or referral to the least restrictive appropriate treatment setting. The Contractor's policies and procedures shall:

1) Require that the CBHC located in the geographic area where the individual is physically located perform the AMCI or YMCI;

2) Not require prior authorization to provide a Crisis Intervention and Assessment;

3) Develop contract standards, reviewed and approved by EOHHS annually, and monitor CBHCs' performance to minimum standards and goals for diversionary rates on:

a) providing same day treatment for Urgent Care,

b) expanded weekend and evening hours,

c) diversion and inpatient admission rates,

d) timeliness of assessment, and

e) rate of community-based AMCI or YMCI

4) Authorize Medically Necessary BH Covered Services within 24 hours following a AMCI or YMCI encounter.

k. Require and ensure that CBHCs have arrangements, agreements or procedures to coordinate care with Network Providers, MassHealth managed care entities, DMH area and site offices, DCF regional offices, and DYS regional offices in the geographic area they serve;

l. Require and ensure that CBHCs make all reasonable attempts to work with local police and EMS to develop models of mutual response to Behavioral Health Emergencies maximizing the value of the 24/7 community based locations when needed. These models may include the delivery of services via telehealth when clinically appropriate.

m. Collaborate with EOHHS regarding CBHC network management and CBHC policy development, including participation in meetings and workgroups, the development and implementation of new policies, and any other tasks as directed by EOHHS.

n. Develop targeted performance measures for CBHCs as approved by EOHHS. Using these performance measures, the Contractor shall develop a baseline performance level for each CBHC provider, and regularly track performance.

6. CBHC Administrative Oversight

The Contractor shall coordinate the administration and management of the CBHCs as specified in this Contract and as further directed by EOHHS. In this role, the Contractor shall:

a. Facilitate at least six (6) statewide meetings each Contract Year, or otherwise as directed by EOHHS, with contracted CBHCs, and invite the participation of MassHealth managed care plans, to support consistency in service delivery;

b. Require CBHCs to refer adult Uninsured Individuals and persons with Medicare only to available beds in psychiatric units of general hospitals first, if beds in such hospitals are available and clinically appropriate, before referring them to psychiatric hospitals;

c. After a court clinician has conducted a psychiatric evaluation pursuant to M.G.L. c. 123 § 12(e), ensure that upon request of such court clinician:

1) CBHCs provide AMCI and YMCI to all Covered Individuals (including onsite mobile evaluations at the court);

2) Identify to the court clinician appropriate diversions from inpatient hospitalization, and assist court clinicians to develop any plan to utilize such diversions. Nothing in this provision shall be construed

as establishing a court clinician evaluation as a prerequisite to an onsite mobile evaluation at the court; and

3) If the court orders the admission of an individual under M.G.L. c. 123 § 12(e), CBHCs conduct a search for an available bed, making best efforts to locate such a bed for the individual by 4:00 p.m. on the day of the issuance of such commitment order. If a bed is not found by 4:00, the CBHC will work with the court clinician to ensure appropriate disposition and transfer of the individual to a safe place outside of the court setting.

d. Adopt the existing Massachusetts Behavioral Health Access System, or adopt such other system as directed by EOHHS, that helps CBHCs and hospital EDs to search on-line for available Inpatient Mental Health Services, Inpatient Substance Abuse Services, 24-hour Diversionary Services and CBHI Services.

1) The system shall provide on-line web access on a 24-hour basis, seven days per week.

2) The Contractor shall ensure that the web-based system is updated at least once every eight hours for 24-hour services, and at least weekly for CBHI Services (Intensive Care Coordination, In-Home Behavioral Services, Therapeutic Mentoring, In-Home Therapy, Family-based Intensive Treatment).

3) The Contractor shall develop an annual report (with specifications subject to EOHHS review and prior approval) that tracks utilization of the Massachusetts Behavioral Health Access System and other data as agreed to by the parties.

7. Monitoring CBHC Performance

The Contractor shall:

a. Have policies and procedures to monitor the CBHC's performance with respect to established diversion and inpatient admission rates;

b. Have policies and procedures to monitor the CBHC's performance with respect to diverting encounters with Covered Individuals from hospital EDs to the CBHC's community-based location or other community settings;

c. Have policies and procedures regarding the circumstances under which CBHCs shall contact the Contractor for assistance in securing an inpatient or 24-Hour Diversionary Service placement. Such policies and procedures shall include that if a CBHC requests the Contractor's assistance in

locating a facility that has the capacity to timely admit the Covered Individual, the Contractor shall contact Network Providers to identify such a facility or, if no appropriate Network Provider has such capacity, shall contact out-of-network Providers to identify such a facility;

d. Have policies and procedures to ensure collaboration between YMCI teams, Community Service Agencies (CSAs), and other youth serving Providers;

e. Have a plan in place to direct Covered Individuals to the least intensive but clinically appropriate service;

f. Have a process to ensure placement for Covered Individuals who require Behavioral Health Inpatient Services when no inpatient beds are available, as described in **Section 2.5.K**;

g. Utilize standardized documents such as risk management/safety plans as identified by EOHHS;

h. Convene meetings to address clinical and administrative issues with CBHCs and to enhance the coordination of care for Covered Individuals;

i. Convene meetings with MassHealth MCOs, ACOs, and EOHHS and CBHCs, as directed by EOHHS;

8. Encounter Forms

The Contractor shall:

a. Create and implement an EOHHS-approved electronic CBHC Encounter form to report on Services provided by CBHCs described in **Appendix A-1**;

b. Require CBHCs to complete and submit the electronic EOHHS-approved CBHC Encounter form for each individual they serve;

c. Work with EOHHS to develop CBHC reporting metrics consistent with the CBHC Encounter data; and

d. Develop reporting procedures, approved by EOHHS, to include but not limited to the following:

1) Monthly CBHC Dashboard including all component services;

2) Monthly network management meeting list; and

3) Standard process for reporting quality issues to EOHHS, including notification of any CBHC provider on a corrective action.

9. Use of Technology

The Contractor shall require CBHC providers to adopt technology to support community-based diversion including:

a. Technology that supports decentralized staffing models and remote dispatch;

b. HIPAA compliant two-way interactive audio-video for services provided via telehealth (e.g., phone, tablet, video conferencing); and

c. Call center technology that includes real-time data dashboard to track staff availability, staff dispatch, stage of crisis, CCS bed census, detail about referral sources, and other metrics as determined by EOHHS.

I. [Reserved]

J. Children's Behavioral Health Initiative (CBHI)

1. CBHI Training and Quality Improvement

a. The Contractor shall:

1) As directed by EOHHS, take all steps and perform all activities necessary to improve the CBHI services, which shall include, without limitation, participation in meetings and workgroups, including joint workgroups with all MassHealth Managed Care payers to develop coordinated network management and quality improvement strategies for all payers on these services and other tasks as directed; and

2) Review records for Intensive Care Coordination, Family Support and Training, In-Home Therapy, In-Home Behavioral Services, and Therapeutic Mentoring when a significant quality concern has been identified by the Contractor or EOHHS, in addition to reviewing the training and supervision logs of staff.

2. Use of the CANS Tool

The Contractor shall ensure the continued use of the CANS Tool by all Behavioral Health Service providers that are required to use it (see **Section 2.7.B**), as directed by EOHHS. The Contractor shall:

a. Pay EOHHS approved rates for initial Behavioral Health Clinical Assessments using the CANS Tool for Covered Individuals under the age of 21 as described in **Section 2.7.B.5.a**;

b. Ensure that it pays only Network Providers whose servicing clinicians are certified in the CANS Tool for providing Behavioral Health Clinical Assessments using the CANS Tool;

c. Ensure that Providers of Behavioral Health Clinical Assessments using the CANS Tool bill for these assessments. The review and updating of the CANS assessment that is required at a minimum every 180 days for Covered Individuals in ongoing individual, group, or family therapy is part of the treatment planning and documentation, and as such, is not a separately billable service.

d. Ensure that its customer services representatives who respond to questions from Network Providers are informed about the requirements and process for applicable Network Providers to become trained and certified in administering the CANS Tool and can respond to questions from Network Providers about these requirements and processes. The Contractor shall provide training to its newly hired and existing customer services representatives about when, where and how Network Providers obtain CANS training and certification, and shall provide refresher trainings as directed by EOHHS and as the Contractor determines is necessary.

e. Ensure that its customer services representatives who are assigned to respond to inquiries from Covered Individuals are informed about the use of the CANS and other CBHI Services, and can respond to Covered Individuals' questions about them. The Contractor shall provide training to its newly hired and existing customer services representatives about the CANS Tool and how it is generally used in Behavioral Health Clinical Assessments and during the Discharge Planning process from Inpatient Psychiatric Hospitalizations, Intensive Community-Based Acute Treatment Services, and Community-Based Acute Treatment Services, and Transitional Care Units.

f. As directed by EOHHS, ensure that Covered Individual materials, including but not limited to the Handbook for Covered Individuals, describe the CANS Tool and its use in Behavioral Health Clinical Assessments and during the Discharge Planning process from Inpatient Psychiatric Hospitalizations, Intensive Community-Based Acute Treatment Services, and Community-Based Acute Treatment Services for Covered Individuals under the age of 21.

g. As directed by EOHHS, ensure that appropriate Network Provider materials exist to describe the CANS Tool, the requirements and process for CANS Tool training and certification, and the CANS IT System.

h. Be able to access and use the CANS IT System and data contained therein to integrate with clinical data, and use in reporting as directed by EOHHS.

i. Participate in any testing or development processes necessary for EOHHS to develop and refine the CANS IT System.

3. CBHI Procedure Codes

The Contractor shall use procedure codes as directed by EOHHS to provide payment for CBHI services.

4. CBHI Service Authorization

a. The Contractor shall inform EOHHS in writing of its authorization procedures for Behavioral Health Covered Services for Covered Individuals under 21 who are receiving CBHI Services, and of any changes to such authorization procedures prior to their implementation. The Contractor shall assist Network Providers in learning how to utilize Contractor's authorization procedures for CBHI Services. The Contractor shall monitor its authorization procedures to ensure that the procedures provide for timely access to services. In the event that the Contractor's authorization procedures for CBHI Services result in delays or Barriers to accessing Medically Necessary BH Covered Services, the Contractor shall modify such authorization procedures. The Contractor shall coordinate with other MassHealth payers to publish a single document that describes the authorization procedures for all MassHealth payers for these services.

b. The Contractor shall ensure that the authorization procedures established for Intensive Care Coordination (ICC) and Family Support and Training (FS&T) allow for at least the first 45 days of services to be provided without prior approval. The Contractor may establish notification or registration procedures during the first 45 days of ICC.

c. The Contractor shall ensure that its authorization procedures comply with all provisions of **Section 2.6.C** of the Contract and, in addition, that all authorization approvals for ICC and FS and T are provided telephonically or electronically.

d. Effective September 1, 2025, the Contractor shall complete length of stay record reviews as directed by EOHHS for Members receiving Intensive Care Coordination, In-Home Therapy, Family Support & Training, In-Home Behavioral Service or Therapeutic Mentoring.

5. Management of CBHI Service Provision

The Contractor shall:

a. Ensure that Network Providers of CBHI Services provide each such service in accordance with all EOHHS-approved CBHI Services Performance Specifications and CBHI Services Medical Necessity criteria.

b. Ensure that appropriate members of Providers' staffs participate in CBHI training, coaching, and mentoring as approved by EOHHS for CBHI

training. The Contractor shall ensure that such members of Providers' staffs complete CBHI training, and utilize their new skills in service delivery. If the Provider is not participating in CBHI training, the Contractor shall engage in Provider Network management activities to increase training.

c. Maintain operational manuals for selected CBHI services.

d. Perform quality assurance and training activities for CBHI services as directed by EOHHS. These activities shall include providers within the networks of MassHealth Managed Care entities who provide CBHI Services.

e. Work collaboratively with all MassHealth payers to manage the network of all CBHI Service providers, including the Community Service Agencies (CSAs) that provide ICC, Family-based Intensive Treatment, and Family Support and Training, as well as the providers of In-Home Therapy, In-Home Behavioral Services and Therapeutic Mentoring, by:

    1) Coordinating regional and statewide meetings for all CBHI service types that include all MassHealth payers, at a frequency agreed to annually by EOHHS. Contractor is responsible for coordination and administrative costs associated with such meetings; and

    2) Coordinating with all MassHealth payers to provide joint technical assistance and network management to all contracted CBHI providers as necessary to address quality improvement and ensure full program implementation.

f. Manage the current, transitioning, and newly contracted Community Service Agencies that are contracted to deliver Intensive Care Coordination, Family Support and Training, and Family-based Intensive Treatment services. Any changes to the CSA network must be approved in advance by EOHHS.

g. Maintain, revising as necessary and submitting to EOHHS for approval whenever revised, the Intensive Care Coordination and Family Support and Training Operations Manual (ICC Ops Manual). The Contractor shall ensure that the ICC Ops Manual conforms to the EOHHS-approved performance specifications for ICC and Family Support and Training. The Contractor shall distribute the EOHHS-approved ICC Ops Manual to all CSAs in the Network.

h. Ensure that CSAs provide ICC and Family Support and Training services according to both the EOHHS-approved performance specifications and the EOHHS-approved ICC Ops Manual. In the event that there are

discrepancies between the two documents, the performance specifications shall control and the Contractor shall notify EOHHS of any discrepancies and submit a correction for EOHHS approval.

i. Assign a point of contact for management for each CSA and identify such individual to EOHHS prior to the Operational Start Date. Responsibilities shall include, but are not limited to, providing technical assistance to CSAs to answer questions regarding authorization of services and assisting CSAs in facilitating and ensuring that Network Providers engaged in a Covered Individual's treatment participate in ICC Individual Care Plan Team (CPT) meetings.

j. Require CSAs to track and report monthly to the Contractor on ICCs and referrals to ICC and FIT services according to the template provided in the ICC Ops Manual. The reported data shall include information for all MassHealth Members using these services, regardless of the Member's managed care enrollment.

k. Require CSAs to provide the Contractor with EOHHS-required data for a particular month in sufficient time to submit such reports to EOHHS by the 30th of the following month (or by the next business day after the 30th if the 30th falls on a weekend day).

l. Ensure that each CSA coordinates and maintains a local Systems of Care committee to support the CSA's efforts to establish and sustain collaborative partnerships among families and community stakeholders in its geographic area. The Contractor shall assign a staff person to oversee the local Systems of Care committees; the staff person's responsibilities shall include but are not limited to:

    1) attending meetings of the Systems of Care committees on a quarterly basis;

    2) monitoring System of Care committees' activities and issues through review of meeting minutes; and

    3) conducting network management meetings with the CSAs.

m. In collaboration with, and as further directed by EOHHS, develop a plan to ensure that the quality of ICC and Family Support and Training services is measured using tools that are consistent with national Wraparound standards, such as the Wraparound Fidelity Index tool, and provide CSAs with such fidelity tools at no cost to the CSAs. In addition, use tools approved by EOHHS to review medical files in both Intensive Care Coordination and In Home Therapy.

n. In collaboration with and as further directed by EOHHS, develop a process to monitor the quality of services using tools such as the MA DRM or another tool approved by EOHHS to evaluate the adequacy of medical record keeping for both ICC and In-Home Therapy Services (IHT). The Contractor shall apply the approved quality-assessing tool at least annually on a mix of ICC and IHT services provided across all of the Contractor's regions. Unless otherwise directed by EOHHS, the Contractor shall use the approved quality assessing tool(s) to evaluate at least 10% of the Covered Individuals who have received ICC or IHT during the applicable Contract Year, except that the Contractor shall not be required to review more than 10 Covered Individuals medical files per region per Contract Year.

6. CBHI Access Reporting

The Contractor shall ensure that the web-based Behavioral Health Access System or the Contractor's equivalent system, as referenced in **Section 2.7.H.6.d** above, is updated at least once a week for CBHI Services (ICC, FIT, IHBS, TM and IHT) to show access and availability.

a. CBHI Service reporting must be available to the public on the system.

b. CBHI access and availability reports must be reported monthly from this system.

7. The Contractor shall continue collaborative work focused on the Children's Behavioral Health Initiative. This collaborative work with EOHHS shall enhance the integration of care and the delivery of services for covered individuals according to the following:

a. As directed by EOHHS issue a Request For Proposal (RFP) to procure CSA providers as defined by EOHHS.

b. As directed by EOHHS, and in collaboration with EOHHS, select providers to be CSAs.

c. In consultation with EOHHS, and as further directed by EOHHS, execute provider agreements with each selected provider for each service area designated by EOHHS. Such provider agreements shall require CSAs to conform to the Performance Specifications for Intensive Care Coordination (ICC), Family Support and Training (FS&T), and Family-based Intensive Treatment (FIT). The Contractor will use the performance specifications and medical necessity criteria documents approved by EOHHS in contracting.

d. Work with EOHHS to produce a workplan to encompass the following deliverables to be executed by July 31, 2025, unless otherwise modified

by EOHHS:

1) Conduct two to three working sessions convening key stakeholders from across EOHHS and other relevant agencies, including the Department of Children and Families (DCF), Department of Public Health (DPH), Department of Mental Health (DMH), Department of Developmental Services (DDS), Department of Youth Services (DYS) and the Massachusetts Commission for the Deaf and Hard of Hearing (MCDHH).

2) Develop detailed performance specifications and medical necessity guidelines, quality metrics and credentialing requirements based on the Program Specifications provided by EOHHS.

3) As further specified by EOHHS, contract with CSAs by July 31, 2025, or on a date specified by EOHHS.

K. Restoration Center

The Contractor shall make available Restoration Center services to Covered Individuals as further directed by EOHHS. The Contractor shall:

1. Execute and maintain contracts with Restoration Center providers;

2. Pay for BH Covered Services rendered at Restoration Centers to Covered Individuals; and

3. Take all steps and perform all activities necessary to maintain contracts with Restoration Centers, including, without limitation, participation in meetings and workgroups, the development and implementation of new policies, and any other tasks as further directed by EOHHS.

L. Special Service Initiatives

1. During the term of the Contract, the Contractor shall propose for EOHHS's review and approval special new services and programs for Covered Individuals for which the Contractor may need to adapt its Provider Network. The Contractor shall perform a cost-benefit analysis for any new service it proposes to develop, as directed by EOHHS, including whether the proposed services would have an impact on Base PMPM Capitation Rates or the Administrative Component of the MassHealth Capitation Payment. The Contractor shall implement new special services and programs as approved by EOHHS.

2. As directed by EOHHS, the Contractor shall support the ongoing development and implementation of structural reforms to the clinical design and delivery of clinic-based outpatient Behavioral Health and CBHC services with the goals of

achieving integrated care for mental health and addiction, open access to Behavioral Health Urgent Care inclusive of prescribing, and improved community-based crisis response. Activities to be performed by the Contractor at the direction of EOHHS may include, but not be limited to:

a. Stakeholder engagement activities;

b. Request for information from providers;

c. Revision of provider performance specifications; and

d. Provider contracting, oversight and/or procurement related activities.

M. [Reserved]

N. M-CAAP Training

The Contractor shall collaborate with MASOC (Massachusetts Society for a World Free of Sexual Harm by Youth) in the development and delivery of training of clinicians about the Massachusetts Child and Adolescent Assessment Protocol (M-CAAP) for sexual behaviors. The training shall include the delivery of an in person, one day training on the assessment and treatment of sexualized behavior in children and adolescents

O. Middlesex County Restoration Center Planning Grants

The Contractor shall administer a planning grant program for Community Behavioral Health Centers (CBHCs) in Middlesex County to fund such CBHCs' preparation for and development of community support for the future launch of the Middlesex County Restoration Center pilot program at the direction of the Executive Office of Health and Human Services, ensuring that providers receiving these grants:

1. Serve cities or towns in Middlesex County;

2. Initiate at least one activity that supports each objective included in the SAMHSA Congressional Directive Spending Award by July 28, 2023;

3. Provide a progress report by August 15, 2023, and a final report by October 13, 2023, to the Contractor;

4. Commit to coordinate with and support the Restoration Center once it is launched, regardless of whether the CBHC receiving the grant is selected to operate the Restoration Center; and

5. Affirm that they will not use the planning grant funds to develop a response to the Executive Office of Health and Human Services' RFR for a Middlesex County Restoration Center pilot program or to supplant any other current funding source.

P. Youth Community Crisis Stabilization (YCCS)

1. YCCS Implementation and Operations

a. The Contractor shall, as directed by EOHHS, perform all activities necessary to support the successful implementation and ongoing operations of the YCCS program, which shall include, without limitation:

1) Include in its provider network YCCS providers as described in **Appendix A-2, Exhibit 1** and as directed by EOHHS;

2) Execute contracts with providers of YCCS;

3) Participate in meetings and workgroups with all MassHealth-contracted managed care entities to develop coordinated network management and quality improvement strategies for all payers and other tasks as directed;

4) Implement performance specifications as specified by EOHHS and ensure compliance with such specifications; and

5) Pay providers in accordance with **Section 2.7.F.3.k**.

2. Management of the YCCS Network

The Contractor shall:

a. Ensure that YCCS providers provide services in accordance with all EOHHS approved performance specifications and Medical Necessity criteria.

b. Ensure that appropriate YCCS staff members participate in CBHC training, coaching, and mentoring as approved by EOHHS for CBHC and YCCS training. The Contractor shall ensure that such YCCS staff members utilize evidence-based practice in service delivery.

c. Perform quality assurance and training activities for YCCS providers as directed by EOHHS.

d. Work collaboratively with all MassHealth payers to manage the network of all YCCS providers by:

1) Including YCCS providers in coordinating regional and statewide meetings for CBHC and YCCS providers that include all MassHealth-contracted payers, at a frequency agreed to annually by EOHHS. The Contractor shall coordinate and pay for administrative costs associated with such meetings.

2) Coordinating with all MassHealth-contracted payers to provide joint technical assistance and network management to specific YCCS providers as necessary to address quality improvement and ensure full program implementation, and to monitor ongoing program operations and outcomes.

3) Assigning a point of contact for management for each YCCS to provide technical assistance to YCCS providers as needed and to monitor individual YCCS performance.

4) Requiring YCCS providers to track and report monthly to the Contractor on the services provided. The reported data shall include information for all MassHealth members using these services, regardless of the member's managed care enrollment.

5) In collaboration with, and as further directed by EOHHS, developing a plan to ensure the quality of YCCS services, including but not limited to access and availability.

3. YCCS Policies and Procedures

The Contractor shall:

a. Ensure that all YCCS providers provide all components of the YCCS program in accordance with the Contract and in a manner that is consistent with the Contractor's performance specifications and maximizes utilization of community-based diversion strategies;

b. Require YCCS providers to implement the YCCS program to meet EOHHS' vision;

c. Require and ensure that YCCS providers have arrangements, agreements or procedures to coordinate care with Network Providers, MassHealth managed care entities, DMH area and site offices, DCF regional offices, and DYS regional offices in the geographic area they serve;

d. Collaborate with EOHHS regarding YCCS network management and YCCS policy development, including participation in meetings and workgroups, the development and implementation of new policies, and any other tasks as directed by EOHHS; and

e. Develop targeted performance measures for YCCS sites as approved by EOHHS. Using these performance measures, the Contractor shall develop a baseline performance level for each YCCS provider, and regularly track performance.

4. Monitoring YCCS Performance

The Contractor shall:

a. Maintain policies and procedures to ensure collaboration between YCCS providers, YMCI teams, Community Service Agencies (CSAs), and other youth serving Providers;

b. Utilize standardized documents such as risk management/safety plans as identified by EOHHS;

c. Convene meetings to address clinical and administrative issues with YCCS providers and to enhance the coordination of care for Covered Individuals; and

d. Convene meetings with MassHealth MCOs, ACOs, and EOHHS and YCCS providers, as directed by EOHHS.

Q. For Applied Behavior Analysis (ABA), the Contractor shall:

a. As further directed by EOHHS, collaborate on EOHHS' efforts to improve network performance and provider capacity;

b. Ensure that ABA is provided in accordance with EOHHS approved ABA performance specifications and ABA Medical Necessity Criteria, as further specified by EOHHS;

c. In accordance with **Section 2.6.C** submit authorization and utilization management policies and procedures for ABA to EOHHS upon request. The Contractor shall make changes to such policies and procedures if directed by the EOHHS; and

d. Require all ABA Providers to maintain an accredited status with a nationally recognized accreditation body specialized in ABA and track status as further directed by EOHHS. Additionally, the Contractor shall:

1) No later than December 31, 2026, require that all ABA Providers who offer center-based ABA Services obtain accreditation with a nationally recognized accreditation body specialized in ABA;

2) No later than December 31, 2027, require that all ABA Providers obtain and maintain accreditation status with a nationally recognized accreditation body specialized in ABA;

3) Maintain records of any ABA Providers who sought and were denied accreditation and provide a summary of the most recent accreditation review to EOHHS upon the ABA Provider accreditation denial notification, including but not limited to:

a) Accreditation results;

b) Recommended actions;

c) Recommended improvements;

d) Corrective action plans; and

e) Expiration date of accreditation.

Section 2.8 BH Provider Network and Network Management

A. Establishment of BH Provider Network

As of the Operational Start Date, the Contractor shall have in effect and maintain a Network of Providers for the delivery of BH Covered Services set forth in **Appendix A-1**, in accordance with the terms of this Contract.

The Contractor shall:

1. Make best efforts to ensure that all network providers in good standing from the previous BH contract continue to participate in the Contractor's Provider Network and, accordingly, renew or execute, prior to the Operational Start Date, Provider Agreements with all such network providers.

2. Ensure that all Provider Agreements the Contractor initially executes with network providers from the previous BH contract are for a term of at least one year unless the Contractor obtains approval from EOHHS for a shorter time period.

3. Enter into Provider Agreements effective no later than January 3, 2023, with each CBHC identified in **Appendix A-2, Exhibit 1** to provide all CBHC component services (including Behavioral Health Urgent Care, AMCI, YMCI, Adult CCS and YCCS) and each Community Service Agency (CSA) identified in **Appendix A-2, Exhibit 9** to provide Intensive Care Coordination and Family Support and Training Services.

4. [Reserved]

5. No later than three months prior to the Operational Start Date, or as otherwise agreed to by EOHHS, submit to EOHHS for its review and approval the Contractor's initial Provider Network. The Contractor shall submit to EOHHS for review and approval the new BH Provider Network following any reprocurement of the Contractor's providers.

6. Ensure that there are sufficient Network Providers to deliver all BH Covered Services in accordance with the terms of this Contract.

7. Develop a BH Provider Network Plan that:

    a. Ensures that the Provider Network is established in a fair and equitable manner, and in accordance with the requirements of this Contract and represents the full continuum of Behavioral Health Covered Services.

    b. Allows all interested providers who are in good standing, including independently practicing licensed social workers, licensed mental health counselors Licensed Alcohol and Drug Counselors 1 (LADC1), and

licensed marriage and family therapists, to apply to become Network Providers.

8. Develop and maintain an up-to-date database that contains, at a minimum, the following information on Network Providers:

   a. Network Provider name and unique National Provider Identifiers (NPIs) for each such Network Provider;

   b. contracted services;

   c. site address(es) (street address, town, ZIP code, region of the state);

   d. site telephone numbers;

   e. site hours of operation;

   f. emergency/after-hours provisions;

   g. professional qualifications and licensing;

   h. areas of specialty relating to Behavioral Health conditions and MassHealth populations;

   i. cultural and linguistic capabilities;

   j. malpractice insurance coverage and malpractice history;

   k. credentialing status;

   l. status as Supplier Diversity Office (SDO) certified business; and

   m. Provider e-mail address.

9. Develop and maintain a list of BH Network Providers, sorted by type of service and by Network Providers' capability to communicate with Covered Individuals in their primary languages. This list shall be available to the Contractor's clinical staff at all times, and available to Network Providers, Covered Individuals, EOHHS, DMH and other interested parties upon their request and at no charge.

10. On a monthly basis and as requested by EOHHS, submit a complete database of all Network Providers via a system interface as directed by EOHHS in a form and format and according to data standards specified by EOHHS.

11. As further specified by EOHHS, contract with state agency providers as follows:

   a. Include in its Provider Network state agency providers, identified in **Appendix A-2** as updated by EOHHS from time to time, of inpatient mental health services, outpatient Behavioral Health, diversionary Behavioral Health services, Acute Treatment Services and Clinical Stabilization Services as set forth in **Appendix A-1**.

b. Not require these state agency providers to indemnify the Contractor, to hold a license, or to maintain liability insurance; and

c. If required by EOHHS, include in its Provider Network or pay as out-of-network providers, other state agency providers as set forth in **Appendix A-2**.

12. Execute and maintain contracts with the following providers:

a. DMH-licensed Providers for psychiatric inpatient child services and psychiatric inpatient adolescent services identified in **Appendix A-2, Exhibit 6** of this Contract, as updated by EOHHS from time to time.

b. Inpatient Substance Use Disorder Services (Level 4) identified in **Appendix A-2, Exhibit 7** of this Contract, as updated by EOHHS from time to time.

c. Effective July 1, 2025, the Contractor shall execute and maintain contracts with providers of Individualized Treatment Services and Youth Withdrawal Management and Stabilization Services approved by the DPH Bureau of Substance Addiction Services, identified in **Appendix A-2, Exhibit 8**, as updated by EOHHS from time to time, and shall pay such providers in accordance with **Section 2.7.F.3.e-f**.

B. BH Provider Network Requirements

1. The Contractor shall maintain and monitor a BH Provider Network sufficient to provide all BH Covered Individuals, including those with limited English proficiency or physical or mental disabilities, with adequate access to BH Covered Services across all regions of the state. As further directed by EOHHS, the Contractor shall maintain information about its BH Provider Network with respect to the above requirement and provide EOHHS with such information upon request.

2. The BH Provider Network shall be composed of a sufficient number of appropriately credentialed, licensed, or otherwise qualified BH Network Providers to meet the requirements of this Contract. As directed by EOHHS:

a. Such Providers must be screened and enrolled with EOHHS as specified by EOHHS.

b. The Contractor may execute Provider Contracts for up to 120 days pending the outcome of EOHHS' enrollment process but must terminate a Provider Network immediately upon notification from EOHHS that the Network Provider cannot be enrolled, or the expiration of one 120 day period without enrollment of the provider. The Contractor shall notify affected Covered Individuals of the termination.

3. The Contractor shall make best efforts to ensure that SDO certified businesses and organizations are represented in the Provider Network. The Contractor will submit annually the appropriate certification checklist on its efforts to contract with SDO-certified entities.

4. As requested by EOHHS, the Contractor shall, in a form and format specified by EOHHS, report to EOHHS data specifications related to its BH Network Providers including but not limited to whether each BH Network Provider is enrolled as a MassHealth provider, and any other information requested by EOHHS about its BH Network Providers including but not limited to each Provider's MassHealth billing ID, provider ID/service location (PID/SL), NPI, tax ID (or TIN), and known affiliations to other providers.

5. The BH Provider Network shall include a sufficient number of Providers with appropriate expertise in treating Covered Individuals with BH needs to address their care needs, including an adequate number of Providers with experience and expertise in various specialty populations.

6. In addition to ensuring its Network includes BH Providers who can address all diagnostic needs and provide care to all Diagnostic and Statistical Manual of Mental Disorders Fifth Edition (DSM 5)(or current version as applicable) conditions as described in the most recent publication, the Contractor shall ensure that its BH Provider Network must have the capacity to provide integrated care to individuals with complex needs across multiple specialty populations and co-occurring disorders, including:

    a. Serious and persistent mental illness;

    b. Post-traumatic stress disorder, especially among children and adolescents;

    c. Children and adolescents, including children and adolescents with Serious Emotional Disturbance and Autism Spectrum Disorder;

    d. Physical disabilities and chronic illness;

    e. Deaf and hard of hearing and blind or visually impaired;

    f. HIV/AIDS;

    g. Homelessness;

    h. Child Welfare and juvenile justice;

    i. Fire-setting behaviors;

    j. Sex-offending behaviors;

    k. Post-adoption issues;

    l. Eating disorders; and

m. Substance use disorders

7. The Contractor shall ensure its Provider Network includes sufficient numbers of BH Network Providers with experience and expertise with the following populations of Covered Individuals:

   a. Persons with physical disabilities;

   b. Persons with chronic illness(es);

   c. Children, adolescents and their families;

   d. Persons who are homeless, including children and families;

   e. Children in the Care and/or Custody of the Commonwealth;

   f. Persons with criminal justice involvement;

   g. Young adults who are transitioning out of state-sponsored programs as they turn 22;

   h. Persons with intellectual and developmental disabilities;

   i. Persons with brain injuries;

   j. Persons with HIV/AIDS;

   k. Pregnant women with substance use conditions;

   l. Young children;

   m. Older adults;

   n. Persons from diverse cultural backgrounds, including persons whose primary language is not English;

   o. Persons who are deaf or hard of hearing; and

   p. Persons who are blind or visually impaired.

8. The Contractor shall provide coverage across all regions of the state.

9. The Contractor shall ensure the availability of the full range of BH Covered Services.

10. The Contractor shall provide access to BH Covered Services according to the standards set forth in **Section 2.9**.

11. The Contractor shall allow independently practicing clinicians with the following licenses to apply to become Network Providers: Licensed Independent Clinical Social Worker (LICSW), Licensed Alcohol and Drug Counselors 1 (LADC1),

Licensed Marriage and Family Therapist (LMFT), Licensed Mental Health Counselor (LMHC) and Licensed Psychologist.

12. In establishing and maintaining the Provider Network, the Contractor must consider the following:

    a. The anticipated enrollment in the PCC Plan and the PCACOs and estimated numbers of other MassHealth Covered Individuals who will receive BH Covered Services through the Contractor;

    b. The expected utilization of services, taking into consideration the characteristics and health care needs of specific MassHealth populations enrolled with the Contractor;

    c. The numbers and types (in terms of training, experience, and specialization) of Providers required to timely furnish the BH Covered Services;

    d. The number of Network Providers who are not accepting new patients; and

    e. The geographic location of Providers and Covered Individuals, considering distance, travel time, the means of transportation ordinarily used by Covered Individuals, and whether the location provides physical access for Covered Individuals with disabilities.

13. The Contractor shall implement written policies and procedures for the selection and retention of Providers in accordance with 42 CFR 438.214, including but not limited to ensuring such policies and procedures for Providers do not discriminate against particular Providers that serve high-risk populations or specialize in conditions that require costly treatment.

14. Share with MassHealth-contracted managed care entities and PCC Plan Providers any changes and/or updates to the CBHC and YCCS provider network prior to disseminating that information to all Covered Individuals. This provision does not require the Contractor to share with the MassHealth-contracted MCOs, ACOs or PCC Plan Providers any information that pertains solely to individuals who are Covered Individuals or Uninsured Individuals or persons with Medicare only.

15. Share with MassHealth-contracted MCOs, ACOs, and PCC Plan Providers, any changes and/or updates to the list of CSAs prior to disseminating that information to all Covered Individuals. This provision does not require the Contractor to share with the MassHealth-contracted MCOs, ACOs or PCC Plan Providers any information that pertains solely to individuals who are Covered Individuals.

16. At the Covered Individual's request, the Contractor shall provide for a second opinion from a qualified health care professional within the Provider Network, or

arrange for the Covered Individual to obtain one outside the Provider Network, at no cost to the Covered Individual.

17. The Provider Network shall be responsive to the linguistic, cultural, and other unique needs of any minority, homeless person, Covered Individuals with special health care needs, including individuals with disabilities, or other special populations served by the Contractor, by, at a minimum, having the capacity to, when necessary, communicate with Covered Individuals in languages other than English, communicate with individuals who are deaf, hard-of-hearing, or deaf blind, and making materials and information available in Alternative Formats as specified in this Contract.

18. The Contractor shall ensure that its Network Providers and Material Subcontractors meet all current and future state and federal eligibility criteria, standard and ad hoc reporting requirements, and any other applicable rules and/or regulations related to this Contract;

19. Out-of-Network Access

    The Contractor shall develop, maintain and utilize EOHHS-approved protocols to address situations when the Provider Network is unable to provide Covered Individual with adequate and timely access to necessary BH Covered Services as defined in **Section 2.9.C** and **42 CFR 438.206** Availability of services**.** The Contractor's protocols must ensure, at a minimum, the following:

    a. If the Contractor is unable to provide a Covered Individual with a particular BH Covered Service through its Provider Network, it will be adequately covered in a timely way out-of-network for as long as the Provider Network is not able to provide such BH Covered Services;

    b. When accessing an out-of-network provider, the Covered Individual is able to obtain the same service or to access a provider with the same type of training, experience, and specialization as within the Provider Network;

    c. That out-of-network providers must coordinate with the Contractor with respect to payment, ensuring that the cost to the Covered Individual is no greater than it would be if the services were furnished through the Provider Network;

    d. That the particular service will be provided by the most qualified and clinically appropriate provider available taking into account the geographic location of the provider and the Covered Individual, considering distance, travel time, the means of transportation ordinarily used by Covered Individuals, and whether the location provides physical access for Covered Individuals with disabilities if applicable to the Covered Individual;

e. That the processes, strategies, evidentiary standards, or other factors in determining access to out-of-network providers for mental health or substance use disorder benefits are comparable to, and applied no more stringently than, the processes, strategies, evidentiary standards, or other factors in determining access to out-of-network providers for medical/surgical benefits in the same classification;

f. That the provider will be informed of his or her obligations under state or federal law to have the ability, either directly or through a skilled medical interpreter, to communicate with the Covered Individual in his or her primary language;

g. That the only Provider available to the Covered Individual in the Provider Network does not, because of moral or religious objections, decline to provide the service the Covered Individual seeks;

h. That consideration is given for an out-of-network option in instances in which the Covered Individual's Provider(s) determines that the Covered Individual needs a service and that the Covered Individual would be subjected to unnecessary risk if the Covered Individual received those services separately and not all of the related services are available within the Provider Network; and

i. That the Contractor cover certain BH Covered Services furnished to a Covered Individual in another state in accordance with 42 CFR 431.52(b) and 130 CMR 450.109.

C. BH Provider Network Management

The Contractor shall:

1. Beginning on the Operational Start Date, develop and implement a strategy to manage the Provider Network with an emphasis on the following:

a. Timely access to treatment for Covered Individuals;

b. Quality of care;

c. Application of principles of rehabilitation and recovery to service planning and service delivery;

d. Reduction of health disparities;

e. Measurement of outcomes for Covered Individuals over the course of receiving Behavioral Health Covered Services. The Contractor shall develop systems to measure outcomes based on goals set for a course of treatment;

f. Full Integration of Behavioral Health Covered Service delivery across Mental Health and SUD providers, and with medical services provided by the Enrollee's PCC, Covered Individual's PCP, or other key health care Providers, including state agency providers;

g. Cost-effectiveness of the delivery of BH Covered Services, and

h. Effective care transitions and care continuity for Covered Individuals.

2. Ensure that its Provider Network management strategy includes at least the following:

a. Actively monitoring the quality of care including effective use of evidence based practices and timely access to treatment provided to Covered Individuals under any Provider Contracts and any other subcontracts, including but not limited to the use of secret shoppers to confirm access;

b. A systematic plan for utilizing Network Provider profiling and benchmarking data to identify and manage Network Providers who fall below established benchmarks and performance standards, and to replicate practices of Network Providers who consistently exceed benchmarks and performance standards;

c. A system for the Contractor and Network Providers to identify and establish improvement goals and periodic measurements to track Network Providers' progress toward improvement goals;

d. Utilization of on-site visits to Network Providers at all Levels of Care, to support quality improvement efforts and benchmarking data; and

e. Steps to ensure Network Provider compliance with the Contractor's performance specifications for each BH Covered Service.

3. Take appropriate management action, including the development and monitoring of corrective action plans for Network Providers whose performance is determined by the Contractor to be in need of improvement.

a. The Contractor shall notify EOHHS of any Network Providers who are placed on a corrective action plan.

4. Take appropriate action related to Network Providers, as follows:

a. Upon the Contractor's awareness of any disciplinary action or sanction taken against a Network Provider, either internally by the Contractor or by any oversight agency or any source outside of the Contractor's organization, such as the Board of Registration in Medicine, the Division of Registration, and the federal Centers for Medicare and Medicaid Services (CMS), immediately inform EOHHS's Business Support

Services vendor of such action taken and work collaboratively with the vendor to maintain a process to share such information.

b. If notified that MassHealth or another state Medicaid agency has taken an action or imposed a sanction against a Medicaid provider, including disenrollment of any such provider from the Medicaid program, review the Provider's performance related to this Contract and take any action or impose any sanction that the Contractor determines is appropriate, including disenrollment from the Contractor's Provider Network.

5. In collaboration with and as further directed by EOHHS, develop and implement BH Network Provider quality improvement activities directed at ensuring that Network Providers:

   a. use the CANS Tool in their Behavioral Health Clinical Assessments and during the Discharge Planning process from Inpatient Psychiatric Hospitalizations and Community-Based Acute Treatment Services for Covered Individuals under the age of 21; and

   b. access and utilize the CANS IT System to input information gathered using the CANS Tool to identify whether or not the assessed Covered Individual is suffering from a Serious Emotional Disturbance.

6. Educate Providers through a variety of means including, but not limited to, Provider Alerts or similar written issuances, about their legal obligations under state and federal law to communicate with individuals with limited English proficiency, including the provision of interpreter services, and the resources available to help Providers comply with those obligations. All such written communications shall be subject to the prior review and approval of EOHHS;

7. Reserved.

8. Propose by the Operational Start Date, and implement subject to EOHHS approval, a Network management strategy to engage with PCCs, specialty Providers, high-volume prescribers, and hospital ED to improve access for Covered Individuals who may be under- or over-utilizing Behavioral Health services. The proposal shall include but is not limited to methods for the Contractor's staff and its Behavioral Health Network Providers to use to identify Enrollees who may benefit from participation in the Care Management Program described in **Section 2.5**;

9. Propose methods the Contractor will use to engage foster parents and other individuals with physical custody of Children in the Care and/or Custody of the Commonwealth in such children's health care needs to ensure that they obtain Early and Periodic Screening, Diagnosis and Treatment (EPSDT), periodic and

inter-periodic screens and Medically Necessary follow-up medical dental and Behavioral Health services; and

10. Propose methods the Contractor will use to establish and maintain specific supports for Providers of Behavioral Health, Primary Care, and specialty health care who provide MassHealth Covered Services to Children in the Care and/or Custody of the Commonwealth to ensure continuity of care for Children in the Care and/or Custody of the Commonwealth who change Providers due to changes in their foster care arrangements or for other reasons.

11. Modify, in whole or in part, any proposal submitted pursuant to this Section, as required by EOHHS to obtain EOHHS' approval.

12. The Contractor shall establish and implement policies and procedures to:

    a. Enhance interoperability of its health information technology to support the continued evolution of patient clinical data and operational data;

    b. Increase utilization of health information exchange services operated or promoted by the Mass HIway (e.g., Direct Messaging, Statewide Event Notification Service Framework).

    c. Upon notification by EOHHS that additional Mass HIway services are developed, operated, or promoted (e.g., FHIR-based APIs) establish and implement policies and procedures to increase connectivity to such services and work with its providers to increase their connectivity;

    d. Increase its ability to make electronic Health Related Social Needs (HRSN) referrals (e.g., secure email, SFTP, platform integrated into EHRs) and to be able to receive updates from providers providing HRSN supports to Covered Individuals;

    e. Increase its ability to participate with the Behavioral Health Treatment and Referral Platform (BHTRP) and to be able to both create and receive updates from providers using the BHTRP to supports to Covered Individuals;

    f. The Contractor shall provide documentation of the policies and procedures set forth in this **Section** within 30 calendar days of an EOHHS request;

13. The Contractor shall ensure that its Providers enable and utilize Query and Retrieve functionality that is natively available in the Providers' EHRs (e.g., via the Carequality or Commonwell networks);

14. The Contractor shall ensure it is able to access or receive event notifications from an EOHHS-Certified ENS Vendor participating in the Statewide ENS Framework. The Contractor shall establish and implement policies and procedures for its Providers to integrate such event notifications into appropriate

care management or population health management workflows; and

15. The Contractor shall comply with the Expedited Psychiatric Inpatient Admission (EPIA) protocol, including but not limited to utilization of the Behavioral Health Treatment and Referral Platform, as directed by EOHHS upon implementation.

16. Have at least 75% of its Providers who are Electronic Health Record (EHR) eligible providers adopt and integrate interoperable EHRs certified by the Office of the National Coordinator (ONC) using ONC's 2015 certification edition along with subsequent edits to the 2015 certification edition pursuant to the 21st Century Cures Act.

D. Network Provider Policy and Procedure Manual

The Contractor shall:

1. At least three months prior to the Operational Start Date, develop and submit to EOHHS for approval a Provider policy and procedure manual, and, following EOHHS approval, publish the manual on Contractor's website and electronically distribute a hyperlink to the manual to all Network Providers. At a Network Provider's request, also electronically distribute the manual to the Providers. The manual shall include, at a minimum, information on:

    a. The Contract, the Contractor, and program priorities;

    b. How to verify a Covered Individual's eligibility for MassHealth Behavioral Health Covered Services;

    c. Network Provider Credentialing Criteria;

    d. Provider Network management;

    e. Procedures for service authorization, concurrent review, extensions of lengths of stay, and retrospective reviews for all BH Covered Services;

    f. Clinical Criteria for admission, continued stay, and discharge for each BH Covered Service;

    g. Administrative and billing instructions, including a list of procedure codes, units and payment rates;

    h. How to appeal payment and service denial decisions;

    i. Reporting requirements for Serious Reportable Events and Reportable Adverse Incidents; and

    j. Performance specifications for each Behavioral Health Covered Service.

2. As necessary, modify or supplement the policy and procedure manual by distributing periodic notices to Network Providers;

3. Review the manual at least biannually and amend it, if necessary, in consultation with EOHHS; and

4. Redistribute the amended portions of the manual to Network Providers.

E. Performance Specifications

The Contractor shall:

1. Require all Network Providers to accept the Contractor's performance specifications that have been approved by EOHHS;

2. Develop and maintain performance specifications for Network Providers and develop performance specifications for new BH Covered Services; and

3. At least annually, review and update as necessary the performance specifications including any new performance specifications that have been developed, and submit any proposed changes to EOHHS for prior review and approval.

F. BH Network Provider Protocols

1. The Contractor shall develop, maintain and utilize EOHHS-approved Network Provider protocols. The protocols must address the following:

   a. How the Contractor intends to ensure, for a particular Covered Individual's needs, that a qualified and clinically appropriate Network or non-Network Provider:

      1) is available to provide the particular BH Covered Service in a timely manner;

      2) is accessible within the access standards required by the Contract, taking into account the availability of public transportation;

      3) is accessible to individuals with physical disabilities, if appropriate; and

      4) has the ability, either directly or through a skilled medical interpreter, to communicate with the Covered Individual in his/her primary language.

   b. How the Contractor intends to facilitate communication between Network Providers and the Contractor, and between Network Providers and PCCs, in a manner that engages the Providers and overcomes Barriers to communication.

2. The Contractor shall require Network Providers to submit to the Contractor a written report of all Reportable Adverse Incidents, using the form found in **Appendix F** or other similar form acceptable to EOHHS, according to the following guidelines:

a. Network Providers of 24-hour BH Covered Services shall, within 24 hours of their occurrence, report to the Contractor all Reportable Adverse Incidents involving a Covered Individual.

b. Network Providers of non-24-hour BH Covered Services shall, within 24 hours of their occurrence, report to the Contractor all Reportable Adverse Incidents involving a Covered Individual.

c. The Contractor shall require Network Providers to coordinate MassHealth Covered Services with the Covered Individual's care manager or BH CP where the Covered Individuals are receiving Care Management services through the Contractor or CP services through their PCACO and/or the case manager when the Covered Individual is receiving case management through a state agency (e.g., DMH, DCF, DDS, and DYS).

3. The Contractor shall require Network Providers to comply with DPH's regulations barring payment for services related to a Serious Reportable Event.

4. The Contractor shall require Network Providers to comply with all of the following Massachusetts regulations and DMH policy memorandums:

a. DMH Policy 14-01 of September 29, 2014, on informed consent, found at https://www.mass.gov/doc/14-01-informed-consent-policy-effective-september-29-2014/download , or any successive policy or regulation;

b. DMH regulations on human rights and restraint & seclusion at 104 CMR 27 and 104 CMR 28, or any successive regulation, and any other applicable DMH regulations; and

c. M.G.L. c. 123, § 23.

5. The Contractor shall require its Network Providers of Community-Based Acute Treatment Services, and Transitional Care Units to comply with Department of Early Education and Care (DEEC) standards for the licensure or approval of residential programs serving Members under 18, as set forth in 606 CMR 3.00, et seq. For those CBAT, ACBAT, and TCU Providers that are not located in a site licensed by DEEC, the Contractor shall ensure that these programs are located in a facility that is licensed by DMH and/or DPH.

6. The Contractor shall require its Network Providers to inform Covered Individuals of their rights under DMH regulations concerning human rights.

7. The Contractor shall comply with EOHHS protocols to ensure access to Behavioral Health Covered Services and tracking in the EOHHS Data Warehouse and MMIS systems by adhering to the following requirements:

a. Maintain a unique Network Provider identification number for each Network Provider, as described in **Section 2.8.A**.

b. Submit to EOHHS's Business Support Services vendor by the Operational Start Date a list of all Network Providers who are both MassHealth Providers and Network Providers (dual Providers). The Contractor shall inform EOHHS's Business Support Services vendor upon enrolling or disenrolling any dual Provider from its Provider Network.

c. Inform EOHHS's Business Support Services vendor immediately upon enrolling any Provider who is not also a MassHealth Provider in its Provider Network. Such notification shall include the following data elements:

1) Network Provider name, address and telephone number;

2) Legal entity's name, address and phone number of the practice (i.e., "doing business as," or d/b/a, name), if different from the above;

3) Network Provider or legal entity's tax identification number; and

4) Effective date of the Network Provider's enrollment in the Provider Network.

5) The Contractor shall submit to the Business Support Services vendor all updates to the list or its data elements whenever they occur.

8. The Contractor shall require, and develop a mechanism to enable, its Network Providers to:

a. Report to the Contractor when it has received an overpayment;

b. Return the overpayment to the Contractor within 60 calendar days after the date on which the overpayment was identified; and

c. Notify the Contractor in writing of the reason for the overpayment;

9. The Contractor shall require its Network Providers of Community-Based Acute Treatment Services and Community Crisis Stabilization that are Institutions of Mental Disease as defined in Section 1905(i) of the Act serving Covered Individuals under the age of 21 to obtain accreditation from a nationally-recognized accreditation agency. The Contractor shall reasonably assist Network Providers in obtaining such accreditation, as further specified by EOHHS.

10. Community Behavioral Health Center Incentive Program

The Contract shall:

a. Collaborate with EOHHS and Community Behavioral Health Centers (CBHCs) to implement the Community Behavioral Health Center (CBHC)

Incentive Program, with a quality component, the CBHC Clinical Quality Incentive (CCQI), and a health equity component, the CBHC Quality and Equity Incentive Program (CQEIP).

b. Make value-based payments, pursuant to 42 CFR 438.6(c) and as specified by EOHHS, to CBHCs listed in **Appendix A-2, Exhibit 1**. The Contractor shall make such payments to such Providers within 14 calendar days of receiving payment from EOHHS.

G. Provider Credentialing, Recredentialing, and Board Certification

1. General Provider Credentialing

The Contractor shall implement written policies and procedures that comply with the requirements of 42 CFR 438.214 regarding the selection, retention and exclusion of Providers and meet, at a minimum, the requirements below. The Contractor shall submit such policies and procedures annually to EOHHS, if amended, and shall demonstrate to EOHHS, by reporting annually in accordance with **Appendix E-1** that all Providers within the Contractor's Provider Network are credentialed according to such policies and procedures. The Contractor shall at a minimum:

a. Participate in any effort by EOHHS to standardize credentialing processes across EOHHS and its MassHealth managed care entities and fee-for-service programs.

b. Require Network Providers to meet the Credentialing Criteria approved by EOHHS.

c. Maintain appropriate, documented processes for the credentialing and re-credentialing of physician Network Providers and all other licensed or certified Network Providers who participate in the Contractor's Provider Network. At a minimum, the scope and structure of the processes shall be consistent with recognized managed care industry standards such as those provided by NCQA and relevant state regulations, including regulations issued by the Board of Registration in Medicine (BORIM) at 243 CMR 3.13. The basic components of these processes shall include a review of the following:

1) licensing, accreditation, certification, training, specialty board eligibility or certification;

2) current status of professional license, restrictions, and history of any loss of licensure in any state;

3) DEA number and copy of certification, where applicable;

4) hospital privileges, name of hospitals, and scope of privileges, where applicable;

5) record of continuing professional education;

6) location, service area and telephone numbers of all offices, hours of operation, and provisions for Emergency care and backup;

7) areas of special experience, skills and training;

8) cultural and linguistic capabilities;

9) review of Covered Individual satisfaction and any complaints made or Grievances filed against the Network Provider within the past two years;

10) physical accessibility for persons with disabilities;

11) malpractice insurance, carrier name, amount of coverage, copy of the face sheet, and scope of coverage;

12) malpractice history, pending claims, and successful claims against the Provider;

13) Medicare, Medicaid, federal tax identification number, and Social Security numbers;

14) reference check;

15) for facility-based Network Providers, a site visit and evidence of a training program for staff on the appropriate and safe use of restraint and seclusion to the extent that the facility's license permits the use of seclusion, and

16) for Network Providers of 24-hour services, evidence of a training program for staff on the appropriate and safe use of restraint and seclusion.

d. Ensure that all Network Providers are credentialed prior to becoming Network Providers and that a site visit is conducted with recognized managed care industry standards such as those provided by NCQA and relevant state regulations;

e. Maintain a documented re-credentialing process that requires that physician Providers and other licensed and certified Behavioral Health Providers maintain current knowledge, ability, and expertise in their practice area(s) by requiring them, at a minimum, to conform with recognized managed care industry standards such as those provided by NCQA and relevant state regulations, when obtaining Continuing Medical

Education (CME) credits or Continuing Education Units (CEUs) and participating in other training opportunities, as appropriate. Such processes shall also be consistent with any uniform re-credentialing policies specified by EOHHS addressing Behavioral Health Providers, and any other EOHHS-specified Providers;

f. Ensure that Network Providers are recredentialed every three years, at a minimum, and take into consideration various forms of data, including but not limited to, Grievances, results of quality reviews, Covered Individual satisfaction surveys, and Utilization Management information;

g. Designate the Contractor's department(s) and staff who will be directly responsible for credentialing and recredentialing Network Providers;

h. To the extent permitted by law and upon request, provide Covered Individuals or their legal guardians with information in the Network Provider database, with the exception of the information described in **Section 2.8.G.1.c.11-16** above;

i. Ensure that that the credentialing process does not discriminate against particular Providers that serve high-risk populations or specialize in conditions that require costly treatment;

j. Not authorize any Network Providers terminated or suspended from participation in MassHealth, Medicare or from another state's Medicaid program, to treat Covered Individuals, and deny payment to such Network Providers for any service provided.

1) The Contractor shall, at a minimum, check the Board of Registration in Medicine (BORIM) website at least once per month and the U.S. Department of Health and Human Services Office of the Inspector General's (OIG) List of Excluded Individuals Entities (LEIE) or Medicare Exclusion Database (MED) websites before the Contractor contracts with a Provider to become part of its Provider Network, at the time of a Provider's credentialing and recredentialing, and at least monthly thereafter.

2) The Contractor shall notify a Network Provider within three business days that, due to its MassHealth, Medicare, or another state's Medicaid program termination or suspension or a state or federal licensing action, such Network Provider is terminated or suspended, as appropriate, from the Contractor's Provider Network, and is no longer eligible to treat Covered Individuals. The Contractor shall have a process in place to immediately effectuate such termination or suspension.

3) When the Contractor terminates or suspends a Network Provider from its Network, or rejects a potential provider's application to join the Network, based on such Provider's termination or suspension with MassHealth, Medicare, or another state's Medicaid program, a state or federal licensing action, or based on any other independent action, the Contractor shall notify EOHHS of the Network Provider termination, suspension or rejection, and the reason thereof, within three business days.

4) On an annual basis, the Contractor shall submit to EOHHS a certification checklist confirming that it has implemented the actions necessary to comply with this Section.

5) This Section does not preclude the Contractor from suspending or terminating Network Providers for cause prior to such Network Provider's ultimate suspension and/or termination by EOHHS from participation in MassHealth.

k. Not employ or contract with a Provider, or otherwise pay for any items or services furnished, directed or prescribed by a Provider that has been excluded from participation in federal health care programs by the OIG under either Section 1128 or Section 1128A of the Social Security Act, or that has been terminated from participation under Medicare or another state's Medicaid program, except as permitted under 42 CFR 1001.1801 and 1001.1901.

l. Ensure that no Network Provider engages in any practice with respect to any Covered Individual that constitutes unlawful discrimination under any other state or federal law or regulation, including but not limited to practices that violate the provisions of 45 CFR Part 80, 45 CFR Part 84, and 45 CFR Part 90.

m. Search for the names of parties disclosed during the credentialing process in the BORIM, OIG LEIE, and Medicare MED exclusion or debarment databases and the MassHealth exclusion list, and do not contract with parties that have been terminated from participation under Medicare or another state's Medicaid program.

n. Notify EOHHS when a Network Provider fails credentialing or re-credentialing because of a program-integrity reason, including those reasons described in this Section, and provide information required by EOHHS or state or federal laws, rules, or regulations.

o. Demonstrate to EOHHS, by reporting annually in accordance with **Appendix E-1**, that all Network Providers within the Contractor's Provider Network are credentialed according to this Section.

2. Network Provider Qualifications

The Contractor shall:

a. Execute Provider Agreements or enter into other arrangements for BH Covered Services only with facility-based Providers that satisfy the following criteria:

1) They are financially stable, as determined by the Contractor;

2) They have established and maintain a Quality Management program, as described in **Section 2.13**;

3) They comply with policies and regulations with respect to patient rights and privileges, as applicable;

4) They maintain records consistent with current professional standards and EOHHS regulations, as well as systems for accurately documenting the following information for each Covered Individual receiving BH Covered Services:

a) demographic information, including race, ethnicity, preferred language, disability status, sexual orientation, and gender identity;

b) clinical history;

c) Behavioral Health Clinical Assessments;

d) treatment plans;

e) services provided in sufficient detail to justify payment;

f) contacts with Covered Individuals' family, guardians, or significant others; and

g) treatment outcomes;

5) Are responsive to linguistic, cultural and other unique needs of any member of a cultural, racial or linguistic minority, or other special population in the region in which they provide services;

6) Have the capacity to communicate with Covered Individuals in languages other than English, when necessary, as well as with those who are deaf or hearing-impaired;

7) Satisfy all federal and state requirements for affirmative action;

8) Satisfy all federal and state legal requirements regarding the Provider's physical plant and premises;

9) Comply with all applicable anti-discrimination requirements described in 42 CFR 438.3(d)(3) and (4);

10) Comply with all other applicable state and federal laws;

11) Meet the Credentialing Criteria; and

12) Have been credentialed pursuant to the policies and procedures specified in **Section 2.8.G**.

b. Ensure that, in addition to the criteria set forth in **Section 2.8.G.2.a**, above, those facility-based Network Providers that are Network Providers of Inpatient Services are fully licensed by DMH and by DPH as applicable. In addition, ensure that such Providers:

1) Comply with DMH regulations concerning human rights set forth in 104 CMR 27.13 and 14 and 104 CMR 28.11, including ensuring that human rights activities are overseen by a human rights committee and officer, and provide training for staff and education for Covered Individuals regarding human rights. To the extent permissible under **Section 5.2**, notify EOHHS and DMH when issues of non-compliance come to the attention of the Contractor whether through the discovery of Serious Reportable Events, or by other means, including but not limited to complaints, Grievances, or Network management activities;

2) Comply with DMH's regulations concerning restraint and seclusion. To the extent permissible under **Section 5.2**, notify EOHHS and DMH when issues of non-compliance come to the attention of the Contractor whether through the discovery of Serious Reportable Events, or by other means, including but not limited to complaints, Grievances, or Network management activities;

3) Submit to the Contractor evidence of implementation of the training programs described in **Section 2.8.G.2.b.1-2** as part of investigations of Serious Reportable Events, implementation of corrective action plans that involve human rights, and the use of restraint and seclusion;

4) Notify the DMH Licensing Unit of an inpatient Provider's non-compliance with these requirements and collaboratively determine whether additional Contractor action is appropriate;

5) Develop organizational and clinical linkages with each of the high-volume referral source CBHCs, as identified by EOHHS, hold regular meetings, and communicate with the CBHCs on clinical

and administrative issues, as needed, to enhance continuity of care for Covered Individuals; and

c. Preferentially execute Provider Agreements or enter into other arrangements for the provision of BH Covered Services with Providers that demonstrate a commitment to the principles of rehabilitation and recovery from mental illness and addiction, including a focus on recovery-oriented services, consumer and family involvement in program management, a strength-based approach to working with children and their families, and training for staff on such principles.

d. Upon notice from EOHHS, not authorize any providers terminated or suspended from participation in MassHealth, Medicare or from another state's Medicaid program, to treat Covered Individuals and shall deny payment to such providers for services provided. In addition:

1) The Contractor shall monitor Providers and prospective Providers by monitoring all of the databases described in **Appendix J**, at the frequency described in **Appendix J**.

2) The Contractor shall submit a monthly Excluded Provider Monitoring Report to EOHHS, as described in **Appendix E-1**, which demonstrates the Contractor's compliance with this **Section 2.8**. At the request of EOHHS, the Contractor shall provide additional information demonstrating to EOHHS' satisfaction that the Contractor complied with the requirements of this Section;

3) If a provider is terminated or suspended from MassHealth, Medicare, or another state's Medicaid program or is the subject of a state or federal licensing action, the Contractor shall terminate, suspend, or decline a provider from its Network as appropriate. In the event EOHHS suspends payment to a provider, including but not limited to when there is an investigation of a credible allegation of fraud, the Contractor shall also suspend such payment, if directed to do so by EOHHS; provided, however, that the Contractor may propose to EOHHS that there is good cause for the Contractor not to suspend, or to suspend in part, such payments. EOHHS shall approve or deny the Contractor's proposal.

4) The Contractor shall notify EOHHS when it terminates, suspends, or declines a Provider from its Network or for any other independent action including;

5) This Section does not preclude the Contractor from suspending or terminating Providers for reasons unrelated to the possible

suspension and/or termination from participation in MassHealth, Medicare or another state's Medicaid program;

e. Not employ or contract with, or otherwise pay for any items or services furnished, directed or prescribed by, a Provider that has been excluded from participation in federal health care programs by the Office of the Inspector General of the U.S. Department of Health and Human Services under either Section 1128 or Section 1128A of the Social Security Act, or that has been terminated from participation under Medicare or another state's Medicaid program, except as permitted under 42 CFR 1001.1801 and 1001.1901. In addition, pursuant to Sections 1903(i), including 1903(i)(2)(B), of the Social Security Act, the Contractor shall not pay for an item or service (other than an emergency item or service, not including items or services furnished in an emergency room of a hospital) furnished at the medical direction or on the prescription of a physician, during the period when such physician is excluded from participation under title V, title VXIII, or XX or under title XIX pursuant to Sections 1128, 1128A, 1156 or 1842(j)(2) of the Social Security Act and when the person furnishing such item or service knew, or had reason to know, of the exclusion (after reasonable time period after reasonable notice has been furnished to the person);

f. Not establish Provider selection policies and procedures that discriminate against particular Providers that serve high-risk populations or specialize in conditions that require costly treatment;

g. Ensure that no credentialed Provider engages in any practice with respect to any Covered Individual that constitutes unlawful discrimination under any other state or federal law or regulation, including, but not limited to, practices that violate the provisions of 45 CFR Part 80, 45 CFR Part 84, and 45 CFR Part 90.

H. Provider Profiling

1. The Contractor must conduct profiling activities for Behavioral Health Network Providers, PCC Plan Providers, as directed by EOHHS including in accordance with **Section 2.19.D** for PCC Plan Providers, and other Provider types, at least annually. As part of its quality activities, the Contractor must document the methodology it uses to identify which and how many non-PCC Plan Providers to profile, and to identify measures to use for profiling such Providers.

2. Provider profiling activities for Network Providers must include, but are not limited to:

a. Developing Provider-specific reports that include a multi-dimensional assessment of a Provider's performance using clinical, administrative, and

Covered Individuals satisfaction indicators of care that are accurate, measurable, and relevant to the enrolled population;

b. Establishing Provider, group, or regional benchmarks for areas profiled, where applicable, including MassHealth-specific benchmarks, if any;

c. Providing feedback to Providers regarding the results of their performance and the overall performance of the Provider Network; and

d. Designing and implementing quality improvement plans for Providers who receive a relatively high denial rate for prospective, concurrent, or retrospective service authorization requests, including referral of these Providers to the Network Management staff for education and technical assistance and reporting results annually to EOHHS.

3. The Contractor shall use the results of its BH Provider profiling activities to identify areas of improvement for Providers, and/or groups of Providers. The Contractor shall:

a. Establish Provider-specific quality improvement goals for priority areas in which a Provider or Providers do not meet established Contractor standards or improvement goals;

b. Develop and implement incentives, which may include financial and nonfinancial incentives, to motivate Providers to improve performance on profiled measures;

c. Conduct on-site visits to Network Providers for quality improvement purposes; and

d. At least annually, measure progress on the Provider Network and individual Providers' progress, or lack of progress, towards meeting such improvement goals.

4. The Contractor shall maintain regular, systematic reports, in a form and format approved by EOHHS, of the above-mentioned Provider profiling activities and related Quality Improvement activities pursuant to **Section 2.13**. Moreover, the Contractor shall submit to EOHHS, upon request, such reports or information that would be contained therein. The Contractor shall also submit summary results of such Provider profiling and related Quality Improvement activities as a component of its annual evaluation of the QM/QI program.

I. Provider Education

The Contractor shall develop an education and training plan that provides appropriate information and learning sessions for Network Providers and their staff, and that aligns with the Roadmap for Behavioral Health Reform's workforce retention goals to increase provider participation in insurance (including MassHealth) and strengthen workforce

diversity and competency. Such education and training plan shall be submitted to EOHHS for approval and shall include, at a minimum:

1. A schedule for the development and release of educational materials;
2. A schedule for the development and timing of training sessions;
3. Regional training opportunities for Network Providers' clinical and administrative staff; and
4. Proposed education and training topics, including but limited to:
    a. evidence-based practices for behavioral health clinicians;
    b. new changes to policies and procedures prior to their implementation;
    c. basics of MassHealth coverage and payment requirements;
    d. cultural and linguistic competency;
    e. quality improvement efforts and the Network Provider's role, including linkages across Behavioral Health and physical health services; and
    f. Health Equity in which the Contractor or designee ensures that meaningful and appropriate trainings to advance Health Equity are periodically received by all staff and Network Providers (contracted or directly employed) that interact with Medicaid Enrollees (through operations, delivery of services, or other Member-facing roles, e.g., security officer or receptionist). The Contractor shall document staff participation in required training and address staff non-compliance with training policies. The training content shall include, at minimum, the following:
        1) An overview of the organization's Health Equity strategy, including populations prioritized for intervention:
            a) The role(s) trainees can play to promote and achieve Health Equity;
            b) The importance of and best practices related to:
                (i) Collecting self-report social risk factors data such as race, ethnicity, language, disability (RELD), sexual orientation and gender identity (SOGI);
                (ii) Addressing inequities experienced by Covered Individuals with social risk factors, including RELD and SOGI;
                (iii) Adherence to CLAS standard as described in **Section 2.20.E**;

(iv) The role of trauma-informed practices for marginalized individuals;

(v) Identifying and mitigating the impact of implicit biases on delivery of high quality, equitable health care;

(vi) Anti-racism, as further specified by EOHHS, including topics such as, but not limited to, the role of structural and institutional racism in health care.

2) A description of how the content reinforces the Contractor's mission, values, and priorities and how trainees have applied or are expected to apply the training to their work.

a) The Contractor shall make its Health Equity, Anti-Racism Implicit Bias and related training available to all its sub-contracted Community Partners.

b) As part of the Health Quality and Equity Strategic Plan and Report, the Contractor shall provide an overview of its Health Equity training.

c) EOHHS may require the Contractor to implement additional training programs related to Health Equity.

d) As directed by EOHHS, The Contractor shall evaluate the effectiveness of its training programs on an annual basis.

J. Collaboration in Policy Development

The Contractor shall participate in any EOHHS efforts related to the development of policies or programs, as well as measurement, analytics, and reporting relating to such policies and programs, that support access, coordination, and continuity of Behavioral Health care, reduce emergency department utilization and lengths of time awaiting placement in inpatient and 24-hour levels of care, and address the opioid epidemic. Such policies or programs may include, but are not limited to, the development of:

1. Specialized inpatient services;

2. New diversionary and urgent levels of care;

3. Expanded substance use disorder treatment services; and

4. Services and supports tailored to populations with significant Behavioral Health needs, including justice involved and homeless populations.

Section 2.9 Accessibility and Availability of BH Covered Services

A. General

The Contractor shall ensure adequate access to BH Covered Services for all Covered Individuals and shall further facilitate access to non-BH Covered Services. All such services shall be accessible and available to Covered Individuals in a timely manner. Accessibility shall be defined as the extent to which the Covered Individual can obtain services at the time they are needed and refers to both telephone access and ease of scheduling an appointment. Availability shall be defined as the extent to which an organization geographically distributes practitioners of the appropriate type and number to meet the needs of Covered Individuals.

The Contractor shall:

1. Ensure access to BH Covered Services in accordance with state and federal laws for persons with disabilities by ensuring that BH Network Providers are aware of and comply with such laws so that physical and communication Barriers do not inhibit Covered Individuals from obtaining services under the Contract; and

2. Assure EOHHS that it has the capacity to serve Covered Individuals in accordance with the access and availability standards specified in **Sections 2.9.B and C**. by submitting reports specified in **Appendix E-1**, on an annual and ad-hoc basis, and whenever there is a significant change in operations of the BH Provider Network and significant changes to the BH Provider Network itself, that would affect the adequacy and capacity of services. Significant changes shall include, but are not limited to:

    a. Changes in BH Covered Services;

    b. Enrollment of a new population in the Contractor's Plan;

    c. Changes in MassHealth benefits, and

    d. Changes in Provider payment methodology.

    If the Contractor is not in compliance with the access and availability standards specified in **Sections 2.9.B and C**, the Contractor shall take corrective action necessary to come into compliance with such standards.

B. Accessibility

The Contractor shall ensure that Covered Individuals have access to BH Covered Services as provided below.

1. Emergency Services: Immediately, on a 24-hour basis, seven days a week, with unrestricted access to Covered Individuals who present at any qualified Provider, whether a Network Provider or a non-Network provider.

2. Adult Mobile Crisis Intervention (AMCI) and Youth Mobile Crisis Intervention (YMCI) Services: Within 60 minutes of time of the Covered Individual's readiness to receive such services.

3. Behavioral Health Crisis Services in Acute Medical Settings: Crisis Evaluation- within 60 minutes of time of the Covered Individual's readiness to receive such an assessment.

4. Behavioral Health Urgent Care: Within 48 hours for services that are not Emergency Services, Mobile Crisis Intervention, or routine services.

5. All Other Behavioral Health Services: Within 14 calendar days.

6. For services described in the Inpatient or 24-Hour Diversionary Services Discharge Plan:

    a. Non-24-Hour Diversionary Services – within two calendar days of discharge;

    b. Medication Management – within 14 calendar days of discharge;

    c. Other Outpatient Services – within seven calendar days of discharge; and

    d. Intensive Care Coordination Services – within the time frame directed by EOHHS.

7. The Contractor shall ensure that Network Providers offer hours of operation that are no less than the hours of operation offered to commercially-insured individuals or MassHealth Fee- For-Service if the Provider serves only Covered Individuals or other Members.

8. The Contractor shall have a system in place to monitor and document access and appointment scheduling standards. The Contractor shall use statistically valid sampling methods for monitoring compliance with the appointment/access standards specified above in **Section 2.9.B** and shall promptly address any access deficiencies, including but not limited to taking corrective action if there is a failure to comply by a Provider. Annually, in accordance with **Appendix E-1**, the Contractor shall evaluate and report to EOHHS Network-wide compliance with the access standards specified in **Section 2.9.B**.

C. Availability

The Contractor shall:

1. Execute and maintain written contracts with Providers to ensure that Covered Individuals have access to BH Covered Services within a reasonable distance and travel time from the Covered Individual's residence, as provided below. The Contractor shall take into account both walking and public transportation.

2. Ensure that Network Providers provide physical access, communication access, accommodations, and accessible equipment for Covered Individuals with physical or mental disabilities.

3. Monitor the practice of creating waiting lists for Covered Individuals who seek outpatient BH Covered Services. If the Contractor determines that a Network Provider has established a waiting list, the Contractor shall create a plan to identify such Network Providers and help them reduce such waiting lists, with the goal of eliminating them. Such activity shall include but not be limited to the Contractor directly assisting Covered Individuals to find an appropriate alternative Provider. The Contractor shall further ensure that:

    a. Waiting lists are established and maintained in such a way as to not violate the provisions of M.G.L. c. 151B, including waiting for appointments after the initial appointment; and

    b. Network Providers with waiting lists refer Covered Individuals to other qualified Network Providers who do not have waiting lists.

4. Maintain a sufficiently broad and robust Provider Network to ensure that, the following standards are met:

    a. it includes in its Network a sufficient number of Behavioral Health Providers to meet the time and distance requirements set forth in **Appendix P** to the extent qualified, willing providers are available.

    b. in addition to the Availability requirements set forth in **Appendix P**, the Contractor shall include in its Network:

        1) At least one Network Provider of each Behavioral Health Covered Service set forth in **Appendix A-1** in every Service Area of the state served by the Contractor or, as determined by EOHHS, to the extent that qualified, interested Providers are available;

        2) Providers set forth in **Appendix A-2** in accordance with the geographic distribution set forth in such appendix, as updated by EOHHS from time to time.

    c. [Reserved];

    d. Intensive Care Coordination and Family Support and Training Services provided by Community Service Agencies as available based on the CSA Provider list in **Appendix A-2, Exhibit 9**;

    e. Other Intensive Home and Community-Based Services, which require Network Providers to travel to the Covered Individual's residence for services, must be available in all cities and towns in the Commonwealth; and

f. All other BH Covered Services within 30 miles or 30 minutes' travel time from the Covered Individual's residence, whichever requires less travel time.

5. Notwithstanding the generality of the foregoing, ensure access to at least one Network Provider, of each BH Covered Service in every geographic region of the state with more than 2.5 percent of Covered Individuals or, as determined by EOHHS, to the extent that qualified, interested Providers are available.

6. Ensure that access to BH Covered Services for Covered Individuals is consistent with the degree of urgency, as set forth in **Section 2.9B**.

7. Offer Covered Individuals who require readmission to Inpatient Mental Health Services readmission to the same Network Provider when there is a bed available in that facility.

8. Include, in its network of Community-Based Acute Treatment providers, providers with the clinical expertise to provide specialized CBAT services to youth with ASD/IDD as directed by EOHHS. The Contractor shall pay such providers at the rate specified in **Appendix L**.

9. Permit Covered Individuals to self-refer to any BH Network Provider of their choice for Medically Necessary Behavioral Health Covered Services and to change BH Providers at any time;

10. Ensure that Covered Individuals have access to a choice of at least two Network Providers who provide Behavioral Health Services to the extent that qualified, willing Providers are available. The Contractor shall ensure that non-English speaking Covered Individuals have a choice of at least two BH Providers within each BH Covered Service as described in **Section 2.9.C.4** in identified Prevalent Languages, provided that such provider capacity exists within a service area.

11. Demonstrate access and availability of BH Covered services by complying with all applicable reporting requirements, including identifying, taking into consideration, and separately reporting on provider specialists with limited Network Provider Agreements, such as single case agreements.

12. At least quarterly, identify Network Providers included in the Contractor's Provider Directory who have not submitted at least two claims for BH Covered Services to Covered Individuals in the past 12 months. The Contractor shall report a list of such providers to EOHHS by BH Covered Service type and geographic location along with the Contractor's network adequacy reports. The Contractor shall examine and describe in its report to EOHHS the extent to which Covered Individuals have meaningful access to these BH Providers in the Network and whether these BH Providers should remain listed in the Provider Directory.

13. At least quarterly, conduct secret shopper and other activities to ensure that the Contract's access requirements are met, and report on findings to EOHHS within 30 days of the end of the quarter, including how the Contractor intends to address issues identified as part of these activities.

14. If the Contractor or EOHHS identifies or anticipates that the Provider Network will not be sufficient to meet the access standards of this Contract for a Covered Service in any location or for any population of Covered Individuals, the Contractor shall notify EOHHS of its strategy for enhancing its network and its contingency plan for connecting impacted Covered Individuals to care.

D. Other Accessibility and Availability Requirements

1. The Contractor may request an exception to the accessibility and availability standards set forth in this Section by submitting a written request to EOHHS. EOHHS will grant such a request only if:

   a. Such request includes alternative standards that are equal to or better than the usual and customary community standards for accessing care and the standards specified in this Section. Such requests must include data on local providers available to the non-Medicaid population.

   b. Upon approval by EOHHS, the Contractor shall notify Covered Individuals in writing of such alternative access standards.

   c. If EOHHS grants the Contractor an exception to a specific accessibility or appointment availability standard, the exception is limited to the identified provider type and geographic region and is granted for a period of up to one (1) year, at which point the Contractor may submit a new request. The Contractor shall describe how it will reasonably deliver Covered Services to Enrollees who may be affected by the exception and how it will work to increase access to the provider type in the designated geographic region.

   d. The Contractor shall monitor, track, and at least annually report to EOHHS on the delivery of such Covered Services to Covered Individuals potentially affected by the exception.

2. Direct Access to Specialists

   For Covered Individuals including, but not limited to, Covered Individuals with special health care needs, determined through an assessment by appropriate health care professionals to need a course of treatment or regular care monitoring, the Contractor shall have a mechanism in place to allow Covered Individuals direct access to a specialist(s) (for example, through a standing referral or an approved number of visits) as appropriate for the Covered Individual's condition and identified needs.

3. Through the execution of Provider Agreements, maintain and monitor a Network of appropriate providers that is sufficient to provide adequate access to all BH Covered Services for all Covered Individuals, including those with limited English proficiency or physical or mental disabilities. When directed by EOHHS, such Providers must be enrolled with the Contractor as specified by EOHHS. The Contractor may execute Network Provider agreements for up to 120 days pending the outcome of EOHHS's enrollment process, but must terminate a Network Provider immediately upon notification from EOHHS that the Network Provider cannot be enrolled, or the expiration of one 120 day period without enrollment of the provider. The Contractor shall notify affected Covered Individuals of the termination.

4. Assure EOHHS that it has the capacity to service expected enrollment of Covered Individuals in accordance with the accessibility and availability standards specified in this Section by submitting the access and availability reports specified in **Appendix E-1**.

E. Certification to EOHHS

The Contractor shall provide to EOHHS, in accordance with the timeframes and other requirements specified by EOHHS all reports, data or other information EOHHS determines necessary for compliance with 42 CFR 438.207(d). Such information shall include a certification, in a form and format specified by EOHHS, attesting that the Contractor satisfies all Contract requirements regarding network adequacy, as well as any supporting documentation specified by EOHHS.

If the Contractor does not comply with the access standards specified in this Section, the Contractor shall take corrective action necessary to comply with such access standards and may be subject to financial penalties or other sanctions.

Section 2.10 Customer Services for Covered Individuals

A. Written Materials, Electronic Information and Handbooks

1. Written Materials

a. Unless otherwise provided in this Contract, the Contractor must ensure that all written materials provided by the Contractor to Covered Individuals:

1) Are Culturally and Linguistically Appropriate, reflecting the diversity of the Contractor's membership;

2) Are produced in a manner, format, and language that may be easily understood by persons with limited English proficiency;

3) Are translated into Prevalent Languages of the Contractor's membership;

4) Are made available in Alternative Formats upon request free-of-charge, including video and audio; and information is provided about how to access written materials in those formats and about the availability of free auxiliary aids and services, including, at a minimum, services for Covered Individuals with disabilities;

5) Are mailed with a language card that indicates that the enclosed materials are important and should be translated immediately, and that provides information on how the Enrollee may obtain help with getting the materials translated;

6) Use a font size no smaller than 12 point; and,

7) Include a large print tagline (i.e., no smaller than 18 point font size).

b. The Contractor shall ensure all written materials intended for general distribution to Covered Individuals, Uninsured Individuals, Providers and Primary Care Clinicians (PCCs) are up to professional business standards, and in compliance with 42 CFR 438.10, before submitting them to EOHHS for review and approval and prior to publication.

2. Electronic Information

The Contractor may only provide Covered Individuals information in electronic form if the following requirements are met:

a. The format is readily accessible;

b. The information is placed in a location on the Contractor's web site that is prominent and readily accessible;

c. The information is provided in an electronic form which can be electronically retained and printed;

d. The information is consistent with the content and language requirements of this Contract; and

e. The Enrollee is informed that the information is available in paper form without charge upon request and the Contractor provides it upon request within 5 business days.

3. Handbook

a. The Contractor must develop, using a model to be provided by EOHHS to the Contractor, a Covered Individual handbook, which serves as a

summary of benefits and coverage and will be included in the PCC Plan and PCACO, or utilized as a separate handbook for those Covered Individuals that are not enrolled in the PCC Plan or a PCACO.

b. At a minimum, this handbook shall contain all of the information required by 42 CFR 438.10(g), including:

1) The benefits provided by the Contractor;

2) How to access BH Covered Services, including the amount, duration and scope of BH Covered Services, in sufficient detail to ensure that Covered Individuals understand the benefits to which they are entitled and the procedures for obtaining such benefits, including the Contractor's toll-free telephone line(s), authorization requirements, information regarding applicable access and availability standards, any cost sharing, self-referral, and referral by family members or guardians, a Provider, PCP or community agency;

3) Inform Covered Individuals of the availability of assistance through the MassHealth Contact Center for help with determining where and how to access non-BH Covered Services. In the case of a counseling or referral service that the Contractor does not cover because of moral or religious objections, the handbook must inform Covered Individuals that the service is not covered by the Contractor;

4) The name and customer services telephone number for all Material Subcontractors that provide BH Covered Services to Covered Individuals unless the Contractor retains all customer service functions for such BH Covered Services;

5) The BH Covered Services that do not require authorization or a referral from the Covered Individual's PCP;

6) The extent to which, and how, Covered Individuals may obtain benefits, including Emergency Services, from out-of-network providers;

7) The role of the PCP, and the policies on referrals for specialty care and for other benefits not furnished by the Covered Individual's PCP;

8) How to obtain information about Network Providers;

9) The extent to which, and how, after-hours and Emergency Services and Poststabilization Care Services are covered, including:

a) What constitutes an Emergency Medical Condition, Emergency Services, and Poststabilization Care Services;

b) The fact that prior authorization is not required for Emergency Services;

c) How to access the Contractor's toll-free 24-hour Clinical Advice and Support Line,

d) The process and procedures for obtaining Emergency Services, including the use of the 911-telephone system;

e) The services provided by CBHCs and how to access them;

f) The locations of any emergency settings and other locations at which Providers and hospitals furnish Emergency Services; and

g) The fact that the Covered Individual has a right to use any hospital or other setting for Emergency Services;

10) Covered Individual cost sharing;

11) Any restrictions on freedom of choice among Network Providers;

12) The availability of free oral interpretation services at the Plan in all non-English languages spoken by Covered Individuals and how to obtain such oral interpretation services;

13) The availability of all written materials that are produced by the Contractor for Covered Individuals in Prevalent Languages and how to obtain translated materials;

14) The availability of all written materials that are produced by the Contractor for Covered Individual in Alternative Formats and how to access written materials in those formats and the availability of auxiliary aids and services;

15) The toll-free Covered Individual services telephone number and hours of operation, and the telephone number for any other unit providing services directly to Covered Individuals;

16) The rights and responsibilities of Covered Individuals;

17) Information on Grievance, Internal Appeal, and Board of Hearing (BOH) procedures and timeframes, including:

a) The right to file Grievances and Internal Appeals;

b) The requirements and timeframes for filing a Grievance or Internal Appeal;

c) The availability of assistance in the filing process;

d) The toll-free numbers that the Covered Individual can use to file a Grievance or an Internal Appeal by phone;

e) The fact that, when requested by the Covered Individual, BH Covered Services will continue to be provided if the Covered Individual files an Internal Appeal or a request for a BOH hearing within the timeframes specified for filing, and that the Covered Individual may be required by EOHHS to pay the cost of services furnished while a BOH Appeal is pending, if the final decision is adverse to the Covered Individual;

f) The right to obtain a BOH hearing;

g) The method for obtaining a BOH hearing;

h) The rules that govern representation at the BOH hearing; and

i) The right to file a grievance directly with EOHHS, how to do so, and EOHHS contact information;

18) Information on advance directives in accordance with **Section 5.1.E**;

19) Information on the access standards specified in **Section 2.9.B**;

20) Information on how to report suspected fraud or abuse; and

21) Information about continuity and transition of care for new Covered Individuals.

c. The Contractor shall distribute this handbook to each Covered Individual as follows:

1) For each existing Covered Individual, the Contractor shall, upon request:

a) Mail a printed copy of the handbook to the Covered Individual at his or her mailing address;

b) Provide an electronic copy of the handbook by electronic mail after obtaining the Covered Individual's agreement to receive the information by electronic mail;

c) Post the handbook on its website and advise the Covered Individual, in both paper and electronic form, that the handbook is available on the internet, including the appropriate URL, provided that Covered Individuals with disabilities who cannot access the handbook online are provided auxiliary aids and services upon request at no cost; and

d) Provide the handbook by any other method that can reasonably be expected to result in the Covered Individual receiving the information contained in the handbook.

2) For new Covered Individuals, the Contractor shall, upon request, within a reasonable time after receiving notice of the Member's enrollment with the Contractor, distribute, upon request, the handbook in accordance with **Section 2.10.A.3.c.1** above.

d. The Contractor shall give Covered Individuals notice of any significant change in the information set forth in **Section 2.10.A.3**, as determined by EOHHS, at least 30 days before the intended effective date of the change.

4. Notices

The Contractor shall develop Covered Individual notices using models to be provided by EOHHS to the Contractor.

B. Covered Individual Services Department, Standards, and Staff

1. The Contractor must maintain a Covered Individual services department to assist Covered Individuals and their family members or guardians, and other interested parties in learning about and obtaining services under this Contract.

2. The Contractor must maintain employment standards and requirements (e.g., education, training, and experience) for Covered Individual services department staff and provide a sufficient number of staff for the Covered Individual services department.

C. Customer Service Telephone Line, Training, and Requirements

1. The Contractor must operate a toll-free Covered Individual services telephone line a minimum of nine hours per day during normal business hours, Monday through Friday, which shall:

a. Have at least 90% of calls answered by a trained customer service department representative (non-recorded voice), within 30 seconds or less as reported in accordance with **Appendix E-1**;

b. Have less than a 5% abandoned call rate;

c. Make oral interpretation services available free-of-charge to Covered Individuals in all non-English languages spoken by Covered Individuals; and

d. Maintain the availability of service free-of-charge, such as TTY services or comparable services for the deaf and hard of hearing;

2. The Contractor must establish a schedule of intensive training for newly-hired and current customer service representatives about Medicaid and MassHealth benefits, customer service and motivational interviewing techniques and any other relevant training the Contractor deems necessary for staff to successfully engage with Members, including the Health Equity training requirements in **Section 2.8.I.4.f**.

D. Information for Covered Individuals and Potential Covered Individuals

The Contractor must, upon request, make available to Covered Individuals and Potential Covered Individuals in the Contractor's Plan information about:

1. The identity, locations, qualifications, and availability of Providers;

2. The rights and responsibilities of Covered Individuals including, but not limited to, those Covered Individual rights described in **Section 5.1.L**;

3. The procedures available to all Covered Individuals and Provider(s) to challenge or appeal the failure of the Contractor to provide a covered service and to appeal any Adverse Action as explained in the Covered Individual handbook;

4. How Covered Individuals and Potential Covered Individuals may access oral interpretation services free-of-charge in any non-English language spoken by Covered Individuals and Potential Covered Individuals;

5. How Covered Individuals and Potential Covered Individuals may access written materials in Prevalent Languages and Alternative Formats;

6. All BH Covered Services and non-BH Covered Services that are available to Covered Individuals either directly or through referral or authorization; and

7. Additional information that may be required by Covered Individuals and Potential Covered Individuals to understand the requirements and benefits of the Plan.

E. Website

The Contractor shall:

1. No later than two months prior to the Operational Start Date, develop and submit for EOHHS's approval a plan for a website containing information specifically related to the Contract.

2. Launch the website as of the Operational Start Date, and maintain it subject to EOHHS's approval.

3. Provide a link from the website to EOHHS's website, including, as further specified by EOHHS, a direct link to MassHealth supported provider directory.

4. Include, at a minimum, the following on its website:

    a. Culturally and linguistically competent information for Covered Individuals regarding services available through the BHP;

    b. A searchable BH Provider Network Directory that is updated at least monthly and as needed;

    c. As directed by EOHHS, a searchable PCC Plan Provider Directory for non-BH providers that is updated at least monthly and more frequently as needed;

    d. The BH Network Provider manual;

    e. The PCC Plan Provider handbook;

    f. The PCC Plan and PCACO Member handbooks;

    g. BHP-only handbook for Covered Individuals that are not enrolled in the PCC Plan or with a PCACO;

    h. Educational materials and links to evidence-based practices;

    i. Information and materials to support integration between Network Providers and PCPs;

    j. Community resources;

    k. As directed by EOHHS, links to PCACOs, Community Partners, and other related websites; and,

    l. Covered Services Lists.

5. Develop and propose to EOHHS within six months following the Contract Start Date a secure Provider and Covered Individual portal as part of the website.

6. Not provide any link to the Contractor's corporate website on any part of the website, unless agreed to by EOHHS.

7. Not provide any link to any type of corporate promotion on any part of the website.

8. Verify and certify to EOHHS on a quarterly basis the accuracy of all information contained on the website.

9. Data Gathering and Reporting Capacity in the Massachusetts Behavioral Health Access (MABHA) Website.

a. Subject to further direction and specification by EOHHS, the Contractor shall collect and report data regarding any MassHealth Member waiting over 24 hours for a 24 Hour Level of Care Placement or on Administratively Necessary Days (AND) status in a 24 Hour Level of Care, as follows:

1) The Contractor shall build and maintain a platform on the Massachusetts Behavioral Health Access (MABHA) website (the "MABHA Platform") to collect and manage the data;

2) The Contractor shall report to EOHHS on Members awaiting placement within a 24-hour level of care or who are on Administratively Necessary Days (AND) status within a 24 hour level of care, respectively, as follows:

a) Member-level reporting on a daily, weekly, and monthly basis;

b) Aggregate reporting on a quarterly and annual basis; and

c) Additional reporting in a form and frequency as requested by EOHHS on an ad hoc basis;

3) The Contractor shall establish a process for CBHCs set forth in **Appendix A-2, Exhibit 1** to input data on individuals who receive services on a fee-for-service basis or who have Third-Party Liability who are waiting over 24 hours for a 24 hour level of care into the MABHA Platform;

4) The Contractor shall establish a process for MassHealth managed care entities and others specified by EOHHS to input data on Members awaiting placement within a 24-hour level of care or who are on Administratively Necessary Days (AND) status within a 24 hour level of care into the MABHA Platform;

5) As directed by EOHHS, the Contractor shall create capacity for MassHealth managed care entities and others specified by EOHHS to view and print reports from the MABHA Platform in a manner allowable under federal and state privacy laws; and

6) The Contractor shall manage access of MassHealth managed care entities and others specified by EOHHS to the MABHA Platform at appropriate security levels.

b. The Contractor acknowledges and agrees that the data to be collected, managed, maintained, reported and otherwise used by the Contractor in developing and maintaining the MABHA website will include Protected

Health information (PHI), as defined in 45 CFR §160.103, and other types of Personal Information (PI). The Contractor further acknowledges and agrees that in collecting, managing, maintaining, transmitting, disclosing and/or using such data for purposes of performing these activities. it is doing so in the capacity of EOHHS' Business Associate, as defined in 45 CFR §160.103, and is subject to, and shall comply with, all applicable terms, conditions and requirements set forth in **Section 5** hereof, including those relating to the Contractor's compliance with the Privacy and Security Rules as the Business Associate of EOHHS. Without limiting the generality of the foregoing, the Contractor agrees that the collection, management, maintenance and use of PI in and using the MABHA Platform shall comply with all applicable security requirements to which Contractor is subject, including those applicable under **Section 5** hereof.

10. Pursuant to Chapter 52 of the Acts of 2016 of the Massachusetts General Laws, Section 61, the Contractor shall post contact information for all insurance payers, including a phone number which is accessible 24 hours per day, for the purpose of enhancing communication between payers and providers.

F. Eligibility Redetermination Assistance

The Contractor is authorized and directed to communicate with Covered Individuals to help them renew their MassHealth coverage. The Contractor is authorized and directed to make appropriate use of prerecorded or artificial autodialed calls and automated texts in compliance with the Federal Communications Commission January 23, 2023, Declaratory Ruling. The Contractor shall consult its legal counsel about the appropriate use of autodialed calls and automated texts to Covered Individuals pursuant to the FCC Declaratory Ruling. The Contractor shall be responsible for complying with the ruling.

Section 2.11 Marketing Activity Requirements

A. General Requirements

In conducting any Marketing activities described herein, the Contractor shall:

1. Ensure that all Marketing Materials regarding the Contractor's services under this Contract clearly state that information regarding all MassHealth Managed Care enrollment options including, but not limited to, the Contractor's Plan, are available from the MassHealth Contact Center. The Contractor shall ensure that all written Marketing Materials prominently display the telephone number and hours of operation of the MassHealth Contact Center in the same font size as the same information for the Contractor's customer service center. EOHHS, in its sole discretion, may exempt, in writing, promotional materials or activities from this requirement upon written request by the Contractor;

2. Comply with all applicable information requirements set forth in 42 CFR 438.10 when conducting Marketing activities and preparing Marketing Materials;

3. Submit all Marketing Materials to EOHHS for review and approval prior to distribution. The Contractor shall submit Marketing Materials to EOHHS for approval 60 days prior to distribution or as early as possible;

4. Comply with any requirement imposed by EOHHS pursuant to **Section 2.11.B** of this Contract;

5. Distribute and/or publish Marketing Materials statewide, unless the Contractor submits a written request which is approved by EOHHS to implement a targeted Marketing campaign. A targeted Marketing campaign involves distributing and/or publishing materials where the campaign relates to a local event (such as a health fair) or to a single Provider (such as a hospital or clinic), to a certain zip code or zip codes; and

6. Provide EOHHS with a copy of all press releases pertaining to the Contractor's MassHealth line of business for prior review and approval.

B. Permissible Marketing Activities

The Contractor may engage in only the following Marketing activities, in accordance with the requirements stated in **Section 2.11.A** above.

1. The Contractor may participate in a health fair or community activity sponsored by the Contractor provided that the Contractor shall notify all MassHealth-contracted Accountable Care Partnership Plans or MCOs within the geographic region of their ability to participate. Such notification shall be in writing and shall be made as soon as reasonably possible prior to the date of the event. If other MassHealth-contracted Accountable Care Partnership Plans or MCOs choose to participate in a Contractor's sponsored event, they shall contribute to the costs of such event as a condition of participation, provided costs are reasonably apportioned among the MassHealth-contracted Accountable Care Partnership Plans and MCOs. The Contractor may conduct or participate in Marketing at Contractor or non-Contractor sponsored health fairs and other community activities only if:

    a. Any Marketing Materials the Contractor distributes have been pre-approved by EOHHS; and

    b. Any free samples and gifts offered by the Contractor are only of a nominal value and are available to all attendees of the health fair or other community activity regardless of their intent to enroll in the Contractor's Plan.

2. The Contractor may participate in Health Benefit Fairs sponsored by EOHHS.

3. The Contractor may market to Covered Individuals by distributing and/or publishing Marketing Materials or implementing a targeted Marketing campaign that is pre-approved by EOHHS. The methods for distributing and/or publishing Marketing Materials may include:

   a. Posting written Marketing Materials that have been pre-approved by EOHHS at Network or PCC Provider sites and other locations; and posting written promotional Marketing Materials throughout the state;

   b. Initiating mailing campaigns that have been pre-approved by EOHHS, where the Contractor distributes Marketing Materials by mail; and

   c. Television, radio, newspaper, website postings, and other audio or visual advertising.

C. Prohibitions on Marketing and Enrollment Activities

The Contractor shall not:

1. Distribute any Marketing Material that has not been pre-approved by EOHHS;

2. Distribute any Marketing Material that is inaccurate or false or that misleads, confuses, or defrauds the recipient of the Marketing Material, including but not limited to, any assertion or statement, whether written or oral, that:

   a. The recipient of the Marketing Material must enroll in the Contractor's Plan, the PCC Plan, or a Primary Care ACO in order to obtain benefits or in order to not lose benefits; or

   b. The Contractor is endorsed by CMS, the federal or state government or similar entity;

3. Seek to influence a Member's enrollment in the Contractor's Plan, the PCC Plan, or a Primary Care ACO in conjunction with the sale or offering of any private or non-health insurance products (e.g., life insurance);

4. Seek to influence a Member's enrollment into the Contractor's Plan, the PCC Plan, or a Primary Care ACO in conjunction with the sale or offering of cash, cash equivalents or in-kind gifts;

5. Directly or indirectly, engage in door-to-door, telephonic, email, texting, or any other Cold-call Marketing activities;

6. Engage in any Marketing activities which could mislead, confuse or defraud Members or Enrollees, or misrepresent MassHealth, EOHHS, the Contractor or CMS;

7. Conduct any Provider site Marketing, except as provided in **Section 2.11.B.3**;

8. Incorporate any costs associated with Marketing or Marketing incentives, or Non-Medical Programs or Services in the report specified in **Appendix E-1**; or

9. Engage in Marketing activities which target Members on the basis of health status or future need for health care services, or which otherwise may discriminate against individuals eligible for health care services.

D. Marketing Plan and Schedules

1. The Contractor shall make available to EOHHS, for review and approval upon request, a comprehensive Marketing plan, including proposed Marketing approaches, current schedules of all Marketing activities, and the methods, modes, and media through which Marketing Materials will be distributed.

2. Annually, the Contractor shall present its Marketing plan in person to EOHHS for review and approval.

3. The Contractor shall annually submit to EOHHS a written statement including an executive summary of its MassHealth Marketing plans and a statement that all of its Marketing plans and Marketing Materials are accurate and do not mislead, confuse, or defraud Members or misrepresent the state, and are otherwise in accordance with the requirements of 42 CFR 438.104.

Section 2.12 Inquiries, Ombudsman Services, Grievances, and Appeals

A. General Requirements

The Contractor shall:

1. Maintain written policies and procedures for:

   a. The receipt and timely resolution of Grievances and Internal Appeals, as further described in **Section 2.12.B**, below. Such policies and procedures shall be approved by EOHHS; and

   b. The receipt and timely resolution of inquiries, where timely resolution means responding to the Inquiry at the time it is raised to the extent possible or, if not possible, acknowledging the inquiry within one business day and making best efforts to resolve the inquiry within one business day of the initial inquiry. Such policies and procedures shall be approved by EOHHS.

2. Review the inquiry, Grievance and Internal Appeals policies and procedures established pursuant to **Section 2.12.B**, at least annually, to amend and improve those policies and procedures. The Contractor shall provide copies of any such amendments to EOHHS, for review and approval, 30 calendar days prior to the date of the amendment, unless otherwise specified by EOHHS;

3. Create and maintain records of inquiries, Grievances, Internal Appeals, and BOH Appeals, using the health information system(s) specified in **Section 3.4**, to document:

   a. The type and nature of each inquiry, Grievance, Internal Appeal, and BOH Appeal;

   b. How the Contractor disposed of or resolved each Grievance, Internal Appeal, or BOH Appeal; and

   c. What, if any, corrective action the Contractor took.

4. Report to EOHHS annually regarding inquiries, Grievances, Internal Appeals and BOH Appeals, as described in **Appendix E-1**;

5. Assure that individuals with authority, such as senior and executive level staff, participate in any corrective action that the Contractor determines is necessary following the resolution of any inquiry, Grievance, Internal Appeal, or BOH Appeal;

6. Provide Covered Individuals with information about Grievance, Internal Appeal, and BOH Appeal procedures and timeframes, as specified in **Section 2.12.B**; and

7. Pursuant to 42 CFR 438.414, provide the information specified in **Section 2.10.A.3.17** to all Providers and Material Subcontractors at the time they enter into a contract with the Contractor.

8. In addition to other obligations set forth in this Contract related to Ombudsman Services, the Contractor shall support Covered Individual access to, and work with, the Ombudsman to address Covered Individual requests for information, issues, or concerns related to the Contractor by:

   a. Providing Covered Individuals with education and information about the availability of Ombudsman services including when Covered Individuals contact the Contractor with requests for information, issues, concerns, complaints, Grievances, Internal Appeals or BOH Appeals;

   b. Communicating and cooperating with Ombudsman staff as needed for such staff to address Covered Individual requests for information, issues, or concerns related to the Contractor, including:

      1) Providing Ombudsman staff, with the Covered Individual's appropriate permission, with access to records related to the Covered Individual; and

      2) Engaging in ongoing communication and cooperation with Ombudsman staff until the Covered Individual's request or

concern is addressed or resolved, as appropriate, including but not limited to providing updates on progress made towards resolution.

B. Grievances and Internal Appeals

The Contractor shall maintain written policies and procedures for the filing by Covered Individuals or Appeals representatives and the receipt, timely resolution, and documentation by the Contractor of any and all Grievances and Internal Appeals which shall include, at a minimum, the following, in accordance with 42 CFR Part 438, Subpart F. (For purposes of this Section, in cases where a minor is able, under law, to consent to a medical procedure, that a minor can request an appeal of the denial of such treatment, or may appoint an Appeal Representative to represent them, without parental/guardian consent.)

1. General Requirements

a. The Contractor shall put in place a standardized process that includes:

1) A means for assessing and categorizing the nature and seriousness of a Grievance or Internal Appeal;

2) A means for tracking how long the Contractor takes to dispose of or resolve Grievances and Internal Appeals and to provide notice of such disposition or resolution, as specified in **Sections 2.12.B.2** below; and

3) A means for expedited resolution of Internal Appeals, as further specified in **Section 2.12.B.2.c.4**, when the Contractor determines (for a request from the Covered Individual) or a Provider indicates (in making the request on the Covered Individual's behalf or supporting the Covered Individual's request) that taking the time for a standard resolution, in accordance with **Section 2.12.B.2.c.3**, could seriously jeopardize the Covered Individual's life or health or ability to attain, maintain, or regain maximum function.

b. The Contractor shall put in a place a mechanism to:

1) Accept Grievances at any time filed either orally or in writing; and

2) Accept Internal Appeals filed either orally or in writing within 60 calendar days from the notice of Adverse Action specified in **Section 2.12.B.2**, provided that if an Internal Appeal is filed orally, the Contractor shall not require the Covered Individual to submit a written, signed Internal Appeal form subsequent to the Covered Individual's oral request for an appeal. Internal Appeals filed later than 60 days from the notice of Adverse Action may be rejected as untimely.

c. The Contractor shall send a written acknowledgement of the receipt of any Grievance or Internal Appeal to Covered Individuals and, if an Appeals representative filed the Grievance or Internal Appeal, to the Appeals representative and the Covered Individual within one business day of receipt by the Contractor.

d. The Contractor shall track whether an Internal Appeal was filed orally or in writing within 60 calendar days from the notice of Adverse Action specified in **Section 2.12.B.2**.

2. Notice of Adverse Action

The Contractor shall put in place a mechanism for providing written notice to Covered Individuals of any Adverse Action in a form approved by EOHHS as follows:

a. The notice must meet the language and format requirements specified in **Sections 2.10.A**.

b. The notice must explain the following:

1) The Adverse Action the Contractor has taken or intends to take;

2) The reason(s) for the Adverse Action, including the right of the Covered Individual to be provided, upon request and free of charge, reasonable access to and copies of all documents, records, and other information relevant to the Adverse Action, such as medical necessity criteria and processes, strategies, and standards related to the Adverse Action;

3) The Covered Individual's right to file an Internal Appeal or to designate an Appeal Representative to file an Internal Appeal on behalf of the Covered Individual, including exhausting the appeal process and right to file an appeal with the Board of Hearings;

4) The procedures for a Covered Individual to exercise his/her right to file an Internal Appeal;

5) The circumstances under which expedited resolution of an Internal Appeal is available and how to request it;

6) That the Contractor will provide the Covered Individual Continuing Services, if applicable, pending resolution of the review of an Internal Appeal if the Covered Individual submits the request for review within 10 days of the Adverse Action; and

7) That the Contractor will provide the Covered Individual Continuing Services, if applicable, pending resolution of a BOH

Appeal if the Covered Individual submits the request for the BOH Appeal within 10 days of receipt of notice of the Final Internal Appeal decision, unless the Covered Individual specifically indicates that he or she does not want to receive Continuing Services.

c. The notice must be mailed within the following timeframes:

1) For termination, suspension, or reduction of a previous authorization for a requested service, at least 10 calendar days prior to the Date of Action in accordance with 42 CFR 431.211, except as provided in 42 CFR 431.213. In accordance with 42 CFR 431.214, the period of advance notice may be shortened to five calendar days before the Date of Action if the Contractor has facts indicating that action should be taken because of probable fraud by the Covered Individual and the facts have been verified, if possible, through secondary sources.

2) For denial of payment where coverage of the requested service is at issue, on the day of the payment denial, except that no notice is necessary for procedural denials of payment where coverage of the requested service is not at issue, which include, but are not limited to, denials for the following reasons:

a) Failure to follow prior authorization procedures;

b) Failure to follow referral rules; and

c) Failure to file a timely claim.

3) For standard service authorization decisions that deny or provide limited authorization for requested services, as specified in **Section 2.6.C.2.c**, as expeditiously as the Covered Individual's health condition requires but no later than 14 calendar days following receipt of the service request, unless the timeframe is extended up to 14 additional calendar days.

a) Extensions to the notice requirements outlined in **Section 2.12.B.2.c** above shall only be allowed if:

(i) The Provider, Covered Individual or Appeal Representative requests the extension; or

(ii) The Contractor can justify (to EOHHS, upon request) that the extension is in the Covered Individual's interest, and there is a need for additional information where there is a reasonable likelihood that the receipt

of such information would lead to approval of the request, if received, and such outstanding information is reasonably expected to be received within 14 calendar days.

b) If the Contractor extends the timeframe, it must give the Covered Individual written notice of the reason for the extension and inform the Covered Individual of the right to file a Grievance if the Covered Individual disagrees with that decision issue and carry out its determination as expeditiously as the Covered Individual's health condition requires and no later than the date the extension expires.

4) For expedited service authorization decisions that deny or provide limited authorization for requested services, as specified in **Section 2.12.B.2.c**, as expeditiously as the Covered Individual's health requires but no later than 3 business days after the receipt of the expedited request for service, unless the timeframe is extended up to 14 additional days.

a) The extension shall only be allowed if:

(i) The Provider, Covered Individual, or Appeal Representative requests the extension; or

(ii) The contractor can justify (to EOHHS upon request) that the extension is in the Covered Individual's interest and there is a need for additional information where there is a reasonable likelihood that the receipt of such information would lead to approval of the request, if received and such outstanding information is reasonably expected to be received within 14 calendar days.

b) If the Contractor extends the timeframe, it must give the Covered Individual written notice of the reason for the extension and inform the Covered Individual of the right to file a Grievance if the Covered Individual disagrees with that decision issue and carry out its determination as expeditiously as the Covered Individual's health condition requires and no later than the date the extension expires.

5) For standard or expedited service authorization decisions not reached within the timeframes specified in **Sections 2.12.B.2.c.3 and 4**, whichever is applicable, on the day that such timeframes expire.

6) When the Contractor fails to provide services in a timely manner in accordance with the access standards in **Section 2.9.B**, within one business day upon notification by the Covered Individual or Provider that one of the access standards in **Section 2.9.B** was not met.

3. Handling of Grievances and Internal Appeals

In handling Grievances and Internal Appeals, the Contractor shall:

a. Inform Covered Individuals of the Grievance, Internal Appeal, and BOH Appeal procedures, as specified in **Section 2.12.A**.

b. Give reasonable assistance to Covered Individuals in completing forms and following procedures applicable to Grievances and Internal Appeals, including, but not limited to, providing interpreter services and toll-free numbers with TTY/TDD and interpreter capability;

c. Provide notice of Adverse Actions as specified in **Section 2.12.B.2**;

d. Accept Grievances and Internal Appeals filed in accordance with **Section 2.12.B.1.b**;

e. Send written acknowledgement of the receipt of each Grievance or Internal Appeal to the Covered Individual and Appeal Representative within one business day of receipt by the Contractor;

f. Ensure that the individuals who make decisions on Grievances and Internal Appeals:

1) Are individuals who were not involved in any previous level of review or decision-making, and are not the subordinates of any such individuals; and

2) Take into account all comments, documents, records, and other information submitted by the Covered Individual or the Appeal Representative without regard to whether such information was submitted or considered in the Adverse Action determination.

g. Ensure that the following types of Grievances are decided by health care professionals who have the appropriate clinical expertise in treating the Enrollee's medical condition, performing the procedure, or providing the treatment that is the subject of the Grievance:

1) An appeal of a denial that is based on lack of medical necessity;

2) Grievances regarding the denial of a Covered Individual's request that an Internal Appeal be expedited, as specified in **Section 2.12.B.4.d.3**; and

3) Grievances regarding clinical issues;

h. Ensure that the following special requirements are applied to Internal Appeals:

1) The Contractor shall offer one level of review of an Adverse Action for Internal Appeals;

2) All reviews of Internal Appeals shall be conducted by health care professionals who have the appropriate clinical expertise in treating the medical condition, performing the procedure, or providing the treatment that is the subject of the Adverse Action;

3) The Contractor shall treat an oral request seeking to appeal an Adverse Action as an Internal Appeal in order to establish the earliest possible filing date for Internal Appeals and shall not require the Covered Individual or an Appeal Representative to confirm such oral requests in writing as specified in **Section 2.12.B.1.b.2**;

4) The Contractor shall provide a reasonable opportunity for the Covered Individual or an Appeal Representative to present evidence and allegations of fact or law, in person as well as in writing, and shall inform the Covered Individual or an Appeal Representative about the limited time available for this opportunity in the case of expedited Internal Appeals;

5) The Contractor shall provide the Covered Individual and an Appeal Representative, before and during the Internal Appeals process, the Covered Individual's case file, including medical records, and any other documentation and records considered, relied upon, or generated during the Internal Appeals process. This information shall be provided free of charge and sufficiently in advance of the applicable resolution timeframe; and

6) The Contractor shall include, as parties to the Internal Appeal, the Covered Individual and Appeal Representative or the legal representative of a deceased Covered Individual's estate;

4. Resolution and Notification of Grievances and Internal Appeals

The Contractor shall:

a. Dispose of each Grievance, resolve each Internal Appeal, and provide notice of each disposition and resolution, as expeditiously as the Covered Individual's health condition requires, within the following timeframes:

1) For the standard resolution of Grievances and notice to affected parties, no more than 30 calendar days from the date the Contractor received the Grievance, either orally or in writing, from a valid party, e.g., the Covered Individual or the Covered Individual's Authorized Appeal Representative, unless this timeframe is extended in accordance with **Section 2.12.B.4.b**;

2) For standard resolution of Internal Appeals and notice to the affected parties, no more than 30 calendar days from the date the Contractor received either in writing or orally, whichever comes first, the Covered Individual request for an Internal Appeal unless this timeframe is extended under **Section 2.12.B.4.b**; and

3) For expedited resolution of Internal Appeals and notice to affected parties, no more than 72 hours from the date the Contractor received the expedited Internal Appeal unless this timeframe is extended under **Section 2.12.B.4.b**. The Contractor shall process the expedited Internal Appeal even if a Provider is allegedly serving as the Covered Individual's Appeal Representative, but the Contractor has still not received in writing the Authorized Appeal Representative form. The Contractor shall require that the Provider submit a signed Authorized Appeal Representative form to the Contractor as documentation that the Covered Individual did in fact authorize the Provider to file the expedited Internal Appeal on the Covered Individual's behalf, as long as the expedited Internal Appeal is not delayed waiting for the Authorized Appeal Representative form;

b. Extend the timeframes in **Section 2.12.B.4.a.1-3** by up to 14 calendar days if:

1) The Covered Individual or Appeal Representative requests the extension, or

2) The Contractor can justify (to EOHHS upon request) that:

a) The extension is in the Covered Individual's interest; and

b) There is a need for additional information where:

(i) There is a reasonable likelihood that receipt of such information would lead to approval of the request, if received; and

(ii) Such outstanding information is reasonably expected to be received within 14 calendar days;

3) For any extension not requested by the Covered Individual, the Contractor shall:

a) Make reasonable efforts to give the Covered Individual and Appeal Representative prompt oral notice of the delay;

b) Provide the Covered Individual and Appeal Representative written notice of the reason for the delay within 2 calendar days. Such notice shall include the reason for the extension of the timeframe and the Covered Individual's right to file a grievance; and

c) Resolve the appeal as expeditiously as the Covered Individual's health condition requires and no later than the date of extension expires.

c. Provide notice in accordance with **Section 2.12.B.4.a** regarding the disposition of a Grievance or the resolution of a standard Internal Appeal or an expedited Internal Appeal as follows:

1) All such notices shall be in writing in a form approved by EOHHS, and satisfy the language and format standards set forth in 42 CFR 438.10. For notices of an expedited Internal Appeal resolution, the Contractor shall also make reasonable efforts to provide oral notice to the Covered Individual; and

2) The notice shall contain, at a minimum, the following:

a) The results of the resolution process and the effective date of the Internal Appeal decision;

b) For Internal Appeals not resolved wholly in favor of the Covered Individual:

(i) The right to file a BOH Appeal and how to do so, and include the Request for a Fair Hearing Form; and

(ii) That the Covered Individual will receive Continuing Services, if applicable, while the BOH Appeal is pending if the Covered Individual submits the appeal request to the BOH within 10 days of the Adverse Action, unless the Covered Individual specifically indicates that he or she does not want to receive Continuing Services.

d. Resolve expedited Internal Appeals as follows:

1) The Contractor shall resolve Internal Appeals expeditiously in accordance with the timeframe specified in **Section 2.12.B.4.a.3** when the Contractor determines (with respect to an Enrollee's request for expedited resolution) or a Provider indicates (in making the request for expedited resolution on the Covered Individual's behalf or supporting the Covered Individual's request) that taking the time for a standard resolution could seriously jeopardize the Covered Individual's life or health or ability to attain, maintain, or regain maximum function. The Contractor shall process the expedited Internal Appeal even if the Provider is allegedly serving as the Covered Individual's Appeal Representative, but the Contractor has still not received in writing the Authorized Appeal Representative form.

2) The Contractor shall not take punitive action against Providers who request an expedited resolution, or who support a Covered Individual's Internal Appeal.

3) If the Contractor denies a Covered Individual's request for an expedited resolution of an Internal Appeal, the Contractor shall:

   a) Transfer the Internal Appeal to the timeframe for standard resolution in **Section 2.12.B.4.a.2** above;

   b) Make reasonable efforts to give the Covered Individual and Appeal Representative prompt oral notice of the denial, and follow-up within two calendar days with a written notice. Such notice shall include the Covered Individual's right to file a Grievance; and

   c) Resolve the appeal as expeditiously as the Covered Individual's health condition requires and no later than the applicable deadlines set forth in this Contract.

4) The Contractor shall not deny a Provider's request (on a Covered Individual's behalf) that an Internal Appeal be expedited unless the Contractor determines that the Provider's request is unrelated to the Covered Individual's health condition.

C. Board of Hearings

The Contractor shall:

1. Require Covered Individuals and their Appeal Representatives to exhaust the Contractor's Internal Appeals process before filing an appeal with the Board of Hearings (BOH). The exhaustion requirement is satisfied if either of the following conditions is met:

a. The Contractor has issued a decision following its review of the Adverse Action; or

b. The Contractor fails to act within the timeframes for reviewing Internal Appeals or fails to satisfy applicable notice requirements.

2. Include with any notice following the resolution of a standard Internal Appeal or an expedited Internal Appeal, as specified in **Section 2.12.B.4.c,** any and all instructive materials and forms provided to the Contractor by EOHHS that are required for the Covered Individual to request a BOH Appeal;

3. Notify Covered Individuals that:

a. Any Continuing Services being provided by the Contractor that are the subject of a BOH Appeal will continue, unless the Covered Individual specifically indicates that he or she does not want to receive Continuing Services; and

b. It is the Covered Individual's or the Appeal Representative's responsibility to submit any request for a BOH Appeal to the BOH and to ensure that the BOH receives the request within the time limits, as specified in 130 CMR 610.015(B)(7), specifically 120 days after the Enrollee's receipt of the Contractor's Final Internal Appeal Decision where the Contractor has reached a decision wholly or partially adverse to the Covered Individual, provided however that if the Contractor did not resolve the Covered Individual's Internal Appeal within the time frames specified in this Contract and described by 130 CMR 508.010(A), 120 days after the date on which the time frame for resolving that Internal Appeal has expired.

4. Be a party to the BOH Appeal, along with the Covered Individual and their representative or the representative of a deceased Covered Individual's estate.

D. Additional Requirements

The Contractor shall:

1. For all Final Internal Appeal Decisions upholding an Adverse Action, in whole or in part, the Contractor shall provide EOHHS upon request, within one business day of issuing the decision, with a copy of the decision sent to the Covered Individual and Appeal Representative, as well as all other materials associated with such Appeal, to assist in EOHHS's review of the Contractor's determination. This requirement shall also apply to situations when the Contractor fails to act within the timeframes for reviewing Internal Appeals. For decisions involving Behavioral Health Services, EOHHS may consult with the Deputy Commissioner of the Department of Mental Health in its review of the Contractor's decision;

2. Upon learning of a hearing scheduled on a BOH Appeal concerning such a Final Internal Appeal Decision, notify EOHHS immediately and include the names of the Contractor's clinical and other staff who will be attending the BOH hearing;

3. Comply with any EOHHS directive to reevaluate the basis for its decision in a manner that is consistent with EOHHS's interpretation of any statute, regulation, and contractual provisions that relates to the decision;

4. Submit all applicable documentation to the BOH, EOHHS, the Covered Individual and the designated Appeal Representative, if any, within 5 business days prior to the date of the hearing, or if the BOH Appeal is expedited, within 1 business day of being notified by the BOH of the date of the hearing. Applicable documentation shall include, but not be limited to, a copy of the notice of Adverse Action, any documents relied upon by the Contractor in rendering the decision resolving the Internal Appeal, and any and all documents that will be relied upon at hearing;

5. Make best efforts to ensure that a Provider, acting as an Appeal Representative, submits all applicable documentation to the BOH, the Covered Individual and the Contractor within 5 business days prior to the date of the hearing, or if the BOH Appeal is expedited, within 1 business day of being notified by the BOH of the date of the hearing. Applicable documentation shall include, but not be limited to, any and all documents that will be relied upon at the hearing;

6. Comply with and implement the decisions of the BOH;

7. In the event that the Covered Individual appeals a decision of the BOH, comply with and implement the decisions of any court of competent jurisdiction; and

8. Designate an Appeals Coordinator to act as a liaison between EOHHS and the BOH to:

    a. Determine whether each Covered Individual who requests a BOH Appeal has exhausted the Contractor's Internal Appeals process, in accordance with **Section 2.12.C.1**;

    b. If requested by the Covered Individual, assist the Covered Individual with completing a request for a BOH Appeal;

    c. Receive notice from the BOH that a Covered Individual has requested a BOH Appeal, immediately notify EOHHS, and track the status of all pending BOH Appeals;

    d. Ensure that Continuing Services are provided when informed by the BOH that a request for a BOH Appeal was timely received, unless the Covered Individual specifically indicates that he or she does not want to receive Continuing Service;

e. Instruct Covered Individuals for whom an Adjustment has been made about the process of informing the BOH in writing of all Adjustments and, upon request, assist the Covered Individual with this requirement, as needed;

f. Ensure that the case folder and/or pertinent data screens are physically present at each hearing;

g. Ensure that appropriate Contractor staff attend BOH hearings;

h. Coordinate with BOH requests to reschedule hearings and ensure that the Contractor only requests that hearings be rescheduled for good cause;

i. Upon notification by BOH of a decision, notify EOHHS immediately;

j. Ensure that the Contractor implements BOH decisions upon receipt;

k. Report to EOHHS within 30 calendar days of receipt of the BOH decision that such decision was implemented;

l. Coordinate with the BOH, as directed by EOHHS; and

m. Ensure that appropriate Contractor staff attend BOH Appeals training sessions organized by EOHHS.

9. Provide information about the Contractor's grievances and appeals policies to all Providers and Material Subcontractors at the time the Contractor and these entities enter into a contract; and

10. Maintain records of Grievances and Appeals in a manner accessible to EOHHS, available to CMS upon request, and that contain, at a minimum, the following information:

a. A general description of the reason for the Appeal or Grievance;

b. The date received, the date of each review, and, if applicable, the date of each review meeting;

c. Resolution of the Appeal or Grievance, and date of resolution; and

d. Name of the Covered Individual for whom the Appeal or Grievance was filed.

E. Continuing Services

The Contractor shall:

1. Comply with the provisions of 42 CFR 438.420 and, in addition, provide Continuing Services while an Internal Appeal is pending and while a BOH Appeal is pending, unless the Covered Individual specifically indicates that he or

she does not want to receive Continuing Services, when the appeal involves the reduction, suspension, or termination of a previously authorized service;

2. Provide Continuing Services until one of the following occurs:

   a. The Covered Individual withdraws the Internal Appeal or BOH Appeal; or

   b. The BOH issues a decision adverse to the Covered Individual;

3. If the Contractor or BOH reverses an Adverse Action to deny, limit, or delay services that were not furnished while the Internal Appeal or BOH Appeal were pending, the Contractor shall authorize or provide the disputed services promptly, and as expeditiously as the Covered Individual's health condition requires but no later than 72 hours from the date it receives notice reversing the determination; and

4. If the Contractor or BOH reverses an Adverse Action to deny, limit, or delay services and the Covered Individual received Continuing Services while the Internal Appeal or BOH Appeal were pending, the Contractor shall pay for such services.

Section 2.13 Quality Management and Quality Improvement

A. Comprehensive QM/QI Program

The Contractor shall implement a comprehensive Quality Management (QM) and Quality Improvement (QI) program that includes ongoing quality assessment and performance improvement of all areas of the Contractor's responsibility under this Contract.

The QM and QI program shall:

1. Assess the quality and appropriateness of care and services furnished to all Covered Individuals, including Covered Individuals with special health care needs;

2. Focus on improving the Covered Individual's health status through the delivery of high quality and cost-effective care, and by the provision of programmatic supports that foster a high level of communication and cooperation among medical and Behavioral Health care providers, with regard to the Covered Individuals they are serving;

3. Incorporate QM and QI principles into all aspects of the operation of the Contract;

4. Be based upon robust data collection, accurate measurement, and data analysis that enhance Behavioral Health service delivery; the integration of care delivered by medical and Behavioral Health care providers; and Covered Individual health outcomes;

5. Include the conducting of annual Member satisfaction surveys and providing EOHHS with results of such surveys. The Contractor shall work with EOHHS to define deliverables for each annual survey. Deliverables may be modified, added, or deleted to meet project needs, at EOHHS' discretion. For each annual survey, the Contractor shall create, develop, compile, and otherwise provide to EOHHS the following deliverables:

    a. Written report, to include survey background, detail on sampling, fielding and data processing protocols, and response rate;

    b. Data file(s) of aggregate adult and child responses to all questions, and additional question-level details, as further specified by EOHHS;

    c. Data dictionaries to accompany the above file(s).

6. Include effective assessment of healthcare disparities and strategies to identify and address variations related to health care access and health outcomes; and

7. Include activities, resources and strategies that support improved clinical outcomes for Covered Individuals that improve function and symptom management.

B. QM/QI Program Structure

The Contractor shall:

1. Establish a set of QM/QI functions and responsibilities that are clearly defined and that are proportionate to, and adequate for, the planned number and types of QM/QI initiatives and for the completion of QM/QI initiatives in a competent and timely manner;

2. Ensure that such QM/QI functions and responsibilities are assigned to individuals with the appropriate skill set to oversee and implement an organization-wide, cross-functional commitment to, and application of, CQI to all clinical and non-clinical aspects of the Contractor's service delivery system;

3. Establish internal processes to ensure that the QM activities for Behavioral Health Services reflect utilization across the Network and include all of the activities in this Section of this Contract and, in addition, the following elements:

    a. A process to utilize HEDIS results in designing QM/QI activities;

    b. A medical record review process for monitoring Network Provider compliance with policies and procedures, specifications and appropriateness of care. Such process shall include the sampling method used which shall be proportionate to utilization by service type. The Contractor shall submit its process for medical record reviews and the results of its medical record reviews to EOHHS;

c. A process to measure Network Providers and Covered Individuals, at least annually, regarding their satisfaction with the Contractor's Plan. The Contractor shall submit a survey plan to EOHHS for approval and shall submit the results of the survey to EOHHS;

d. A process to measure clinical reviewer consistency in applying Clinical Criteria to Utilization Management activities, using inter-rater reliability measures;

e. A process for including Covered Individuals and their families in Quality Management activities, as evidenced by participation in Covered Individual and family advisory councils;

f. [Reserved]; and

4. In collaboration with and as further directed by EOHHS, develop a process to monitor the quality of services using tools such as the MA DRM (Document Review Measure), or another tool approved by EOHHS, to evaluate the adequacy of medical record keeping for both Intensive Care Coordination and In-Home Therapy Services. The Contractor shall apply the approved quality-assessing tool at least annually on a mix of Intensive Care Coordination and In-Home Therapy Services provided across all of the Contractor's Service Areas. Unless otherwise directed by EOHHS, the Contractor shall:

a. Use the approved quality assessing tool(s) to evaluate at least 10% of the Contractor's Covered Individuals who have received ICC or IHT during the applicable Contract Year, except that the Contractor shall not be required to review more than 10 Covered Individual's medical files per Service Area per Contract Year.

b. Effective September 1, 2025, apply the approved quality-assessing tool for three Covered Individuals receiving Intensive Care Coordination within every contracted Community Service Agency (CSA) and annually apply the approved quality-assessing tool for one Covered Individual at every contracted provider of In-Home Therapy. The Contractor shall submit to EOHHS an annual report on the record reviews in accordance with **Appendix E-1**.

5. Have in place a written description of the QM/QI Program that delineates the structure, goals, and objectives of the Contractor's QM/QI initiatives.

C. Quality Improvement Projects

1. Development of QIPs

a. The Contractor shall annually develop and propose to EOHHS a minimum of two quality improvement projects (QIPs) to be incorporated into the Contract each year.

b. The Contractor shall design Quality Improvement Projects (QIPs) to achieve significant improvement in clinical care and non-clinical care areas that have a favorable effect on health outcomes and Covered Individual satisfaction. Such QIPs shall be designed as ongoing interventions, sustained over time and shall be targeted to areas that present significant opportunities for performance improvement.

c. The QIPs shall be based on the Contractor's actual experience serving Covered Individuals, the findings of the assessments required in **Section 2.13.F**, or direction from EOHHS. The Contractor also may identify other areas, such as those internal to the Contractor's operation, for inclusion in quality improvement projects.

d. Data sources for the design of the QIP may include without limitation:

1) critical incident (Reportable Adverse Incident) reports;

2) continuing care after discharge from one Level of Care to another, community tenure, and recidivism rates;

3) Grievances and Internal Appeals and other feedback from Covered Individuals;

4) Provider concerns;

5) medical record reviews;

6) Provider waiting lists;

7) Covered Individual and Provider satisfaction/experience surveys;

8) direction from EOHHS and DMH related to agencies' goals;

9) data related to PCC Plan Support Services activities;

10) the Care Management Program; and

11) data relative to the Contractor operations, such as Claims processing time frames and telephone response time.

e. [Reserved]

f. Each proposed QIP shall incorporate a project statement that includes highly specified and measurable goals and objectives, methodology, as well as detailed metric calculation specifications.

g. For each QIP, the Contractor shall develop a work plan for completion of the project including time frames by which the Contractor must demonstrate that the goals of the project have been achieved.

h. Both QIPs the Contractor proposes shall be as described in **Section 2.13.F.5** that satisfy the requirements of 42 CFR 438.240(b) and (d). EOHHS's External Quality Review (EQR) vendor shall validate the Contractor's performance of these quality improvement projects. Current listing of BH priority area standard goals including performance measures and quality improvement project initiatives is in **Appendix G**.

i. Should EOHHS and Contractor be unable to reach agreement on the improvement projects and/or the measures, EOHHS shall establish the improvement projects and/or measures.

2. Management of the QIPs

a. The Contractor shall designate relevant QM staff to meet with EOHHS twice a year to review operational issues, milestones and initiatives, as well as progress toward the QIPs, in Contract status meetings.

b. The Contractor shall evaluate the outcome of the QIPs and present its findings to EOHHS in the forms and time frames agreed to by EOHHS.

c. If EOHHS determines that the Contractor is not in compliance with the requirements for proposed annual QIPs, the Contractor shall prepare and submit a corrective action plan to EOHHS for review and approval.

D. Data Management

The Contractor's QM program shall be informed by consistent utilization and analysis of data, incorporating at least the following elements:

1. A process for collecting, analyzing and managing with utilization, clinical and outcomes data to improve Covered Individuals' health outcomes;

2. A process for collecting and submitting performance measurement data in accordance with 42 CFR 438.330;

3. A process for tracking to resolution areas targeted for QI as identified by the Contractor, EOHHS or CMS;

4. Using multiple data sources and drawing conclusions based on data to drive system improvement through evidence-based practices, Practice Guidelines, and other data-driven clinical initiatives.

E. NCQA Accreditation

1. If the Contractor is NCQA accredited as a Health Plan/MCO or as an MBHO (Managed Behavioral Healthcare Organization) for its Medicaid product covered by this Contract as of the Operational Start Date of this Contract, the Contractor shall maintain full NCQA accreditation pursuant to the requirements of NCQA throughout the term of this Contract.

2. If the Contractor does not have such NCQA accreditation for its Medicaid product covered by this Contract as of the Operational Start Date, the Contractor shall attain such interim and then full accreditation within time frames determined acceptable by EOHHS and consistent with current NCQA accreditation requirements.

    a. The Contractor's application for interim and full NCQA accreditation shall be submitted at the earliest point allowed by NCQA. The Contractor shall provide EOHHS with a copy of all correspondence with NCQA regarding the application process and the accreditation requirements.

    b. Once accredited, the Contractor shall maintain full NCQA accreditation pursuant to the requirements of NCQA throughout the term of this Contract.

3. The Contractor shall authorize NCQA to provide EOHHS a copy of its most recent accreditation review for its Massachusetts plan(s), including but not limited to, as applicable, accreditation status, survey type, level, accreditation results, recommended actions, recommended improvements, corrective action plans, summaries of findings; and expiration date of accreditation.

4. The Contractor shall provide EOHHS with updates of its NCQA accreditation status at least annually, whenever if there are any changes within the accreditation period, and upon request by EOHHS.

5. If the Contractor achieves provisional accreditation status from NCQA EOHHS shall require the Contractor to initiate a corrective action plan within thirty (30) calendar days of receipt of the Final Report from NCQA and work to address the findings contributing to the provisional accreditation status.

6. The Contractor's failure to attain full NCQA accreditation as a managed care plan for its Medicaid product covered by this Contract or its failure to maintain full NCQA accreditation at any time, may be considered a breach of the Contract and may result in termination of the Contract.

F. QM Plan for Behavioral Health Management

On an annual basis, the Contractor shall create and implement a single, comprehensive Quality Management plan that defines the QM program, details the Contractor's quality activities and provides for self-assessment of the Contractor's responsibilities under the Contract.

1. The Contractor shall submit such QM plan for EOHHS review and approval by January 31st of each Contract Year.

2. The QM plan for the first year of the Contract shall focus on the establishment of baselines and benchmarks for use in setting and assessing health improvement targets and quality improvement goals in subsequent years of the Contract.

3. The QM plan shall include activities, measures, and performance improvement projects that are specifically relevant to CBHCs, ASD/ID for MCPAP and EC MCPAP.

4. The QM plan shall describe planned improvement activities related to:

    a. The Contractor's management of the BH services provided to Covered Individuals;

    b. The Contractor's Management Support Services for the PCC Plan;

    c. The Contractor's efforts to improve care integration across medical and Behavioral Health care services; and

    d. The Contractor's Care Management Program.

5. Each year's proposed QM plan shall be informed by an assessment of prior years' activities and results through an annual retrospective report, which the Contractor shall prepare and submit to EOHHS for approval within the first month of each Calendar Year. The annual QM plan shall include but not be limited to:

    a. Monitoring of the following performance indicators, at a minimum, and others as directed by EOHHS. If the results of the performance indicator(s) meet or exceed the benchmark, the Contractor shall continue to monitor the indicator(s); if the results of the performance indicator(s) fall below the benchmark, the Contractor shall implement a Quality Improvement Program (QIP) as directed by EOHHS. Performance Indicators shall, at a minimum:

        1) Assess whether qualified and clinically appropriate Network Providers are available to provide BH Covered Services, and the degree to which the Provider Network met the needs of Covered Individuals for:

            a) access within the access standards required by the Contract;

            b) access within different geographic areas across the Commonwealth;

            c) access to individuals with physical disabilities;

d) ability to communicate, either directly or through a skilled interpreter, with a Covered Individual in his/her primary language; and

e) ability to address Covered Individuals' health disparity needs.

2) Assess Network Providers' success at communicating with Primary Care Practitioners, when appropriate.

3) Assess the development of the Behavioral Health service delivery system, including overuse, underuse and misuse of services; special measures shall be developed and implemented to highlight Provider best practices.

4) Assess and measure of utilization reviewers' consistency in applying Medical Necessity criteria in UM activities and in the medical record (chart) review process.

5) Assess and summarize critical incidents reported by Network and non-Network Providers, including actions taken in response.

6) Assess the subjects and outcomes of Appeals, Grievances and complaints, including timeframes required to reach resolution, and opportunities for improvement.

7) Consistent with NCQA accreditation requirements, assess Covered Individual, Network Provider and PCC satisfaction through administration of satisfaction surveys.

b. Timelines, objectives and goals for improvement projects and activities, including clinical and non-clinical activities as well as those BH improvement projects generated by the quality improvement (QI) goals as required by EOHHS. The projects shall be designed to achieve, through ongoing measurements and intervention, significant improvement, sustained over time, in clinical care and non-clinical care areas that are expected to have a favorable effect on health outcomes and Covered Individual, Network Provider and PCC satisfaction. The performance improvement projects must involve the following:

1) measurement of performance using objective indicators of quality;

2) implementation of system interventions to achieve improvement in quality;

3) evaluation of the effectiveness of the interventions; and

4) planning and initiation of activities for increasing or sustaining improvement.

The Contractor must complete each project in a reasonable time period so as to generally allow information on the success of performance improvement projects in the aggregate to produce new information on quality of care every year. The Contractor must report and present the status and results of each project to EOHHS at least twice a year, and as requested.

c. Analysis of the effectiveness of treatment services, employing standard measures of symptom reduction/management as well as measures of functional status and recovery. The Contractor shall recommend to EOHHS an approach to meet this requirement, including the assessment instrument, or scale, to be used and the methodology for its application. EOHHS reserves the right to approve or specify the instrument(s) and analysis methodology to be used.

d. Administration of satisfaction surveys to Covered Individuals on an annual basis.

e. Administration no less often than biennially of Network Provider satisfaction surveys, with results stratified by provider type and specialty.

f. Administration biennially of PCC satisfaction surveys with results stratified by provider type and specialty.

G. Quality Management Plan for PCC PSS

1. Comprehensive Quality Management plan

The Contractor shall create and implement a single, comprehensive Quality Management plan, containing the same elements as described in **Section 2.13.F**, that reflects the Contractor's organizational QM philosophy and structure and includes PCC Plan Support Services-related activities. Such QM plan shall be submitted to EOHHS for review and approval by January 31st of each Contract Year. This component of the QM plan shall describe planned improvement projects and activities, including but not limited to:

a. Timelines, objectives and goals for the planned improvement projects and activities, including clinical and non-clinical initiatives;

b. A process for monitoring data for, and tracking to resolution, areas targeted for quality improvement (QI) as identified by the Contractor or EOHHS;

c. A process for comparing QI project results against established goals;

d. Plans for coordinating medical and Behavioral Health care services;

e. A process for monitoring PCCs' ability to manage the health care needs of culturally diverse PCC Plan Enrollees;

f. A process to evaluate annually the effectiveness of QM plan activities and, based on the results, to identify and implement improvement activities;

g. An annual retrospective QM activities report based on the previous year's QM plan, which the Contractor shall prepare and submit to EOHHS for approval within the first month of each Calendar Year, beginning with January 2024.

H. Provider and PCC Quality Forums

The Contractor shall:

1. Annually organize and conduct at least two quality forums, as follows:

   a. The quality forums shall be held through a webinar at a variety of times convenient to PCCs, Network Providers and other providers as directed by EOHHS. Some or all of the forums may also be held at locations throughout the state, in comfortable environments that encourage PCCs, Network Providers and other providers as appropriate to attend, and including refreshments (food and non-alcoholic beverages) as part of the event.

   b. The quality forums shall be offered on topics that primarily focus on EOHHS goals, quality improvement, increased coordination and collaboration of medical and Behavioral Health care services, or improved service delivery and health outcomes for Covered Individuals.

2. Submit to EOHHS for review and approval a proposal for the quality forum topics for each Contract Year at least 90 days prior to the start of the Contract Year. For the first Contract Year, at least one quality forum must include Health Equity and CLAS topics consistent with requirements in **Section 2.20**. EOHHS may require the Contractor to conduct quality forums on topics of EOHHS's choosing.

3. Develop the content of each quality forum in collaboration with EOHHS and key stakeholders.

4. Implement a mechanism for attendees and the Contractor to evaluate the quality forums and identify areas for improvement and, with EOHHS's approval, incorporate such improvements into future quality forums.

5. Obtain the required approval to offer and grant continuing medical education, risk management, and continuing education units to participants.

6. Within 30 days after the last session of a quality forum series, provide EOHHS a summary report on the forum series which shall include, at a minimum, information on the number and type of attendees (profession and practice name), the location, the presentation topic and responses from attendees regarding the quality of the program presented.

Section 2.14 Data Management, Information Systems, and Reporting Requirements

A. General Requirements

The Contractor shall:

1. Maintain information systems (Systems) that will enable the Contractor to meet all of EOHHS's requirements as outlined in this Contract, as described in this Section and as further directed by EOHHS.

2. Accept all Contract-related files and data delivered by EOHHS, in the format specified by EOHHS.

3. Ensure a secure, HIPAA-compliant exchange of information on Covered Individuals and Uninsured Individuals and persons with Medicare only, as applicable, between the Contractor and EOHHS and any other entity EOHHS deems appropriate. Such files shall be transmitted to EOHHS through secure FTP, HTS, or a similar secure data exchange as determined by EOHHS. The Contractor shall align its HIPAA Companion Guide for its Network Providers with the MassHealth Companion Guide for Providers.

4. Develop and maintain a website that is accurate, up-to-date, and designed in a way that enables Covered Individuals and Providers to quickly and easily locate all relevant information, as specified by EOHHS. If directed by EOHHS, establish appropriate links on the Contractor's website that direct users back to the EOHHS website(s).

5. Cooperate with EOHHS in its efforts to verify the accuracy of all Contractor data submissions to EOHHS.

6. Actively participate in any EOHHS Systems Workgroup or other workgroups, as directed by EOHHS. The workgroup shall meet in the location and on a schedule determined by EOHHS.

B. Member Eligibility System Requirements

The Contractor shall ensure that its enrollment system performs, at a minimum, the following functions:

1. On each business day, obtains from EOHHS by electronic communications link and immediately updates its database with all information pertaining to all Covered Individual enrollments.

2. Uniquely identifies each Covered Individual, and includes in the Contractor's data system information provided by the EOHHS eligibility feed regarding the Covered Individual's state agency affiliations, PCACO or PCC Plan enrollment, PCC, and TPL status. This information must also be incorporated into the Contractor's clinical Information Systems. The Contractor must use the EOHHS-assigned MID as the Covered Individual identifying number.

3. On each business day receives and processes an electronic file of EOHHS's MID merges.

4. On each business day, receives from EOHHS by electronic communications link and processes information pertaining to all disenrollments.

5. Once a month receives and processes a copy of EOHHS's carrier file, including carrier codes, and uses this file to reconcile the Contractor's cost avoidance and recovery activities.

6. Once a month receives a list of EOHHS's PCCs and tracks the accuracy of information on PCCs if directed to do so by EOHHS.

7. Receives and processes on a quarterly basis, or as otherwise agreed to by EOHHS, a file containing a list of all Covered Individuals, by MID, Plan Type and effective dates, and uses this file to reconcile the Contractor's Covered Individual enrollment file with EOHHS data.

C. Automated Service Authorization

The Contractor shall employ an automated service authorization system that supports the service authorization requirements and procedures in **Section 2.6.C** and provides for the documentation of at least the following information for each Covered Individual:

1. Identifying demographic information;

2. Identification of Provider delivering service, including his/her national provider identifier (NPI);

3. Diagnosis code(s);

4. Authorized service units.

D. Claims Processing Requirements

The Contractor shall ensure that its Claims processing system performs, at a minimum, the following functions:

1. Maintains a unique Provider identification number for each Provider and utilizes the NPI for purposes of billing.

2. Accepts Claims submitted by Network Providers or their designated representative(s). The Contractor shall:

a. Accept national UB-04 and national CMS 1500 electronic formats;

b. Accept paper-based Claims using standardized forms.

3. Adjudicates Claims and issues payment for approved Claims once a week, at a minimum.

4. Adjudicates and issues payment for all Clean Claims within 30 days of receipt of the Clean Claim.

5. Provides policies and procedures that track all Claims from point of receipt to final disposition, in order to ensure that all invoices and electronic media Claims are processed to completion and have not been previously paid.

6. Creates payment and HIPAA 835 remittance advices for each Provider for Claims activities during a current cycle. The system specifications and file layout must:

   a. Identify each Claim in a cycle and its status, including a description of all errors and denial reasons; and

   b. Generate the remittance advices in electronic or paper format, as appropriate for each Provider.

7. Collects and maintains Network Provider financial data and issues state and federal income tax documents in accordance with state and federal law. This shall include, at a minimum, TIN/FEIN and NPI.

8. Maintains all Claims files and records in accordance with all applicable laws, and submits them to EOHHS, the Commonwealth or federal agencies, as needed and upon request.

9. Ensures that security controls are in accordance with current industry standards and relevant CMS policy.

10. Ensures confidentiality of all data in accordance with state and federal laws and regulations, including 42 CFR 431, Subpart F, implementing procedures to properly safeguard and dispose of data. (See also **Section 5.2**.)

E. Encounter Data

The Contractor shall collect, manage, and report Encounter Data as described in this Section and as further specified by EOHHS. The Contractor shall:

1. Collect and maintain 100% Encounter Data for all Behavioral Health Covered Services provided to Covered Individuals and Uninsured Individuals, including from any subcapitated sources. Such data must be able to be linked to MassHealth eligibility data;

2. Participate in site visits and other reviews and assessments by EOHHS, or its designee, for the purpose of evaluating the Contractor's collection and maintenance of Encounter Data;

3. Upon request by EOHHS, or its designee, provide medical records of Covered Individuals and a report from administrative databases of the Encounters of such Covered Individuals in order to conduct validation assessments. Such validation assessments may be conducted annually;

4. Produce Encounter Data according to the specifications, format, and mode of transfer reasonably established by EOHHS, or its designee, in consultation with the Contractor. Such Encounter Data shall include, but is not limited to, the data elements described in **Appendix D**, the delivering physician, and elements and level of detail determined necessary by EOHHS. As directed by EOHHS, such Encounter Data shall also include the National Provider Identifier (NPI) of the Servicing/Rendering, Referring, Prescribing and Primary Care Provider, and any National Drug Code (NDC) information on drug claims. As directed by EOHHS, such Encounter Data shall also include information related to denied claims and 340B Drug Rebate indicators on drug claims, if applicable;

5. Provide Encounter Data to EOHHS on a monthly basis or within time frames specified by EOHHS in consultation with the Contractor, including at a frequency determined necessary by EOHHS to comply with any and all applicable statutes, rules, regulations and guidance. The Contractor shall submit Encounter Data by the last calendar day of the month following the month of the claim payment. Such submission shall be consistent with all Encounter Data specifications set forth in **Appendix D**;

6. Submit Encounter Data that is at a minimum compliant with the standards specified in **Appendix D**, including but not limited to the standards for completeness and accuracy. To meet the completeness standard, all critical fields in the data must, at a minimum, contain valid values. To meet the accuracy standard, the Contractor must, at a minimum, have systems in place to monitor and audit claims. The Contractor must also correct and resubmit denied encounters as necessary;

7. Ensure that all EPSDT screens, including Behavioral Health screenings, are explicitly identified in the Encounter Data in accordance with this **Section 2.14.E**;

8. Ensure that all initial Behavioral Health Clinical Assessments are explicitly identified in the Encounter Data submitted in accordance with this **Section 2.14.E**;

9. If EOHHS, or the Contractor, determines at any time that the Contractor's Encounter Data is not compliant with the benchmarks described in **Appendix D-1** the Contractor shall:

a. Notify EOHHS, prior to Encounter Data submission, that the data is not complete or accurate, and provide an action plan and timeline for resolution;

b. Submit for EOHHS approval, within a time frame established by EOHHS which shall in no event exceed 30 days from the day the Contractor identifies or is notified that it is not in compliance with the Encounter Data requirements, a corrective action plan to implement improvements or enhancements to bring the accuracy and/or completeness to an acceptable level;

c. Implement the EOHHS-approved corrective action plan within a time frame approved by EOHHS which shall in no event exceed 30 days from the date that the Contractor submits the corrective action plan to EOHHS for approval; and

d. Participate in a validation study to be performed by EOHHS, or its designee, following the end of a twelve-month period after the implementation of the corrective action plan to assess whether the Encounter Data is compliant with the standards described in **Appendix D**. The Contractor may be financially liable for such validation study;

10. Submit any correction/manual override file within 10 business days from the date EOHHS places the error report on the Contractor's server. Such submission shall be consistent with all Encounter Data specifications set forth in **Appendix D**;

11. Report as a voided claim in the monthly Encounter Data submission any claims that the Contractor pays, and then later determines should not have paid;

12. EOHHS may, at any time, modify the specifications required for submission of Encounter Data, including but not limited to requiring the Contractor to submit additional data fields to support the identification of Covered Individuals' affiliation with their Primary Care Provider;

13. At EOHHS' request, the Contractor shall submit denied claims, as further specified by EOHHS;

14. EOHHS may impose an intermediate sanction in accordance with **Section 5.3.L** in the event that Contractor's submitted Encounter Data does not meet the completeness, accuracy, timeliness, form, format, and other standards described in this Section;

15. At a time specified by EOHHS, the Contractor shall comply with all Encounter Data submission requirements related to HIPAA and the ASCX12N 837 format. This may include submitting Encounter Data to include professional, institutional and dental claims and submitting pharmacy claims using NCPDP standards. This

submission may require the Contractor to re-submit Encounter Data previously supplied to EOHHS in alternative formats.

F. Design Requirements

The Contractor shall:

1. Comply with EOHHS requirements, policies and standards in the design and maintenance of its Information Systems in order to successfully meet the requirements of this Contract.

2. Ensure that its Information Systems interface with and are compliant with EOHHS's MMIS, the EOHHS Virtual Gateway, and other EOHHS IT architecture that EOHHS identifies.

3. Have adequate resources to support the MMIS interfaces. The Contractor shall demonstrate the capability to successfully send and receive interface files including HIPAA transaction files, as specified on the 820 Companion Guide, 834 Outbound Companion Guide available at: https://www.mass.gov/lists/masshealth-hipaa-companion-guides.

4. Interface files in the Contract include but are not limited to:

   a. HIPAA 834 History Request File

   b. HIPAA 834 Outbound Daily File

   c. HIPAA 834 Outbound Full File

   d. HIPAA 834 History Response

   e. HIPAA 820

5. Have the ability to receive and analyze data from the EOHHS Data Warehouse regarding medical and pharmacy Claims, as provided by EOHHS.

6. Conform to HIPAA-compliant standards for data management and information exchange.

7. Implement controls to maintain information security and integrity.

8. Maintain appropriate internal processes to determine the validity and completeness of data submitted to EOHHS. These processes may be reviewed by EOHHS upon request.

9. Collaborate with EOHHS to verify its compliance with Version 5010 standards during the readiness review period prior to the Operational Start Date.

10. Use Version 5010 standards for HIPAA electronic health care transactions, including claims, remittance advice, eligibility inquiries, referral authorization, and other administrative transactions.

11. Implement Version 5010 standards and framework for the most recent version of medical data code sets (e.g., ICD-11-CM and ICD-11-PCS).

12. Ensure that an automated health information system (HIS) to support all of the Contractor's responsibilities under the Contract is operative as of the Operational Start Date and remains operative for the duration of the Contract, unless otherwise directed or agreed to by EOHHS. The HIS must achieve the objectives of 42 CFR Part 438, Subpart D and shall collect, analyze, integrate and report data, including but not limited to information regarding:

    a. Service authorizations;

    b. Utilization;

    c. Inquiries, Grievances, Internal Appeals, and BOH Appeals;

    d. Disenrollments for reasons other than for loss of MassHealth eligibility;

    e. Claims;

    f. Provider information;

    g. Services furnished to Covered Individuals through an Encounter data system, as specified in **Section 2.14.E**;

    h. Covered Individual characteristics, including but not limited to race, ethnicity, spoken language, hearing loss and use of ASL Interpreter or CART services by deaf, hard-of-hearing and deaf blind persons, blindness and wheelchair dependence, and characteristics gathered through Contractor contact with Covered Individuals, e.g., through the Care Management Program, Behavioral Health Clinical Assessments, or other reliable means;

    i. Enrollee participation in the Care Management Program; and

    j. Identification of Covered Individuals as belonging to any of the special populations or subgroups identified through provision of clinical services.

13. Ensure that data received from Providers is 99 percent complete and 95 percent accurate by:

    a. Verifying the accuracy and timeliness of reported data;

    b. Screening the data for completeness, logic and consistency;

    c. Establishing a remediation process for data that is deemed inaccurate during verification and screening; and

    d. Collecting service information from Providers, in standardized formats to the extent feasible and appropriate or as directed by EOHHS, including

secure information exchanges and technologies utilized for State Medicaid quality improvement and care coordination efforts.

14. Make all collected data available to EOHHS and, upon request, to CMS, as required by 42 CFR 438.242(b)(3).

15. Utilize its HIS to pay Network Providers for BH Covered Services rendered to Covered Individuals, and ESP, AMCI, and YMCI services as directed by EOHHS, rendered to Uninsured Individuals, including persons covered by Medicare only, in accordance with the Contractor's service authorization, Claims processing, enrollment and disenrollment procedures, and data handling and administrative billing requirements.

16. As set forth in 42 CFR 438.242(b)(1), comply with Section 6504(a) of the Affordable Care Act.

17. The Contractor shall establish and sustain a Patient Access application programming interface (API) in accordance with federal law, including but not limited to 42 CFR 438.242(b)(5), the Consolidated Appropriations Act, 2023, and the CMS Interoperability and Patient Access final rule.

G. System Access Management and Information Accessibility Requirements

1. The Contractor shall make all Information Systems and system information available to authorized EOHHS and other agency staff as determined by EOHHS to evaluate the quality and effectiveness of the Contractor's data and Information Systems.

2. The Contractor is prohibited from sharing or publishing EOHHS data and information without prior written consent from EOHHS.

H. System Availability and Performance Requirements

1. The Contractor shall ensure that its Covered Individual and Provider web functions and phone-based functions are available to Covered Individuals and Providers 24 hours a day, seven days a week. At a minimum, these functions shall be available 99.9% of the month.

2. The Contractor shall draft an alternative plan that describes access to Covered Individual and Provider information in the event of Information System failure. Such plan shall be contained in the Contractor's Continuity of Operations Plan (COOP) (see **Section 2.3.C.4**) and shall be updated annually and submitted to EOHHS upon request. In the event of Information System failure or unavailability, the Contractor shall notify EOHHS upon discovery, and implement the COOP immediately.

3. The Contractor shall preserve the integrity of Covered Individual-sensitive data whether active or archived.

I. Virtual Gateway

If EOHHS directs the Contractor during the term of this Contract to access certain services through the Virtual Gateway, the Contractor shall:

1. Submit all specified information, including but not limited to invoices, Contract or other information to EOHHS through these web-based applications;

2. Comply with all applicable EOHHS policies and procedures related to such services;

3. Use all business services through the EOHHS Virtual Gateway, as required by EOHHS;

4. Take necessary steps to ensure that the Contractor and its subcontractors or affiliates have the ability to access and utilize all required web-based services; and

5. Execute and submit all required agreements, including subcontracts, agreements, memorandums of understanding, confidentiality and/or end user agreements in connection with obtaining necessary end user accounts for any Virtual Gateway business service.

J. Telephone System

1. General Requirements

As of the Operational Start Date, the Contractor shall:

a. Maintain the telephone number (800-495-0086), with telecommunications device for the deaf (TDD) and teletypewriter (TTY) transmission and reception capability for the deaf and hearing-impaired, as the Contractor's toll-free number, unless otherwise agreed to by EOHHS.

b. Provide access through the toll-free number to Member and Provider Customer Service representatives via dedicated menu option(s).

c. Maintain a telephone system that performs the following functions:

1) Assigns priority status to Covered Individuals in crisis to ensure immediate response from a clinician staffing the Clinical Referral and Service Authorization line;

2) Provides a sufficient number of telephone lines and trunks to handle all incoming calls so that no caller receives a busy signal;

3) Provides a means for callers to leave messages for the Contractor after business hours, and ensures that such calls are handled by the next business day; and

4) Allows the Contractor to directly connect the caller to other agencies or contractors, as specified by EOHHS.

d. Develop, implement, maintain and enhance, as necessary, a call management system for Clinical Authorization and Referral and Member and Provider Customer Service calls that:

1) Records and tracks all calls handled, to include the following information:

a) name of caller and Covered Individual, Provider or PCC identification number, where applicable;

b) call date and time;

c) reason for the call;

d) disposition of the call, including whether the matter was resolved at the time of first contact if a complaint, was resolved by the end of the next business day, or if the call is pending resolution; and

e) if the call is pending resolution, additional information to assist in the escalation and resolution of outstanding issues.

2) Tracks Covered Individual call volume by PCC, DYS, DCF, TPL, etc.; and

3) Provides service representatives with online access to relevant information from previous calls.

e. Arrange for appropriate telephone listings of the Contractor, as approved by EOHHS, to be submitted for publication at least one month prior to the Operational Start Date.

f. Periodically, and as directed by EOHHS, evaluate the effectiveness of the Provider and Member Customer Services telephone system, and submit proposals for improvement to EOHHS.

2. Telephone Response Requirements

The Contractor shall ensure that:

a. Calls from Covered Individuals in crisis are handled immediately by a staff clinician;

b. For each line, including Clinical Referral and Service Authorizations, Member and Provider Customer Service and PCC Hotlines, staff make best efforts to answer all calls from Covered Individuals and Providers and PCCs within 30 seconds of when callers select the menu option for the

line they are trying to reach; but in no case shall fewer than 90 percent of these calls be answered within 30 seconds;

c. Calls to all lines have an abandoned call rate of less than 5 percent; and

d. Calls to each specific line are answered within the specified time frames by the appropriate staff:

1) Calls to clinical lines are answered by a clinician;

2) Calls to Customer Service are answered by customer service staff; and

3) Calls to the PCC Hotline are answered by trained and dedicated Provider service representatives.

K. Medical Records

The Contractor shall:

1. Comply with, and require Network Providers to comply with, all state and federal statutory and regulatory requirements applicable to medical records, including the requirements set forth in 130 CMR 130 CMR 433.409, 130 CMR 450.205, 42 CFR 456.111 and 42 CFR 456.21 (if applicable), and any amendments thereto. In addition, all medical records, whether paper or electronic shall, at a minimum:

a. Be maintained in a manner that is current, detailed, and organized and that permits effective patient care and quality review;

b. Include sufficient information to identify the Covered Individual, date of encounter and pertinent information that documents the Covered Individual's diagnosis;

c. Describe the appropriateness of the treatment and services, the course and results of the treatment and services; and

d. Be consistent with current and nationally accepted professional standards for providing the treatment/services, as well as systems to accurately document the following:

1) Covered Individual information including, among other things, primary language spoken;

2) Clinical information;

3) Behavioral Health Clinical Assessments;

4) Treatment plans;

5) Treatment or services provided;

6) Contacts with Covered Individuals' family, guardians, or significant others; and

7) Treatment goals and outcomes;

8) All contacts with state agencies, as applicable; and

9) Pharmacy records.

2. Comply with, and require Network Providers to comply with, all state and federal statutory and regulatory requirements applicable to confidentiality of medical records, including but not limited to M.G.L. c. 66A and, if applicable, M.G.L. c. 123 § 36, 104 CMR 27.17, and 104 CMR 28.09.

3. Provide EOHHS with a copy of any Covered Individual's medical records, in general within 10 days of EOHHS's request; except that EOHHS may allow the Contractor up to one month from the date of EOHHS's initial request to produce such records if the Contractor has made best efforts to produce them in the specified time and EOHHS reasonably determines that the need for such record(s) is not urgent.

4. Conduct medical record audits periodically and at the request of EOHHS. Such audits may be subject to validation by EOHHS or its agent.

L. Reports and Notifications

1. General

a. The Contractor shall provide and require its Material Subcontractors and other subcontractors to provide, in accordance with the timelines, definitions, formats and instructions contained herein or as further specified by EOHHS:

1) All information required under this Contract, including but not limited to, the requirements of **Appendix E** or other information related to the performance of its or their responsibilities hereunder or under the subcontracts as reasonably requested by EOHHS;

2) Any information in its or their possession sufficient to permit EOHHS to comply with 42 CFR 438;

3) Any data from their clinical systems, authorization systems, claims systems, medical record reviews, Network Management visits, and Covered Individual and family input;

4) Delivery of time sensitive data to EOHHS in accordance with EOHHS timelines; and

5) High quality, accurate data in the format and in the manner of delivery specified by EOHHS;

6) Names of the required Appendix E-1 reports using the following naming convention: 'BH-##-report name-cadence-submission date'.

b. The Contractor shall participate in work groups led by EOHHS to develop and comply with reporting specifications and to adopt the reporting models formulated by these work groups and approved by EOHHS, pursuant to the timeline established by EOHHS; and

c. Upon request, the Contractor shall provide EOHHS with the original data sets used by the Contractor in the development of any required reporting or ad-hoc reporting in accordance with the time frames and formats established by EOHHS.

2. Contract-Related Reports

Such reports shall include, but shall not be limited to, reports related to Contract performance, management and strategy.

a. The Contractor shall submit **Appendix E** reports in accordance with the timeframes and other requirements specified in **Appendix E**. For any report that indicates the Contractor is not meeting the targets set by EOHHS, the Contractor shall provide immediate notice explaining the corrective actions it is taking to improve performance. Such notice shall include root cause analysis of the problem the data indicates, the steps the Contractor has taken to improve performance, and the results of the steps taken to date. The Contractor may also include an executive summary to highlight key areas of high performance and improvement.

b. Failure to meet the reporting requirements in **Appendix E** shall be considered a breach of Contract.

3. Internal Management Reports

The Contractor shall submit to EOHHS, upon request, any internal reports that the Contractor uses for internal management. Such reports shall include, but not be limited to, internal reports that analyze the medical/ loss ratio, financial stability, or other areas where standard compliance reports indicate a problem in performance.

4. Additional Reports

a. In addition to the reports specifically required in **Appendix E**, the Contractor shall participate with EOHHS in the annual development of additional reports based on specific topics identified jointly by EOHHS

and the Contractor as a result of ongoing analysis and review of data, and/or administrative and clinical processes. The Contractor shall participate in meetings led by EOHHS to develop analytical approaches and specifications for such reports. The Contractor shall produce data and written analyses of each topic in a time frame established by EOHHS but, at minimum, by the end of each Contract Year.

b. Pursuant to 42 CFR 438.3(g), the Contractor shall comply with any reporting requirements on Provider Preventable Conditions in the form and frequency as may be specified by EOHHS.

c. The Contractor shall provide to EOHHS, in accordance with the timeframes and other requirements specified by EOHHS all reports, data or other information EOHHS determines necessary for compliance with program report requirements set forth in 42 CFR 438.66(e).

5. Other Ad Hoc Reports

The Contractor shall provide EOHHS with additional ad hoc or periodic reports related to this Contract at EOHHS's request and as mutually agreed by the parties.

M. Certification Requirements

In accordance with 42 CFR 438.600 et seq., the Contractor's Chief Executive Officer or Chief Financial Officer shall, at the time of submission of the types of information, data, and documentation listed below, sign and submit to EOHHS the form provided in **Appendix E-2**, certifying that the information, data and documentation being submitted by the Contractor is true, accurate, and complete to the best of their knowledge, information and belief, after reasonable inquiry, under the penalty of perjury:

1. Data on which payments to the Contractor are based;
2. All enrollment information, Encounter Data, and measurement data;
3. Data related to medical loss ratio requirements in aggregate for the Contractor's Covered Individual population;
4. Data or information related to protection against the risk of insolvency;
5. Documentation related to requirements around Availability and Accessibility of services, including adequacy of the Contractor's Provider Network;
6. Information on ownership and control, such as that pursuant to **Section 5.1.O**;
7. Reports related to overpayments; and
8. Data and other information required by EOHHS, including but not limited to, reports and data described in this Contract.

Section 2.15 Financial Stability Requirements

Throughout the term of the Contract, the Contractor, at a minimum, shall meet the solvency standards established by EOHHS consistent with 42 CFR 438.116(b).

A. Financial Stability

Throughout the term of this Contract, the Contractor shall remain financially stable and maintain adequate protection against insolvency, as determined by EOHHS. To meet this general requirement, the Contractor, at a minimum, shall comply with, and demonstrate such compliance to the satisfaction of EOHHS, the solvency standards in this Contract. The Contractor shall also submit reports to EOHHS set forth in **Appendix E-4** of this Contract.

1. Cash Flow: The Contractor shall maintain sufficient cash flow and liquidity to meet obligations as they become due. The Contractor shall submit to EOHHS upon request a cash flow statement to demonstrate compliance with this requirement and a statement of its projected cash flow for a period specified by EOHHS.

2. Net Worth: As directed by EOHHS, the Contractor shall comply with the adjusted initial net worth requirements set forth in M.G.L. c 176G § 25 (a) and 211 CMR 43:07(1) and continue to maintain an adjusted net worth in accordance with M.G.L. c 176G § 25(b) and 211 CMR 43:07(2).

3. Cash Reserves: Throughout the term of this Contract, the Contractor shall maintain a minimum cash reserve of $1,000,000 to be held in a restricted reserve entitled "Reserve for MassHealth Behavioral Health Managed Care Program Obligations." Funds from this restricted cash reserve may be dispersed only with prior written approval from EOHHS during the term of this Contract.

4. Working Capital Requirements: The Contractor shall demonstrate and maintain working capital as specified below. For the purposes of this Contract, working capital is defined as current assets minus current liabilities. Throughout the term of this Contract, the Contractor shall maintain a positive working capital balance, subject to the following conditions:

   a. If, at any time, the Contractor's working capital decreases to less than 75% of the amount reported on the prior year's audited financial statements, the Contractor shall notify EOHHS within two business days and submit, for approval by EOHHS, a written plan to reestablish a positive working capital balance at least equal to the amount reported on the prior year's audited financial statements.

   b. EOHHS may take any action it deems appropriate, including termination of the Contract, if the Contractor:

1) Does not maintain a positive working-capital balance; or

2) Violates a corrective plan approved by EOHHS.

5. Throughout the term of this Contract, the Contractor shall: a) remain financially stable, and b) maintain adequate protection against insolvency in an amount determined by EOHHS to be at least adequate to both:

a. Provide to Covered Individuals all BH Covered Services required by this Contract for a period of 45 days following the date of insolvency; and

b. Continue to provide all such services to Covered Individuals who are receiving Inpatient Services at the date of insolvency until the date of their discharge.

The Contractor shall maintain liability protection sufficient to protect itself against any losses arising from any claims against it, including, at a minimum, workers' compensation insurance, comprehensive liability insurance, and property damage insurance (see also **Section 5.3.R**).

B. Performance Guarantees and Additional Security

1. Insolvency Reserve

The Insolvency Reserve shall be defined as the funding resources necessary to meet the costs of providing services to Covered Individuals for a period of 60 days in the event that the Contractor is determined insolvent. For the first year of the Contract, the Contractor shall provide at minimum fifty-percent of the Insolvency Reserve, consistent with the risk corridor calculation.

a. EOHHS shall calculate the amount of the Insolvency Reserve annually and provide this calculation to the Contractor within 45 days of the start of the Contract Year.

b. The Insolvency Reserve calculation shall be an amount equal to 60 days of the Contractor's Capitation Payment revenue.

c. Within 30 calendar days of receipt of the Insolvency Reserve calculation, the Contractor shall submit to EOHHS written documentation of its ability to satisfy the Insolvency Reserve requirement. The documentation shall be signed and certified by the Contractor's chief financial officer.

d. The Contractor shall submit to EOHHS for approval, documentation that the Contractor has satisfied the insolvency Reserve Requirement through any of the following, or combination of the following:

1) Restricted cash reserves;

2) Net worth of the Contractor;

3) Performance bond or guarantee;

4) Insolvency insurance;

5) An irrevocable letter of credit; or

6) A written guarantee from the Contractor's parent or organization.

2. Prior to the Operational Start Date, the Contractor shall provide EOHHS with:

a. Performance Guarantees as specified in **Appendix H-2**, the form of which shall be subject to EOHHS's prior review and approval.

b. A promissory note from the Contractor's parent(s) to guarantee performance of the Contractor's obligation to provide Covered Services in the event of the Contractor's insolvency, the form and amount of which shall be subject to EOHHS's prior review and approval.

c. A promissory note from the Contractor's parent(s) to guarantee performance of the Contractor's obligations to perform activities related to the administration of the Contract in the event of the Contractor's insolvency, the form and amount of which shall be subject to EOHHS's prior review and approval.

3. Direct Service Reserve Account

The Contractor shall establish a Direct Service Reserve Account (DSRA) into which all payments received from EOHHS must be deposited.

a. The DSRA shall be:

1) An interest-bearing trust account in a banking institution located in Massachusetts and approved by EOHHS. The Commonwealth of Massachusetts shall have the right and title to any and all interest earned in the DSRA.

2) Maintained, to the extent legally permissible, in a manner that prevents the creditors of the Contractor from in any way encumbering or acquiring any funds in the DSRA.

b. In no event shall funds in the DSRA be used by the Contractor or any other agent or third party to satisfy, temporarily or otherwise, any Contractor liability, or for any other purpose except as provided under the Contract.

c. EOHHS may require at any time that the Contractor confer upon an authorized representative of EOHHS, or a third party approved by EOHHS the obligation to approve all withdrawals and countersign all checks drawn on the DSRA.

d. The Contractor shall obtain approval of all aspects of the DSRA from EOHHS before establishing or making changes to the account and shall make changes to the DSRA at the direction of EOHHS, as necessary.

e. Subject to EOHHS approval, the Contractor may transfer deposits for the BH Covered Services Capitation Rate out of the DSRA to a separate bank account established and maintained by the Contractor for the purposes of processing covered services claims from services providers.

f. The Contractor shall transmit all interest income from the DSRA and from any bank account maintained by the Contractor to which BH covered services capitation deposits are transferred, net of bank charges, to EOHHS in the form of a check payable to the Commonwealth of Massachusetts, twice a year on dates to be specified by EOHHS.

    1) In no case shall the Contractor use interest income as any Earnings or bonus payment.

    2) The Contractor shall exclude interest income from reconciliations of capitated expenditures.

g. The Contractor shall perform a reconciliation of funds transferred from the DSRA to claims payments from the Contractor's bank account every six months and shall transfer any unspent BH services capitation funds to the DSRA.

h. EOHHS may, at any time and at its discretion, audit the Contractor's administration of the DSRA funds consistent with the Contract requirements.

i. The Contractor shall comply with the following requirements relative to the management of the DSRA:

    1) Separately tracking the following types of deposits from EOHHS into the DSRA:

        a) BH Covered Services Capitation Rate payments, which includes the Administrative Component of the BH Covered Services Capitation Rate payments and any funds the Contractor transfers from the DSRA into another bank account maintained by the Contractor;

        b) Care Management Engagement payment;

        c) All Performance Incentive Arrangement payments;

        d) PCC Plan Support Services payments;

        e) DMH Specialty Services payments;

f) DMH Administrative payments;

g) DCF MCI Payments; and

h) DPH payments.

2) Establishing an audit trail that evidences that all payments and transfers from the DSRA are made from deposits received from EOHHS for that express purpose; specifically that:

a) All payments for BH Covered Services are made from deposits received from EOHHS for Covered Services for Covered Individuals and the administration and arrangement of BH Covered Services are made from deposits from EOHHS for that purpose (the Administrative Component of the BH Covered Services Capitation Rate);

b) All transfers from the DSRA for the Care Management Program- Engagement are made from deposits received from EOHHS for the Care Management Program;

c) All transfers from the DSRA for PCC Plan Support Services are made from deposits received from EOHHS for the PCC Plan Support Services;

d) All payments from the DSRA for DMH Specialty Programs are made from deposits received from EOHHS for DMH Specialty Programs;

e) All DCF payments from the DSRA are made from deposits from EOHHS for MCI Wrap Services; and

f) All DPH programs payments are made from deposits from EOHHS.

3) Tracking the interest earned on all deposits into the DSRA and all funds the Contractor transfer from DSRA to another Contractor-owned bank account.

j. Except as specifically set forth in this Section 2.15.B.3 the Contractor shall not withdraw funds from the DSRA except to transfer to the bank account used by the Contractor to pay Claims properly submitted by Providers for Covered Services authorized by the Contractor pursuant to the Contract.

k. The Contractor and EOHHS shall reconcile deposits into and transfers from the DSRA within 120 days of the end of each state fiscal year for the preceding fiscal year.

C. Medical Loss Ratio (MLR) Requirements

1. Annually, and upon any retroactive change to the Capitation Rates by EOHHS, the Contractor shall calculate a Medical Loss Ratio (MLR) in accordance with 42 CFR 438.8. The Contractor shall perform such MLR calculation in the aggregate for the Contractor's Covered Individual population and individually for each Rating Category. Within 212 days following the end of the Contract Year, the Contractor shall report such MLR calculations to EOHHS in a form and format specified by EOHHS and as set forth in **Appendix E-4**. Such report shall include at least the following, pursuant to 42 CFR 438.8(k):

    a. Total incurred claims

    b. Expenditures on quality improving activities;

    c. Expenditures related to activities compliant with 42 CFR 438.608(a)(1)-(5),(7),(8), and (b);

    d. Non-claims costs;

    e. Premium revenue;

    f. Taxes, licensing, and regulatory fees;

    g. Methodology(ies) for allocation of expenses;

    h. Any credibility adjustment applied;

    i. Any remittance owed to the State, if applicable;

    j. The calculated MLR;

    k. A comparison of the information reported in this Section with the audited financial report required under this **Section 2.15**;

    l. A description of the aggregation method used in calculating MLR;

    m. The number of Covered Individual months;

    n. An attestation that the calculation of the MLR is accurate and in accordance with 42 CFR 438.8; and

    o. Any other information required by EOHHS.

2. As further specified by EOHHS, the Contractor shall calculate its MLR in accordance with 42 CFR 438.8, as follows:

    a. The numerator of the Contractor's MLR for each year is the sum of the Contractor's incurred claims; expenses for activities that improve health care quality, including medical sub-capitation arrangements; and fraud

reduction activities, all of which must be calculated in accordance with 42 CFR 438.8.

b. The denominator of the Contractor's MLR for each year is the adjusted premium revenue as set forth in 42 CFR 438.8(f). For purposes of this Section, the Contractor's adjusted premium revenue shall be the Contractor's premium revenue as defined in 42 CFR 438.8(f)(2) minus the Contractor's federal, state, and local taxes and licensing and regulatory fees as defined in 42 CFR 438.8(f)(3).

3. As further directed by EOHHS, the Contractor shall maintain a minimum MLR of 85 percent in the aggregate for the Contractor's Covered Individual population. If the Contractor does not maintain such minimum, the Contractor shall, pursuant to 42 CFR 438.8(j), remit an amount equal to the difference between actual medical expenditures and the amount of medical expenditures that would have resulted in a MLR of 85%.

4. The Contractor shall require Material Subcontractors to which the Contractor delegates risk, as reported in accordance with Appendix E-4, to meet the MLR requirements set forth above and include such requirements in its subcontracts with its Material Subcontractors; provided, however that Material Subcontractor shall comply with the remittance requirement above no later than January 1, 2025. In addition:

a. The Contractor shall require that Material Subcontractors report to the Contractor its MLR consistent with reporting requirements set forth in 42 CFR 438.8. The Contractor shall submit such data to EOHHS in a form and format specified by EOHHS; and

b. The Contractor shall confirm to EOHHS, in a form and format specified by EOHHS, that its Material Subcontracts satisfy the requirements set forth in this Section.

D. Auditing and Other Financial Requirements

The Contractor shall:

1. Ensure that an independent financial audit of the Contractor, and any parent or subsidiary, is performed annually. These audits must comply with the following requirements and must be accurate, prepared using an accrual basis of accounting, verifiable by qualified auditors, and conducted in accordance with generally accepted accounting principles (GAAP) and generally accepted auditing standards:

a. No later than 120 days after the Contractor's fiscal year end, the Contractor shall submit to EOHHS its most recent year-end audited financial statements (balance sheet, statement of revenues and expenses,

source and use of funds statement and statement of cash flows that include appropriate footnotes) both:

1) Specific to this Contract; and

2) If directed by EOHHS, statements for the overall organization or consolidated statements that include other lines of business or other Medicaid products.

b. The Contractor shall demonstrate to its independent auditors that its internal controls are effective and operational as part of its annual audit engagement. The Contractor shall provide to EOHHS an attestation report from its independent auditor on the effectiveness of the internal controls over operations of the Contractor related to this Contract in accordance with statements and standards for attestation engagements as promulgated by the American Institute of Certified Public Accountants. The Contractor shall provide such report annually and within 30 days of when the independent auditor issues such report; provided, however, if the Contractor is Service Organization Control (SOC) compliant, the Contractor shall annually submit a copy of the SOC report in lieu of the attestation report described above within 30 days of the Contractor's independent auditors issuing its SOC report.

c. The Contractor shall submit, on an annual basis after each annual audit, the final audit report together with all supporting documentation, a representation letter signed by the Contractor's chief financial officer and its independent auditor certifying that its organization is in sound financial condition and that all issues have been fully disclosed.

2. Submit annually, by September 30th, a Financial Ratio Analysis that describes the Contractor's performance for financial ratios required by EOHHS in accordance with **Appendix E-4**. The report shall be generated from the Contractor's audited financial statements.

3. Maintain separate records of all Direct and Indirect administrative Costs, in accordance with generally accepted accounting principles, and make these financial records available to EOHHS on a quarterly basis, for audit purposes.

4. Obtain EOHHS's approval of and utilize a methodology to estimate IBNR claims adjustments.

5. Immediately notify EOHHS of any material negative change in the Contractor's financial status that could render the Contractor unable to comply with any requirement of this Contract, or that is significant enough for the Chief Executive Officer or Chief Financial Officer to notify its Board of the potential for insolvency.

6. Notify EOHHS in writing of any default of its obligations under this Contract, or any default by a parent corporation on any financial obligation to a third party that could in any way affect the Contractor's ability to satisfy its payment or performance obligations under this Contract.

7. Advise EOHHS no later than 30 days prior to execution of any significant organizational changes, new contracts or business ventures being contemplated by the Contractor that may negatively impact the Contractor's ability to perform under this Contract.

8. Not invest funds in, or loan funds to, any organization in which a director or principal officer of the Contractor has a financial interest.

9. Provide EOHHS with any other information that CMS or EOHHS deems necessary to adequately monitor and evaluate the financial strength of the Contractor or that must be provided to CMS or EOHHS by law. Such information shall include, but not be limited to, the quarterly revenue expenses and utilization reports set forth in **Appendix E-4**; the annual financial ratios set forth in **Appendix E-4**; and the annual outstanding litigation report set forth in **Appendix E-4**.

E. Reporting

The Contractor shall submit to EOHHS all required financial reports, as described in this **Section 2.15** or in **Appendix E-4**, in accordance with specified timetables, definitions, formats and assumptions, and certifications, as well as any ad hoc financial reports required by EOHHS.

Section 2.16 Operational Audits

A. The Contractor or its Material Subcontractor shall cooperate and facilitate EOHHS's conduct of periodic on-site visits as described under **Section 3.1.C.4** of this Contract. At the time of such visits, the Contractor or Material Subcontractor shall assist EOHHS or its designee in activities pertaining to an assessment of all facets of the Plan's operations, including, but not limited to financial, administrative, clinical, pharmacy and claims processing functions and the verification of the accuracy of all data submissions to EOHHS as described herein.

B. The Contractor or Material Subcontractor shall respond to requests for information associated with such on-site visits in a timely manner, and shall make senior managers available for on-site reviews.

Section 2.17 Additional Enrollee Groups

A. Consistent with **Section 3.6**, EOHHS may require the Contractor to accept additional Covered Individuals into the Contractor's Plan including, but not limited to, Covered

Individuals with Medicare or other third party health insurance or new expansion population.

B. The Contractor shall cooperate with EOHHS to develop an implementation strategy for providing services to any new Covered Individual group.

Section 2.18 Third-Party Liability Benefit Coordination and Recovery

A. General Requirements

1. The Contractor shall develop and submit to EOHHS for approval a work plan for Third-Party Liability (TPL) benefit coordination and recovery that:

   a. Ensures that MassHealth is the payer of last resort for the BH Covered Services provided under this Contract;

   b. Ensures recovery of funds inappropriately paid to Network Providers;

   c. Avoids payment for all Claims or services that are subject to third-party payment;

   d. Ensures that the Contractor identifies and determines the legal liability of third parties to pay for services furnished to Covered Individuals and Uninsured Individuals, including persons covered by Medicare only;

   e. Includes tasks and time frames associated with the plan; and

   f. Addresses systems and resources required to perform at a minimum the following activities:

      1) Identification of Covered Individuals and Uninsured Individuals who have other health insurance, and notification of EOHHS with respect to Covered Individuals; and

      2) Reporting to EOHHS information on cost avoidance and recovery amounts.

B. Payment Recovery

The Contractor shall retain any payments recouped from Network Providers as a result of the discovery of TPL, deposit them into the Direct Service Reserve Account (DSRA) and use all such recoveries to offset BHP expenditures related to the delivery of BH Covered Services.

C. System Requirements Related to Third-Party Liability and Benefit Coordination

Unless otherwise directed by EOHHS, the Contractor shall coordinate the Behavioral Health benefits of Covered Individuals with TPL with the other insurance resource, such as Medicare or commercial insurance, as described in **Section 2.18.A**. In order to meet this requirement, the Contractor shall have all necessary changes to its operations in place by the Operational Start Date, and shall continue to make all appropriate changes to its operations in compliance with any new policies from the EOHHS TPL Unit, including but not limited to changes to the following:

1. Management information systems;
2. Claims authorization systems;
3. Claims payment systems;
4. Staffing within the Claims Operation Department; and
5. Reporting.

D. Claims Payment Requirements for Covered Individuals under Age 21 with TPL

1. The Contractor shall ensure that providers who provide BH Covered Services to Covered Individuals with TPL make diligent efforts to identify and obtain payment from all other liable parties, including insurers, as described in 130 CMR 450.316;
2. If a third-party resource is identified after the Provider has already billed and received payment from the Contractor, the Provider promptly returns any payment it received from the Contractor and ensure that the Provider bills all third-party resources before resubmitting a Claim to the Contractor;
3. The Contractor shall ensure that providers who submit Claims for Covered Individuals who have Medicare in addition to Medicaid:
    a. bill the Medicare fiscal intermediary or carrier in accordance with their billing rules, including using the appropriate Medicare claim form and format;
    b. accept assignment according to Medicare instructions; and
    c. follow the Contractor's billing instructions, including any billing instructions specific to Medicare crossover claims.
4. The Contractor shall not pay Providers:
    a. who do not make diligent efforts to obtain payment from other liable parties; or
    b. for services provided to a Covered Individual, if on the date of service the Covered Individual had other health insurance, including Medicare, that may have covered the service, and the Provider did not participate in or

resort to the Covered Individual's other insurance plan, including Medicare.

5. For Covered Individuals under 21 with commercial Third Party Liability, payment shall not exceed the Covered Individual's liability, including co-insurance, deductibles and copayments; or the Provider's charges or the Contractor's payment amount, whichever is less.

6. For Covered Individuals under 21 with Medicare, the payment amount shall not exceed the coinsurance and deductible amounts as reported on the explanation of benefits or remittance advice from Medica re; the Contractor's payment amount, or the Medicare-approved amount, except for specific programs as approved and directed by EOHHS.

7. The terms of this **Section 2.18.D** apply to all Covered Services provided to Covered Individuals.

Section 2.19 PCC Plan Support Services (PSS) Program

A. PCC Plan Support Services (PSS)

The Contractor shall:

1. Establish, implement and maintain a PSS program for PCCs that measures, monitors and promotes improvements in health care delivery systems, including integration of care, at the PCC practice level;

2. Review, update, and establish any new written standard operating policies and procedures for the Contractor's staff associated with the PSS program;

3. Provide to EOHHS for review and approval, copies of the standard operating policies and procedures for the PSS program as part of the readiness review process and annually, within three months of the first day of the Contract Year and modify such policies and procedures in support of the PCC Plan as directed by EOHHS;

4. Conduct profiling of PCC Plan providers as detailed in **Section 2.8.H**.

5. Accept and promptly utilize any data files that EOHHS provides in connection with the PSS program, in the format determined by EOHHS;

6. Notify EOHHS if, after diligent effort on the part of the Contractor, a PCC refuses to cooperate with the PSS program or other Contract requirements;

7. Develop and implement written action plans, as needed, related to reports produced for PCC Service Locations. Prior to developing such reports, the Contractor shall certify the accuracy of the data to EOHHS regarding these reports as required in **Section 2.14.M;**

8. Provide support to PCCs consistent with integration of Behavioral Health, medical care, long-term services and support, and social services;

9. Provide support to PCCs as required related to ICMP activities as follows:

    a. Strengthen PCCs' relationship to ICMP, including improving communications, and enhancing and expanding use of ICMP for Enrollees; and

    b. Manage and coordinate PCC inquiries, requests, and concerns regarding interacting with ICMP.

10. Provide support to PCCs as required related to PBCM activities as follows:

    a. Support PCCs with the implementation of new PBCM programs, including evaluating the PCC for readiness to perform care management activities;

    b. Provide on-going support to the PBCM program, including identifying strategies for process improvements for outreaching and engaging Enrollees in the PBCM program, improving workflows, and providing technical assistance related to reporting and other operational issues;

    c. Monitor compliance of PBCM programs with care management activities; and

    d. Manage and coordinate PCC inquiries, requests, and concerns regarding interacting with the PBCM program.

11. Support PCCs in understanding and, as appropriate, transitioning to the ACO programs, as directed by EOHHS. These areas of support may include but are not limited to:

    a. Maintaining and implementing protocols for handling PCC inquiries, requests and concerns received by the Contractor regarding the ACOs; and

    b. Collaboratively working with current PCC sites, which may be joining an ACO in the future, to assist with coordination and transition of care.

12. Represent the PCC Plan and EOHHS with respect to PCC Plan activities at provider conferences, community agency meetings and other forums that require a PCC Plan presence, if requested or approved by EOHHS;

13. Establish relationships with other EOHHS contractors (e.g., the MassHealth Contact Center vendor, the Business Support Services vendor) and refer PCCs to the appropriate vendor in order to resolve questions and issues such as eligibility, claims and billing inquiries, and to provide file updates; and

14. In addition to submission of the monthly PSS report(s) outlined in **Appendix E-1**, submit to EOHHS an annual report on the PSS activities for the Contract Year.

B. Compliance with PCC Plan Provider Contract with EOHHS

The Contractor shall:

1. Annually submit a report to EOHHS documenting the process used to monitor PCC compliance with the EOHHS PCC Plan Provider Contract in areas such as outreach and appointment times as set forth in **Appendix C**;

2. Refer PCCs to the Customer Service Center for Providers for enrollment with the MassHealth Provider Online Service Center (POSC) and Job Aids (Enrollment Roster, Referral) to support compliance with the PCC Contract;

3. Reinforce the importance of updating and inform PCCs on how to update PCC information with MassHealth Customer Service Center for Providers including but not limited to Provider information and capacity;

4. Assist PCC Plan staff with ensuring that all Providers who wish to remain in the PCC Plan network sign and return to EOHHS new PCC Provider Contracts whenever MassHealth updates such contracts; and

5. Report to EOHHS any PCC who could benefit from outreach by MassHealth's Customer Service Center for Providers, Provider Outreach and Education Unit to support delivery of services to PCC Plan members.

C. PSS Site Visits

1. PSS Introduction Visit to new or returning PCCs

The Contractor shall:

a. Conduct an introduction visit with each PCC new to participation in or returning to the PCC Plan, regardless of the PCC's enrollment roster/panel size;

b. Ensure that the PSS introduction visit includes:

1) An introduction to the Contractor and a description of the Contractor's role and the PSS program;

2) A discussion regarding the PCC's current priorities and engagement with MassHealth Covered Individuals and health plans;

3) A discussion of the current EOHHS and PCC Plan goals and policies;

4) A description of available Contractor programs, including but not limited to care management (ICMP and PBCM) and CBHCs;

5) A description of materials that are used in the PSS program;

6) The PCC's Support Manager's name, telephone number, and e-mail address;

7) A description of any additional reports and and/or information as directed by EOHHS; and

8) A review of the PCC Plan Contract.

2. PSS On-going Site Visits

After the introduction visit, the Contractor shall conduct PSS site visits according to an EOHHS-approved schedule. The Contractor shall review the needs of the PCC, PCC Service Location, or EOHHS prior to scheduling a site visit, including PCC-specific and/or PCC Service Location-specific data, and shall conduct site visits to PCCs and PCC Service Locations as appropriate, or as requested by the PCC or PCC Service Location.

a. Within 30 days of the start of the Contract Year, the Contractor shall develop and propose for EOHHS's approval a detailed plan for PSS site visits to all PCCs and PCC Service Locations that meet the site visit criteria agreed to by EOHHS. Such proposal shall include, at a minimum, the following elements:

1) A schedule for PSS site visits that is specific to each PCC and PCC Service Location, based on the agreed-upon site visit criteria and the PCC's priorities and performance;

2) The criteria by which PCCs and PCC Service Locations will be visited, including frequency for visits;

3) The content and subject matter of the site visits or, for those PCCs that may not receive a visit, other communications;

4) A description of how the Contractor will support PCC questions regarding Claims payment or other PCC Plan services not managed by the Contractor;

5) A description of how the Contractor will prioritize and promote integration of Behavioral Health and medical care, and care management efforts for Enrollees as part of each site visit;

6) A method for documenting the site visits and the communications that have taken place with PCCs and PCC Service Locations;

7) A method and timeframe for evaluating the success of PSS site visits under the Contractor's proposal;

8) A description of any additional reports and/or information as directed by EOHHS; and

9) A plan to prioritize in person site visits for both new and on-going site visits.

b. Subject to EOHHS approval, the Contractor shall implement its PSS site visit proposal.

c. The Contractor shall work with PCCs and PCC Service Locations to schedule a convenient time for PSS site visits.

d. The Contractor shall make best efforts to inform the medical director of the PCC in the site visit, and shall advise the PCCs and PCC Service Locations that appropriate clinical and non-clinical staff should attend the site visit.

e. The Support Manager shall discuss other related PCC issues as identified by the PCC or the Support Manager, or as directed by EOHHS.

f. The Support Manager shall conduct the PSS site visit and other EOHHS or Contractor staff shall attend, at the discretion of EOHHS.

g. At each PSS site visit, the Support Manager shall review with the PCC any new PCC Plan Support Services Materials and inquire of any PCC-developed materials useful for Enrollees including how and where the materials can be accessed.

h. The Contractor shall maintain and document ongoing communication with PCCs and PCC Service Locations through additional site visits, email, and telephone follow-up, as appropriate or as directed by EOHHS.

i. The Contractor and EOHHS may negotiate a modified schedule and methodology for PSS site visits and, with EOHHS approval, the Contractor shall perform PSS site visits in accordance with such alternate schedule and methodology.

j. The Contractor shall prepare, deliver to, and discuss with PCC Plan staff a detailed report of site visits on a monthly basis. The Contractor and EOHHS may negotiate report format, contents, and frequency during the term of the Contract.

k. At the direction of EOHHS, the Contractor shall perform an in-person site visit with a PCC Service Location irrespective of the PCC enrollment roster/panel size. The Contractor will submit a Standard Operating

Procedures/Policies and Procedures with details of the in-person site visits agreed upon with EOHHS.

l. At the direction of EOHHS, the Contractor shall collaborate with former PCC Plan Services locations that intend to re-apply to become a PCC Plan Service location.

3. PSS Joint Visits with the Contractor's Behavioral Health Provider Quality Manager and a Member of the Contractor's ICMP

The Contractor shall develop and propose for EOHHS's approval a plan for PSS and BH or ICMP joint site visits. Such proposal shall include, at a minimum:

a. The criteria by which joint visits will be conducted;

b. The content and subject matter of the site visit; and

c. A description of how the Contractor will support integration of Behavioral Health, medical care, and social services.

D. PCC Performance Dashboard

1. PCC Performance Dashboard (PD)

At the request of EOHHS, the Contractor shall:

a. Develop a PCC Performance Dashboard (PD) for each PCC and PCC Service Location(s) that meets the threshold number of Enrollees as agreed to by EOHHS and the Contractor. The PD shall be implemented and updated according to a schedule determined by EOHHS. The population included in the PCC Performance Dashboard shall only be Covered Individuals who are PCC Panel Enrollees. It shall not include Covered Individuals who are members enrolled in a Primary Care ACO, Children in the Care and/or Custody of the Commonwealth, and members in MassHealth Standard or CommonHealth with other insurance;

b. Produce the PDs as requested by EOHHS;

c. Ensure the PDs are formatted in a user-friendly style approved by EOHHS;

d. One month prior to the dissemination of the PD, prepare for EOHHS's prior approval a written user's guide that explains the purpose of the report and the information it contains;

e. Include in each PD PCC-specific site information and PCC Panel Enrollee demographics;

f. Include in each PD all measures agreed to by EOHHS. Measures shall be reported by both PCC and PCC Service Location level, when applicable.

Such measures are subject to change during the term of the Contract. For each measure, the Contractor shall:

1) Present PCC-specific data; and

2) Compare each PCC's performance using appropriate benchmarks and trended indicator rates as directed by EOHHS, such as:

a) aggregate PCC Plan performance;

b) available national, state, local or industry benchmarks; and

c) the PCC's PD trended data;

g. Include in the PD a one-page summary of trended rates for the PCC and by PCC Service Location for all clinical measures, as appropriate; compare the Service Location rates to that of the PCC entity, other PCC Service Locations, the overall PCC Plan rates, and other benchmarks as directed by EOHHS;

h. Maintain a secure platform that provides each PCC and PCC Service Location access to their current PD report and ensure that the current PD report remains posted until the next cycle's PD is released or, subject to EOHHS's approval, develop an alternative mechanism for dissemination of the PCC PD report;

i. Within one business day of posting the updated PD, notify PCCs and PCC Service Locations via email that the reports are available; and

j. Design and propose for EOHHS approval additional clinical indicators that address medical and Behavioral Health integration as aligned with EOHHS's dashboard.

2. Additional Reports and Reporting Activities

a. The Contractor shall propose to EOHHS additional reports to support the PSS program, as appropriate.

b. Upon the request of EOHHS, the Contractor shall produce additional PSS reports, including but not limited to, analysis of trends identified from PSS data, data and analytics on population health management, and other supplemental and management reports that support quality and integration activities as negotiated by the parties.

c. Upon the request of EOHHS, the Contractor shall participate in activities to enhance and align with any existing dashboards designed by EOHHS. EOHHS and the Contractor may negotiate alternate PD measures, report formats, methods and timeframe for these activities including design and

propose for EOHHS approval additional clinical indicators that address medical and Behavioral Health integration.

d. EOHHS may, at its discretion, instruct the Contractor to replace the production of certain existing reports with reports generated for PCCs and PCC Service Locations as part of other EOHHS programs and/or initiatives.

3. Reports for PCCs

The Contractor shall:

a. Develop and distribute reports to the PCCs at a frequency approved by EOHHS in content areas, including but not limited to, Enrollees identified as High Risk as defined by EOHHS and the Contractor and:

1) Their enrollment in the Care Management Program;

2) Their emergency department utilization; and

3) The Top Five Outpatient Behavioral Health Report that identifies the top five Behavioral Health providers of outpatient services used by PCC Plan Enrollees in a PCC panel;

b. Maintain a secure transmittal process for such reports to each PCC and PCC Service Location.

E. PCC Plan Support Materials

The Contractor shall:

1. Develop and update the Health Literacy Library as directed by EOHHS. Topics shall clearly and concisely describe relevant health education, including medical, Behavioral Health, substance use, chronic disease management, and wellness/prevention topic areas. The Contractor shall submit new or updated materials to EOHHS for prior approval.

2. Establish a plan to review with EOHHS the current PCC Plan Support Materials, at EOHHS's request, to determine the need for revised, additional, or replacement Support Material necessary to support improved Member experience and integration of physical and Behavioral Health care. The Contractor shall deliver materials for EOHHS approval within required timeframes, as determined by EOHHS.

3. Maintain a sample original package of all PCC Plan Support Materials and an inventory including a list of topics for which PCC Plan Support Materials are available.

F. Education and Training

The Contractor will be responsible for the coordination of educational and training opportunities for PCCs and PBCMs that serve Enrollees. The Contractor shall collaborate with stakeholders and subject matter experts both internally and externally to identify relevant training topics that will support current and future EOHHS initiatives. These shall include educational opportunities, such as learning collaboratives, regional learning sessions, or other educational modes that support PCCs and PBCMs that serve Enrollees to engage in group learning and identified topics.

G. Provider and PCC Publications

1. Provider Connection Newsletter

a. The Contractor shall

1) At the direction of EOHHS, annually create, produce and electronically transmit to each network provider and PCC a PCC Plan newsletter to be entitled "Provider Connection." Each issue may include relevant information regarding Contractor efforts to enhance the integration between medical and Behavioral Health care and the opportunities for support of PCCs and other Providers in the care of Enrollees who have complex medical and/or Behavioral Health care needs through the Care Management Program. EOHHS reserves the right to modify the name, format or content of this newsletter at any time.

2) At least one time per year, meet with EOHHS staff regarding the mission and themes for the upcoming year's newsletters.

3) Submit a written plan to EOHHS for approval regarding the formatting, production and distribution of the newsletter prior to each scheduled publication of "Provider Connection" in a timeframe agreed to by EOHHS.

4) Prepare newsletter content as follows:

a) Collect potential article ideas consistent with the approved newsletter theme from appropriate sources;

b) Present all the potential article ideas to EOHHS for review and approval to be included in the upcoming newsletter;

c) Solicit authors for approved articles ideas. If an appropriate author cannot be identified, the Contractor may author the article; and

d) Edit articles submitted and review draft with appropriate stakeholders, including a medical professional, before submitting a final draft to EOHHS.

5) Format and design the layout of the newsletter such that is visually appealing, using graphics and illustrations in the production of each issue, unless otherwise approved by EOHHS.

6) Distribute the "Provider Connection" newsletter with EOHHS approval.

7) Track Provider Connection reader engagement, including email open rate link clicks, and other metrics determined by EOHHS.

8)

2. PCC Plan Member Newsletter

a. The Contractor shall:

1) At the direction of EOHHS, create, produce and mail to each PCC Plan Member's head-of-household a newsletter entitled "Health Highlights." The "Health Highlights" newsletter may focus on promoting and supporting EOHHS and/or PCC Plan initiatives, its quality improvement activities, the integration of medical and behavioral healthcare, and information on MassHealth covered services as appropriate. EOHHS reserves the right to modify the name, format or content of this newsletter at any time.

2) At least one time per year, meet with EOHHS staff regarding the mission and themes for the upcoming year's newsletter.

3) Submit a written plan to EOHHS for approval regarding the formatting, production and distribution of the newsletter prior to each scheduled publication of "Health Highlights" in a timeframe agreed to by EOHHS.

4) Prepare newsletter content as follows:

a) Collect potential article ideas consistent with the approved newsletter theme from appropriate stakeholders;

b) Present all potential articles ideas to EOHHS for review and approval to be included in the upcoming newsletter;

c) Solicit authors for approved article ideas. If an appropriate author cannot be identified, the Contractor may author the article; and

d) Edit articles submitted and review drafts with appropriate stakeholders, including a medical professional, before submitting a final draft to EOHHS.

5) Format and design the layout of the newsletter such that it is visually appealing, using graphics and illustrations, unless otherwise approved by EOHHS.

6) Submit to EOHHS a proposal for review and approval if the Contractor would like to distribute "Health Highlights" electronically. Such a proposal must maintain the capability to distribute "Health Highlights" in a print format.

7) Print and distribute "Health Highlights" with EOHHS approval.

Section 2.20 Health Equity

A. Health Quality and Equity Committee

1. At all times during the Contract Term, the Contractor shall maintain a Health Quality and Equity Committee (HQEC) designated by, and accountable to a governing board. Such Health Quality and Equity Committee may be an existing Health Equity committee, so long as the committee meets the criteria of this **Section 2.20**.

2. The composition of the Health Quality and Equity Committee shall, to the extent possible, include individuals that represent the diversity of the MassHealth population. The HQEC shall have representation from various stakeholders of the Contractor, including but not limited to:

   a. Representatives from Network Providers that are high performers in Health Equity as determined by the Contractor;

   b. At least two MassHealth Covered Individuals or family members of Covered Individuals;

   c. Providers; and

   d. Frontline staff (e.g., Community Health Workers).

3. Responsibilities of the Health Quality and Equity Committee include but are not limited to:

   a. Developing and steering implementation of the Contractor's Health Equity strategy;

   b. Monitoring progress towards addressing inequities;

   c. Developing Health Equity reporting in accordance with Appendix E-1; and

   d. Sharing all relevant information with the Contractor's PFAC.

B. Population and Community Needs Assessment

1. The Contractor shall conduct a population and community needs assessment that provides an initial description of the Contractor's Covered Individual population, including:

   a. A brief description of the population of Covered Individuals the Contractor serves and the communities in which they live;

   b. A description of the characteristics of such population and communities, including, at a minimum:

      1) The approximate number of Covered Individuals in the population;

      2) The population's demographic characteristics, including but not limited to, age, race, ethnicity, languages spoken, disability status, sexual orientation, and gender identity; and

      3) A description of any other salient characteristics of the population that informs the Contractor's strategy for improving the quality and cost of Covered Individuals care, such as any particular public or environmental health concerns.

   c. A description of the health, functional, and other care needs of such population and communities, including but not limited to:

      1) A list and description of prevalent conditions in the population, including chronic diseases;

      2) A description of the population's behavioral health needs;

      3) A description of the population's Health Related Social Needs;

      4) A description of the community resources that currently exist in such communities.

2. The Contractor shall conduct an updated Population and Community Needs Assessment prior to the start of Contract Year 3.

3. The Contractor must submit this Population and Community Needs Assessment upon EOHHS request.

4. The Contractor may leverage existing community needs assessments to develop its Population and Community Needs Assessment, as long as the assessment meets the requirements of this **Section 2.20.B**.

C. Health Quality and Equity Strategic Plan and Reporting

The Contractor with input from its Health Quality and Equity Committee shall create, monitor, and update as needed a five-year Health Quality and Equity Strategic Plan, which shall be submitted to EOHHS for review and approval in accordance with Appendix E-1. In developing the Contractor's Health Quality and Equity Strategic Plan,

the Contractor shall seek input from the Health Quality and Equity Committee, providers representing the composition of the Contractor's Provider Network, Covered Individuals, and Covered Individual's families.

1. The Health Quality and Equity Strategic Plan shall describe:

    a. How the Contractor sought and incorporated input from the Health Quality and Equity Committee, Providers representing the composition of the Contractor's Provider Network, Covered Individuals, and Covered Individuals' families;

    b. How the Contractor partners with hospitals affiliated with the Contractor for the purposes of the Hospital Health Equity incentive program to further joint Health Equity goals, including a description of joint priorities and how they were determined, as well as joint governance over any included workstreams;

    c. The Contractor's approach to establishing a culture of equity that recognizes and prioritizes the elimination of inequities through respect, fairness, cultural competency, and advocacy, including through the provision of trainings for Health Equity, implicit bias, anti-racism, and related trainings to all staff (contracted or directly employed) that interact with Medicaid enrollees;

    d. The Contractor's approach to ensure all Contractor policy and procedures consider health inequities and are designed to promote Health Equity where possible and in accordance with all federal and state laws, including but not limited to:

        1) marketing strategy;

        2) enrollment and disenrollment;

        3) medical, behavioral health, and other health services policies;

        4) enrollee and provider outreach;

        5) PFACs;

        6) grievances and appeals;

        7) utilization management; and

        8) the Flexible Services program;

    e. How the Contractor used its Population and Community Needs Assessment to inform the Health Quality and Equity Strategic plan;

    f. The Contractor's planned approach to maintaining robust structures to identify and understand inequities to support the implementation of

evidence-based interventions, including to:

1) Engage Covered Individuals and communities to inform Health Equity initiatives;

2) Achieve complete and comprehensive member-reported social risk factor data as further specified by EOHHS (e.g., race, ethnicity, language, disability, sexual orientation, gender identity, Health-Related Social Needs);

g. The Contractor's planned interventions to reduce inequities, including how it will:

1) Collaborate and partner with other sectors that influence the health of individuals;

2) Ensure equitable access to healthcare;

3) Deliver high-quality care that continuously reduces inequities.

2. The Contractor shall include in the plan an executive summary, in a form and format as further specified by EOHHS, and include an overview of all the key sections of the plan.

3. In accordance with Appendix E-1, the Contractor shall regularly report to EOHHS, in a form and format as further specified by EOHHS, on items related to its Health Quality and Equity Strategic Plan, including but not limited to:

a. Any modifications to the organization's Health Quality and Equity Strategic Plan;

b. Health Quality and Equity Committee composition, activities, and how MassHealth Covered Individual and front-line staff feedback is incorporated into decision making processes or otherwise utilized as part of the Health Equity work;

c. PFAC composition, summary of activities, and a summary of how consumer feedback is utilized;

d. Progress towards targeted milestones and any other achievements in the preceding year and since the beginning of the contract period related to:

1) Establishing a culture of equity, as described in **Section 2.20.D**;

2) Establishing necessary structures and partnerships, including but not limited to, with community providers and community hospitals, to support Health Equity;

e. Progress towards targeted milestones in the preceding year and since the beginning of the contract period on implementing interventions related to:

1) Collaborating and partnering with other sectors that impact the health of individuals;

2) Ensuring equitable access;

3) Delivering high quality care that continuously reduces the inequities;

4) Other interventions to reduce health inequities experienced by MassHealth Covered Individuals.

f. Progress towards annual improvement targets for specified Health Equity improvement key performance indicators, supplemented by a description of what contributed to successful achievement of annual targets;

g. Gaps in achievement of targeted annual Health Quality and Equity Strategic Plan goals, observed barriers to achieving goals, and specific plans for the upcoming year to overcome such gaps.

4. At EOHHS's request, the Contractor shall meet with EOHHS to discuss its reporting on items in this **Section 2.20.C**;

5. The Contractor shall publicly post the executive summaries of its Health Quality and Equity Strategic Plan on its website, and make these documents available to EOHHS for posting on EOHHS' website.

D. Health Equity, Anti-Racism, Implicit Bias, and Related Trainings

The Contractor shall ensure that meaningful and appropriate trainings to advance Health Equity are periodically received by all staff and Network Providers (contracted or directly employed) that interact with Covered Individuals (through operations, delivery of services, or other patient interfacing roles (e.g., security officer or receptionist)), in accordance with Section 2.8.I.4.e and as further specified by EOHHS.

E. Culturally and Linguistically Appropriate Services (CLAS) Standards

1. The Contractor shall ensure its Provider Network provides Culturally and Linguistically Appropriate Services (CLAS) to Covered Individuals.

2. In a form and format to be determined by EOHHS, the Contractor shall describe how it intends to assess and address the needs of the populations and communities it intends to serve, including:

a. The linguistic accessibility needs of its Covered Individual population, including Covered Individuals' preferred languages, the needs of Covered Individuals' who are Deaf or hard of hearing, and Covered Individuals' needs related to health literacy. Such linguistic accessibility shall also include access to the Contractor's Provider Network via newer communication modalities, including telehealth;

b. The cultural accessibility needs of its Covered Individuals populations;

c. The needs of Covered Individuals for accessible medical and diagnostic equipment;

d. The process utilized to verify that their Provider directories accurately capture member accommodations capabilities; and

e. Demonstrating current adoption of national CLAS standards within the organization and proposing how it shall further develop CLAS and evaluate gaps in achieving CLAS, including:

1) Training and assessing staff for cultural competencies, including reporting the name of the training curriculum to EOHHS if any;

2) Selecting a CLAS Champion (any individual, clinical or non-clinical, who is knowledgeable about CLAS Standards and can serve as a subject matter expert to support and train others).

3. The Contractor shall have clear and user-friendly processes and policies in place for Covered Individuals to request linguistic interpreters and other linguistic or physical accommodations. The Contractor shall, at a minimum, post such policies on its website and include such policies in its Covered Individual Handbook as set forth in Section 2.10.A.3. They shall also offer this option on their customer service lines, including understanding processes for how to request interpreter services and accommodations. The Contractor shall include a description of Covered Individual rights including but not limited to those Covered Individual rights described in Section 5.1.L, in its Covered Individual Handbook and on its website.

4. The Contractor shall complete a CLAS Standards self-evaluation annually, which can be used as a quality improvement tool to support efforts to implement CLAS and to assess performance and continuous improvement. The Self-Evaluation shall include the following metrics:

a. The percentage of calls conducted in a language other than English, the percentage of Covered Individual-facing materials available in languages other than English, and the number of languages available for real-time interpreter services;

b. Number and types of language or accommodation requests, including any denials;

c. Number of grievances on this topic and/or related to discrimination based on race, ethnicity, language, disability, sexual orientation, gender identity or other characteristics;

d. Number of staff who receive training in culturally and linguistically

appropriate service delivery; and

e. Member satisfaction data to inform culturally and linguistically appropriate services.

5. The Contractor shall take immediate action to improve the delivery of CLAS when deficiencies are identified.

F. Quality and Equity Incentive Program Arrangements

The Contractor shall participate in the MBHV Quality and Equity Incentive Program Arrangement, as set forth in **Appendix G**.

G. Data Collection

The Contractor shall ensure that every Covered Individual is given an opportunity to update their social risk factor data (e.g., race, ethnicity, language, disability, sexual orientation and gender identity) as requested.

H. Demographic Data Governance Function

The Contractor shall establish and maintain a demographic data governance function responsible for overseeing the collection, use, analysis, and communication of demographic data. This function must ensure that all member demographic data is handled with the highest level of respect, privacy, and integrity. The governance function shall:

1. Support the appropriate and ethical use of demographic data including through providing guidance on allowable and disallowable uses of the data.

2. Provide guidance for the appropriate analysis and stratification of demographic data to identify, understand, and address disparities.

3. Identify and implement standards for communicating demographic data and associated findings in a respectful, accurate, and contextually appropriate manner.

4. Work with appropriate internal staff to restrict demographic data access to the appropriate personnel and implement data minimization principles for demographic data users.

Section 2.21 COVID-19 Efforts

A. As further specified by EOHHS, the Contractor shall help manage COVID-19 and any additional Public Health Emergencies (PHE) as set forth in MassHealth bulletins, including but not limited to MassHealth managed care entity bulletins, and other MassHealth guidance. Such activities to help manage COVID-19 or other PHE shall include, but may not be limited to:

1. Taking all necessary steps to enable Covered Individuals to obtain medically necessary and appropriate Covered Services.
2. Delivering all Covered Services in an amount, duration and scope that is no more restrictive than the MassHealth fee-for-service program, and staying up to date on any changes to the amount, duration, and scope of services that MassHealth may announce via bulletins or guidance.
3. Communicating, with EOHHS prior approval, relevant benefits, prevention, screening, testing, and treatment options to Covered Individuals and guidelines for contacting a Covered Individual's local board of health or health care provider.

Section 3. EOHHS RESPONSIBILITIES

Section 3.1 Contract Management

A. Administration

EOHHS shall:

1. Designate a Contract Manager for the Contract, who shall act as liaison, coordinate all requests and activities between the Contractor and EOHHS, and between the Contractor and the other state agencies involved with or affected by the Contract, for the duration of the Contract. EOHHS may change its designation of Contract Manager at any time during the Contract, and shall provide the Contractor with notification of any such change. The Contract Manager shall represent EOHHS in all programmatic and operational aspects of the Contract.
2. Provide the Contractor with available information and data in its possession necessary for successful performance of the Contract.
3. Furnish the Contractor with copies of EOHHS regulations, policies and procedures that may materially affect the Contractor's performance of its contractual obligations.
4. Notify the Contractor of any changes to the PCC Plan, the PCACOs and other EOHHS programs, regulations, policies and procedures, operations or systems that may materially affect the Contractor's performance of its contractual obligations.
5. Notify the Contractor of the Contract requirements on which EOHHS will base its annual review of the Contractor's performance on its Quality Management/Quality Improvement program.
6. Review and approve all materials, policies and procedures developed by the Contractor when such review and approval is required by the Contract.
7. Review the Contractor's submitted reports and reserve the right to request additional reports.
8. Meet with the Contractor's representative(s) on a monthly basis, or more often as either party deems necessary.
9. At its discretion, attend meetings or other activities conducted by the Contractor.
10. At any time during the term of the Contract, as appropriate, initiate negotiations with the Contractor to revise the scope of the Contract to meet EOHHS's needs.
11. Review any Contractor-proposed revisions to the scope of the Contract and approve, reject or modify the Contractor's proposal.

12. Pay the Contractor in accordance with **Section 4** of the Contract.

13. At its discretion, attend Provider site visits conducted by the Contractor.

14. Inform the Contractor of new PCCs to be included in PSS activities.

15. EOHHS may, in its discretion direct the Contractor to establish payment rates that are no greater than a certain percentage of the MassHealth Fee-For-Service (FFS) rate or another payment rate specified by EOHHS. Such maximum payment rate shall not be less than 100% of the MassHealth FFS rate. EOHHS may approve an exemption from any such requirement upon the Contractor's written request, which shall include the reason(s) why it is necessary for the Contractor to pay a higher rate, such as in order for the Contractor to implement value-based payment arrangements. Nothing in this Section shall relieve the Contractor of its obligations to ensure access to BH Covered Services in accordance with **Section 2.6** of this Contract.

16. At its reasonable discretion, impose financial penalties or other sanctions on the Contractor for failure to meet certain contract provisions or performance measures as detailed in **Sections 5.3.L and M**.

B. Contract Readiness Review

Prior to the Operational Start Date, EOHHS shall conduct a readiness review of the Contractor.

1. EOHHS shall conduct a readiness review of the Contactor that may include on-site review. This review shall include an assessment of the Contractor's ability and capability to perform satisfactorily in the areas set forth in 42 CFR 438.66(d)(4), as applicable. Additionally, this review may include, but is not limited to, the elements described in **Section 2.2.B.3.b**.This review begin no later than 90 days prior to the Operational Start Date.

2. EOHHS may conduct the readiness review to verify the Contractor's assurances that the Contractor is ready and able to meet its obligations under the Contract. EOHHS reserves the right to conduct an additional readiness review in the event that additional populations become managed care eligible or eligible to enroll with the Contractor.

3. EOHHS shall identify to the Contractor all areas where the Contractor is not ready and able to meet its obligations under the Contract and may, in its reasonable discretion, allow the Contractor to propose a plan to remedy all deficiencies prior to the Operational Start Date. Alternatively, EOHHS may, in its reasonable discretion, postpone the Operational Start Date if the Contractor fails to satisfy all readiness review requirements

4. If, for any reason, the Contractor does not fully satisfy EOHHS that it is ready and able to perform its obligations under the Contract prior to the Operational Start Date, and EOHHS does not agree to postpone the Contract Operational Start Date, or extend the date for full compliance with the applicable Contract requirement, then EOHHS may terminate the Contract and shall be entitled to recover damages from the Contractor.

C. Performance Evaluation

EOHHS shall, at its discretion:

1. Annually review the impact and effectiveness of the Quality Management/Quality Improvement program by reviewing the results of performance improvement projects, performance on standard measures, and all other quality initiatives specified in **Section 2.13.C.**

2. On an ongoing basis, monitor and evaluate the Contractor's compliance with the terms of this Contract, including, but not limited to, the reporting requirements in **Appendix E-1,** the performance measurement and performance improvement projects set forth in **Section 2.13.C** and the Behavioral Health performance incentives set forth in **Appendix G**, and shall at its discretion, monitor and evaluate any or all of the Contractor's operational processes and metrics that indicate the Contractor's organizational health. EOHHS will provide the Contractor with the written results of such evaluations, including, at its discretion, how the Contractor has performed relative to its own previous performance and relative to the MassHealth benchmarks.

3. Conduct periodic audits of the Contractor, as further described in **Sections 4.8 and 5.4**, including, but not limited to, annual Quality Improvement Projects, as specified in **Section 2.13.C**, and an annual operational review site visit pursuant to **Section 2.16**.

4. Perform additional periodic programmatic and financial reviews. These may include on-site inspections and audits, by EOHHS or its agent, of the records of the Contractor and Network Providers. EOHHS reserves the right to confirm and validate, through both the collection of information and documentation from the Contractor and onsite visits to Network Providers, the existence of a contract between the Contractor and each individual Provider in the Provider Network;

5. Evaluate, in conjunction with the U.S. Department of Health and Human Services, through inspection or other means, the quality, appropriateness, and timeliness of services performed by the Contractor and all Behavioral Health Network Providers and PCC Plan Providers.

6. On a semiannual basis, conduct a "lessons learned" exercise with the Contractor. The results shall be used by EOHHS and the Contractor to improve and refine performance as it relates to the responsibilities of this Contract.

7. Provide reasonable notice to the Contractor prior to any on-site visit to conduct an audit, and further notify the Contractor of any records EOHHS wishes to review.

8. Inform the Contractor of the results of any performance evaluations and of any dissatisfaction with the Contractor's performance, and reserve the right to demand a corrective action plan as set forth in **Section 5.3.M**, or to apply one or more of the sanctions provided in **Section 5.3.L**, including termination of the Contract in accordance with **Section 5.5**.

Section 3.2 Coordination of Benefits

A. EOHHS shall, via the HIPAA 834 Outbound Enrollment file, provide the Contractor with all third party health insurance information on Covered Individuals where it has verified that third party health insurance exists.

B. EOHHS shall refer to the Contractor the Covered Individual's name and pertinent information where EOHHS knows a Covered Individual has been in an accident or had a traumatic event where a liable third party may exist.

C. EOHHS shall develop Base Capitation Rates that are net of expected TPL recoveries, consistent with the Contractor's obligation under this Contract to recover claims paid to Providers where the other insurer was primary.

Section 3.3 Enrollment and Disenrollment

A. EOHHS shall, as appropriate, enroll, disenroll and re-enroll Covered Individuals with the Contractor. EOHHS shall:

1. Maintain the sole responsibility for the enrollment of Covered Individuals into the Contractor's plan, as described in this **Section 3.3**. The Contractor shall accept all Covered Individuals enrolled or re-enrolled by EOHHS.

2. On each business day of the Contract Year, make available to the Contractor, via the HIPAA 834 Outbound Daily Enrollment file, information pertaining to all enrollments, including the Effective Date of Enrollment, which will be updated on a daily (business day) basis.

3. At its discretion, and as appropriate, instruct the Contractor to resolve enrollment discrepancies through a manual system approved by EOHHS.

4. At its discretion, automatically re-enroll on a prospective basis with the Contractor any Covered Individuals who were disenrolled due to loss of eligibility and whose eligibility was re-established by EOHHS.

5. Disenroll a Covered Individual from the Contractor's plan and he or she shall no longer be eligible for services following:

   a. Loss of MassHealth eligibility;

   b. Completion of the Covered Individual's voluntary disenrollment request; or

   c. Loss of eligibility for MassHealth Managed Care.

6. On each business day of the Contract Year, make available to the Contractor, via the HIPAA 834 Outbound Enrollment File, information pertaining to all disenrollments, including the Effective Date of Disenrollment and the disenrollment reason code.

7. Make best efforts to provide the Contractor with the most current demographic information available to EOHHS. Such demographics shall include, when available to EOHHS, the Covered Individual's name address, MassHealth identification number, date of birth, telephone number, race, gender, ethnicity and primary language.

8. Review and respond to written complaints from the Contractor about EOHHS's Customer Services vendor or such vendor's subcontractors, or EOHHS's contracted Enrollment Broker within a reasonable time. EOHHS may request additional information from the Contractor in order to perform such review.

Section 3.4 Information Systems

EOHHS shall:

A. Cooperate with the Contractor on any system implementation or enhancement necessary to meet the requirements of the Contract that affects either EOHHS's MMIS or the Contractor's MIS through the term of the Contract.

B. Provide technical assistance as necessary for the Contractor to gain access to specified EOHHS systems where such access is required by the Contract.

C. Provide and maintain a list of access codes for all Contractor staff requiring access to EOHHS systems.

D. Assist the Contractor, as necessary, to verify a Covered Individual's eligibility status with the Contractor.

Section 3.5 Marketing

EOHHS shall:

A. Monitor the Contractor's Marketing activities and distribution of related materials; and

B. Within fifteen (15) business days of receipt of Marketing Material submitted by the Contractor in compliance with **Section 2.11.A.3**, take one of the following actions:

1. Approve or disapprove the Marketing Material;
2. Require modification to the Marketing Material; or
3. Notify the Contractor that EOHHS requires an additional ten (10) business days from the date of such notification to take the actions described in **B.1** or **B.2** above.

The Contractor shall comply with any such EOHHS action. EOHHS's failure to take any of the actions described in **B.1, 2 or 3** above within 30 business days after receipt of the Contractor's Marketing Material, shall be deemed to constitute approval of said Marketing Material. Further, EOHHS's failure to take any of the actions described in **B.1 or B.2** above within ten (10) business days after notification of the Contractor in accordance with **B.3**, shall be deemed to constitute approval of the Marketing Material, as shall EOHHS's failure to respond within ten (10) business days of receipt of modifications to Marketing Materials submitted to EOHHS pursuant to **B.2** above.

Section 3.6 Additional Covered Individual Groups

EOHHS may:

A. Develop and implement, in consultation with the Contractor, and other entities such as but not limited to Accountable Care Partnership Plans and MassHealth-contracted MCOs, necessary processes and procedures required to implement enrollment of additional MassHealth Covered Individual groups, as further specified by EOHHS;

B. Develop a Behavioral Health benefit package for any such MassHealth coverage group which to the extent practicable is consistent with Behavioral Health Covered Services for other MassHealth coverage groups;

C. Inform the Contractor regarding demographic characteristics and utilization experience of any new group of Covered Individuals group prior to initiation of enrollment to the extent that such information is available;

D. Develop a Capitation Rate(s) for such Covered Individual group(s) consistent with 42 CFR 447.361 and in consultation with the Contractor; and

E. Develop, in cooperation with the Contractor, an implementation strategy for providing services to Covered Individuals.

Section 4. PAYMENT AND FINANCIAL PROVISIONS

Section 4.1 Rating Categories (RCs) for Covered Individuals

A. RC I (Families) Adults

RC I Adults includes MassHealth Members between the ages of 21 and 65 who are enrolled in MassHealth Standard, including individuals receiving Transitional Aid to Families with Dependent Children (TAFDC) benefits; MassHealth Members who are categorically related to the TAFDC program, (excluding spend-down cases); MassHealth Members between the ages of 21 and 65 under the Refugee Resettlement Program, MassHealth Members in MassHealth (Family Assistance); RC I Adults excludes individuals who have Third-Party Liability coverage.

B. RC I Children (Families)

RC I Children include MassHealth members under the age of 21 who are enrolled in MassHealth Standard, including individuals receiving Transitional Aid to Families with Dependent Children (TAFDC) benefits; MassHealth Members who categorically related to the TAFDC program, (excluding spend-down cases); MassHealth Members from the age of 0 through age 20 under the Refugee Resettlement Program, MassHealth Members in MassHealth (Family Assistance); RC I Children excludes individuals who have Third-Party Liability coverage.

C. RC I Children under 21 with TPL Only

RC I Children under 21 with TPL Only includes MassHealth Members in MassHealth Standard under age 21 with Third- Party Liability coverage, including Medicare, coverage from any other public payer, or commercial insurance.

D. RC II (Disabled) Adults

RC II Adults includes: MassHealth Members between the age of 21 and 65 who are disabled and receiving Supplemental Security Income (SSI), excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Members who are disabled, excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Members receiving SSI and Massachusetts Commission for the Blind benefits, excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Members of the Massachusetts Commission for the Blind excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Standard (Disabled) Members; and Members of MassHealth CommonHealth who have no Third-Party Liability coverage.

E. RC II Children (Disabled)

RC II Children includes: MassHealth Member under the age of 21 who are disabled and receiving Supplemental Security Income (SSI), excluding those individuals who receive

either Medicare Part A or Medicare Part B benefits; MassHealth Members who are disabled, excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Members receiving SSI and Massachusetts Commission for the Blind benefits, excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Members of the Massachusetts Commission for the Blind excluding those individuals who receive either Medicare Part A or Medicare Part B benefits; MassHealth Standard (Disabled) Members; and Members of MassHealth CommonHealth who have no Third-Party Liability coverage.

F. RC II Children under 21 with TPL Only

RC II Children under 21 with TPL Only includes MassHealth Members in MassHealth Standard (Disabled) and CommonHealth under age 21 with Third-Party Liability coverage, including Medicare, coverage from any other public payer, or commercial insurance.

G. RC IX (CarePlus)

RC IX includes Covered Individuals over the age of 20 and under the age of 65 with incomes up to 133 percent of the Federal Poverty Level (FPL), who are not pregnant, disabled, or a parent or a caretaker relative of a child under age 19, or eligible for other MassHealth coverage. Also excluded from RC IX are individuals who are dually-eligible for Medicaid and Medicare.

H. RC X (CarePlus)

RC X includes Covered Individuals over the age 20 and under the age of 65 with incomes up to 133 percent of the FPL, who are receiving Emergency Aid to the Elderly, Disabled and Children (EAEDC) through the Massachusetts Department of Transitional Assistance. Excluded from RC X are individuals who are pregnant, disabled, or a parent or caretaker relative of a child under age 19, or eligible for other MassHealth coverage. Also excluded from RC X are individuals who are dually eligible for Medicaid and Medicare.

Section 4.2 Payment Provisions and Methodologies

A. Payment for Provision of Covered Services to Covered Individuals

EOHHS shall make payments to the Contractor in accordance with the payment provisions in this Section, including the Behavioral Health Covered Services Capitation Rates, the Administrative Component of the BH Covered Services Capitation Rates, payments made for Risk Sharing, Care Management Payments, and payments made for Performance Incentive Arrangements shall be made in accordance with 42 CFR 438.4-438.8. Except as expressly set forth herein, the Contractor shall accept the payments set forth below as payment in full for the provision of Behavioral Health Covered Services and all other activities described in this Contract.

All payments under this Contract are subject to state appropriation and all necessary federal approvals.

1. Behavioral Health Covered Services Capitation Rates

   EOHHS shall pay the Contractor Behavioral Health Covered Services Capitation Rates for all BH Covered Services provided under this Contract except as set forth in **Section 4.2.A.2** below. All Behavioral Health Covered Services Capitation Rates shall be as set forth in **Appendix H-1**.

2. Exclusions from the Behavioral Health Covered Services Capitation Rates

   EOHHS shall pay the Contractor for AMCI/YMCI including follow-up, CCS and three units of outpatient bundle services provided by CBHC providers to Uninsured Individuals and persons with Medicare only according to the methodology set forth in **Section 4.2.L** and **Section 4.2.V**. EOHHS shall pay the Contractor for AMCI/YMCI including follow-up CCS, and three units of outpatient bundle services provided by CBHC providers to Individuals without Mobile Crisis Coverage according to the methodology set forth in Section 4.2.R. EOHHS shall pay the Contractor for crisis evaluation services provided by hospital providers to Uninsured Persons and Persons with Medicare Only according to the methodology set for in **Section 4.2.S.**

3. Risk-Sharing Arrangements

   The Contractor and EOHHS may share financial risk for Behavioral Health Covered Services. Risk sharing arrangements shall be as set forth in **Section 4.6** and **Appendix H-1**.

4. Administrative Component of the Behavioral Health Covered Services Capitation Rate and Care Management Program.

   a. EOHHS shall pay the Contractor an Administrative Component of the Behavioral Health Covered Services and Care Management Program Capitation Rate for each Contract Year as set forth in **Appendix H-1**.

   b. The Administrative Component of the Behavioral Health Covered Services Capitation Rate shall be based on a Per Member (Covered Individual) Per Month (PMPM) rate that is determined using the Covered Individuals served under the Contract.

5. Performance Incentive Arrangements

   EOHHS and the Contractor may establish Performance Incentive Arrangements. If such Performance Incentive Arrangements are established, EOHHS shall pay the Contractor Performance Incentive Arrangement payments based on EOHHS's assessment of the Contractor's achievement of such Performance Incentives and all terms and conditions for payment as set forth in this Contract and **Appendices**

G and **H-1**. Any such incentive payment shall not result in payments in excess of 105 percent of the approved Capitation Payments.

6. PCC Plan Support Services

EOHHS shall pay the Contractor for the PCC Plan Support Services activities described in **Section 2.19** and other Sections of the Contract, as identified by the parties each Contract Year, as set forth in **Appendix H-1**.

The PCC Plan Support payments shall be based on a fixed rate plus an additional Per Member (Enrollee) Per Month (PMPM) rate that is determined using the number of Enrollees in the PCC Plan above a set number of Enrollees identified in **Appendix H-1**. In its discretion, at any time, EOHHS may review with the Contractor the PCC SS PMPM rate based on significant changes in enrollment, case mix, or other factors. EOHHS may change the fixed and the additional PMPM amount consistent with **Section 4.2.H. and Appendix H-1**.

7. Payment for Provision for ASD-ID and EC MCPAP Programs

EOHHS shall pay the Contractor to provide the ASD-ID, EC MCPAP Programs, as described in **Section 2.6.D.2**. Such payments shall be set forth in **Appendix H-1**. These funds may be used to support MCPAP's role in the expansion of MCPAP for ASD-ID to support pediatric primary care providers, as long as the use of the funds for this purpose has no impact on MCPAP for ASD-ID's ability to fully meet all program requirements.

8. Payment for Crisis Service Safety Net Initiative

EOHHS shall pay the Contractor to administer the Crisis Service Safety Net Initiative. Such payments shall be set forth in **Appendix H-1**.

9. [Reserved]

10. Contractor's Use of Earnings for Compliance with Financial Stability Requirements

In no event shall any portion of the any payments made under this Contract, other than earnings, be used to pay the Contractor's cost for compliance with financial stability provisions (**Section 2.15**).

11. [Reserved]

B. Modification of Covered Services

If, at any time during the term of the Contract, EOHHS directs the Contractor to eliminate or modify BH Covered Services, the Contractor shall accept a modification in Behavioral Health Covered Services Capitation Rates which shall be calculated by EOHHS in consultation with the Contractor.

C. Periodic Rate Review

In its discretion, at any time, EOHHS may review with the Contractor BH Covered Services Capitation Rates and the other financial provisions of this Contract to determine if such provisions should be adjusted due to changes in enrollment, case mix, or other factors. To the extent required by applicable federal law, such payment adjustments shall comply with the principles of actuarial soundness as determined by EOHHS in accordance with 42 CFR 438.4. In the event that EOHHS performs such a Periodic Rate Review and proposes modifications to any financial provisions as a result, the Contractor shall have 60 days to accept such modifications. In the event that the Contractor does not accept the financial provisions within 60 days, EOHHS may terminate the Contract and the provisions of **Section 5.5** shall apply.

D. Adjustment of Compensation

Notwithstanding anything herein to the contrary, in the event of a material change in the scope of Contractor's obligations under this Agreement, including but not limited to a modification of Covered Services, change in applicable law, regulation, accreditation guidelines, policy, process or procedure, or other requirements, ability to perform utilization review, Member enrollment, case mix or other factors, that materially affects Contractor's obligations under this Agreement, Contractor may provide written notice thereof to EOHHS, and the parties shall negotiate in good faith an appropriate adjustment to the compensation to be paid under this Agreement. Such good faith negotiation shall conclude no later than sixty (60) days from the commencement thereof.

E. Annual Negotiation of Financial Terms

In determining the financial terms of the Contract, the Contractor shall meet with EOHHS annually to renegotiate the financial terms for each Contract Year. Such meetings shall begin no later than three months before the end of each Contract Year. EOHHS shall incorporate annual financial terms into the Contract as **Appendix H-1**.

F. Failure to Accept Financial Provisions

1. In the event that the Contractor does not accept financial provisions for the next Contract Year at least 21 days before the start of the new Contract Year, EOHHS shall continue to pay the Contractor under the current year's financial provisions and the Contractor shall accept such payment as payment in full under the Contract subject to **subsections a and b below**. In the event that any component of the current year's financial provisions is outside the actuarially sound range for the new Contract Year as determined by EOHHS' actuaries, then EOHHS shall pay the Contractor within the actuarially sound range for the new Contract Year, and the Contractor shall accept such payments as payment in full under the Contract subject to **subsections a and b** below. EOHHS may halt all new Enrollee assignments into the PCC Plan until the Contractor accepts the financial provisions offered by EOHHS.

a. In the event that the payments made under **Section 4.2.F.1** are higher than the financial provisions for the new Contract Year that the Contractor ultimately accepts, EOHHS may recoup the higher payments made during the interim period.

b. In the event that the payments made under **Section 4.2.F.1** are lower than the financial provisions for the new Contract Year that the Contractor ultimately accepts, EOHHS will not retroactively adjust the lower payments made during the interim period.

c. In the event that the Contractor does not accept the financial provisions within 60 days of EOHHS's offer, EOHHS may terminate the Contract in accordance with **Section 5.5** and the Contractor shall be obligated to continue to perform all obligations under the Contract as described in **Section 5.5.C**, until such time as all Covered Individuals are disenrolled from the Contractor's plan. The Contractor shall accept the lower of the prior year's financial provisions or the financial provisions EOHHS offered for the current year as payment in full during this time period.

G. Monthly Estimated BH Covered Services Capitation Rate Payment Process

1. Each month EOHHS shall pay the Contractor an Estimated Capitation Payment, which will include the BH Covered Services Capitation Payment, in accordance with the following methodology. EOHHS shall:

a. Determine the BH Covered Services Capitation Rates Per-Covered Individual per month (PMPM) rate for each RC.

b. Multiply the estimated number of Covered Individuals for the month, as determined by EOHHS in each RC, by the PMPM amount for the RC.

c. Sum the calculations for each RC; this is the Estimated Monthly BH Covered Services Capitation Amount.

d. For Covered Individuals for whom EOHHS has assigned a specific disenrollment date due to a qualifying event such as a member attaining age 65 within the Payment Month, EOHHS shall make a pro-rated Estimated Capitation Payment to the Contractor. The pro-rated Estimated Capitation Payment will equal:

1) The Behavioral Health Covered Services Capitation Rate,

2) Multiplied by the number of Enrollee Days during the Payment Month

3) Divided by the total number of days in the Payment Month.

H. Methodologies for Administrative Component of BH Capitation Rate

1. Estimated Monthly Administrative Payments

Each month EOHHS shall pay the Contractor an Estimated Administrative Payment, which will include the care management administrative rate, in accordance with the following methodology. EOHHS shall:

a. Determine the estimated number of Covered Individuals in the month.

b. Multiply the estimated number of Covered Individuals, as determined by EOHHS, by the PMPM rate; this is the Estimated Monthly Administrative Component of the BH Covered Services Capitation Rate amount.

I. Methodology for PCC Plan Support Services

Each month EOHHS shall pay the Contractor an Estimated PCC Plan Support Services Payment. The applicable PMPM Plan management support rate will be based in part on the number of Enrollees in the PCC Plan, as further described in **Appendix H-1**.

J. Payment for Provision of Services by Indian Health Care Providers to Indian Enrollees

1. All payments to the Contractor are conditioned on compliance with the provisions below, 42 CFR 438.14, and all other applicable provisions of the American Recovery and Reinvestment Act of 2009. The Contractor shall:

a. Permit Indian Covered Individuals to obtain BH Covered Services from out-of-network Indian Health Care Providers from whom the Covered Individual is otherwise eligible to receive such services. The Contractor shall also permit an out-of-network Indian Health Care Provider to refer an Indian Covered Individual to a Network Provider;

b. Demonstrate that it has sufficient access to Indian Health Care Providers to ensure that Indian Covered Individuals have timely access to BH Covered Services from such providers;

c. Pay both network and non-network Indian Health Care Providers who provide BH Covered Services to Indian Covered Individuals a negotiated rate which shall be no lower than the MassHealth fee for service rate for the same service or the applicable encounter rate published annually in the Federal Register by the Indian Health Service, whichever is greater, or, in the absence of a negotiated rate, an amount not less than the amount that the Contractor would pay for the BH Covered Service provided by a non-Indian Health Care Provider or the MassHealth fee for service rate for the same service, whichever is greater;

d. Make prompt payment to Indian Health Care Providers; and

e. Pay non-network Indian Health Care Providers that are Federally Qualified Health Centers (FQHCs) for the provision of services to an Indian Covered Individual at a rate equal to the rate that the Contractor

would pay to a network FQHC that is not an Indian Health Care Provider, including any supplemental payment described in 42 CFR 438.14(c)(1).

K. Other Provider Payment Provisions

The Contractor shall ensure the following payment provisions are met:

1. Payments to FQHCs and Rural Health Centers (RHCs) for services to Covered Individuals are greater than or equal to the payment amounts described in 42 USC § 1396a(bb). In order to comply with this requirement, the Contractor shall pay FQHCs and RHCs at least the amount MassHealth would pay for such services on a fee-for-service basis as specified in 101 CMR 304.04, et seq., excluding any supplemental rate paid by MassHealth to FQHCs or RHCs.

2. For all allowable individual mental health visits (as defined in 101 CMR 304.02) furnished at FQHCs and RHCs, the Contractor shall use the Health Care Common Procedure Codes (HCPC), G0469 and G0470, and T1040 and TI040-HQ for new and established patients respectively, specified in 101 CMR 304.00, et seq., and shall use no alternative codes for the same or similar services.

3. Payments to any licensed hospital facility operating in the Commonwealth that has been designated as a critical access hospital under 42 U.S.C. 1395i-4 are in an amount equal to at least 101 percent of allowable costs under the Contractor's plan, as determined by utilizing the Medicare cost-based reimbursement methodology, for both inpatient and outpatient services.

L. Payment Provisions for AMCI/YMCI, including follow-up, and Community Crisis Stabilization services for Uninsured Individuals and Persons with Medicare Only

1. General Provisions

The Contractor shall:

a. For AMCI and YMCI, including follow-up, and CCS services for Uninsured Individuals and persons with Medicare only, require CBHCs to bill other insurances (TPL), where available and consistent with **Section 2.18**, and the Health Safety Net in accordance with applicable law.

1) The Contractor shall ensure that providers make diligent efforts to identify and obtain payment from all other liable parties, including insurers;

2) If a third-party resource is identified, the Contractor shall ensure that the Provider bills all third-party resources before resubmitting a Claim to the Contractor;

3) The Contractor shall not pay Providers who do not make diligent efforts to obtain payment from other liable parties.

b. Pay CBHCs the rate for AMCI and YMCI, including follow-up, and CCS services established by EOHHS and, as further directed by EOHHS, implement all policies and procedures with regard to payments and payment methodologies to CBHCs for AMCI, YMCI, and CCS services for Uninsured Individuals and persons with Medicare only delivered under the Contract.

c. Not utilize the Community Crisis Amount except to pay for AMCI and YMCI, including follow-up, and CCS services delivered to Uninsured Individuals and persons with Medicare only.

2. Payment Methodology

a. EOHHS shall annually provide the Contractor with an estimated amount it expects to pay each CBHC for AMCI and YMCI, including follow-up, and CCS services delivered on a Fee-for-Service basis by EOHHS.

b. The Contractor shall provide EOHHS with an annual report of the Contractor's estimate of the total amount it expects to pay for AMCI and YMCI, including follow-up, and CCS services, including both BH Covered Services and DMH Specialty Program delivered under the Contract.

c. Based on the Contractor's estimate of the amount it expects to pay for such AMCI and YMCI, including follow-up, and CCS services, EOHHS shall establish a Community Crisis Amount for Uninsured Individuals and persons with Medicare only.

d. The Community Crisis Amount shall be in accordance with **Appendix H-1**. The Contractor shall develop a plan to monitor and report on, throughout each Contract year, AMCI and YMCI, including follow-up, and CCS expenditures for Uninsured Individuals and persons with Medicare only compared to the amount in **Appendix H-1**. Such report shall also include monitoring of AMCI and YMCI, including follow-up, and CCS expenditures for Covered Individuals.

e. Notwithstanding any other provision of this Contract, EOHHS shall not be required to make any payments for AMCI and YMCI, including follow-up, and CCS services until it has received funding from DMH or the Behavioral Health Access and Crisis Intervention Trust Fund in the amounts necessary to make any such payments.

M. Payment Provisions for ED-based Behavioral Health Crisis Evaluation services for Uninsured Individuals and Persons with Medicare Only

The Contractor shall:

1. For ED-based Behavioral Health Crisis Evaluation services for Uninsured

Individuals and persons with Medicare only, require hospitals to bill other insurances (TPL), where available and consistent with **Section 2.18**, and the Health Safety Net in accordance with applicable law.

2. Pay hospitals the rate for ED-based Behavioral Health Crisis Evaluation services established by the EOHHS and, as further directed by EOHHS, implement all policies and procedures with regard to payments and payment methodologies to hospitals for ED-based Behavioral Health Crisis Evaluation services for Uninsured Individuals and persons with Medicare only delivered under the Contract.

N. [Reserved]

O. Payments for the Department of Public Health Emergency Department Boarding Reduction Grant Initiatives

1. EOHHS shall issue payments to the Contractor, in an amount and frequency specified in **Appendix H-1,** in support of DPH Emergency Department (ED) Boarding Reduction Grant Initiatives aimed at reducing the amount of time individuals wait in EDs for disposition to a 24-hour level of BH care.

   a. The Contractor shall expend the amount described in **Appendix H-1**, to provide grants to reduce the amount of time individuals wait in EDs for disposition to a 24-hour level of BH care through staffing investments and rate incentives associated with fully operationalizing inpatient mental health acute care beds community based acute treatment or crisis stabilization.

   b. The Contractor shall fund staffing investments for culturally and linguistically-competent workforce recruitment, retention and training, such as hiring and retention incentives and loan repayment programs; and

   c. The Contractor shall give priority to grants that support new beds that would be located in underserved areas of the Commonwealth.

P. [Reserved]

Q. [Reserved]

R. Payment Provision for AMCI/YMCI, CCS, and urgent outpatient CBHC bundle services Provided to Individuals without Mobile Crisis Coverage

1. General Provision

   The Contractor shall:

   a. For AMCI and YMCI services for Individuals without Mobile Crisis Coverage, require CBHCs to bill other insurances (TPL), where available and consistent with **Section 2.18**.

1) The Contractor shall ensure that providers make diligent efforts to identify and obtain payment from all other liable parties including insurers;

2) If a third-party resource is identified, the Contractor shall ensure that the Provider bills all third-party resources before resubmitting a Claim to the Contractor;

3) The Contractor shall not pay Providers who do not make diligent efforts to obtain payment from other liable parties.

b. For CBHCs, utilize the rate for AMCI and YMCI services including follow-up, CCS and outpatient CBHC bundle, established by the EOHHS and, as further directed by EOHHS, implement all policies and procedures with regard to payments and payment methodologies to CBHCs for AMCI and YMCI, CCS, and outpatient CBHC bundle services for Individuals without Mobile Crisis Coverage.

1) For AMCI and YMCI services including follow-up, CCS, and urgent outpatient CBHC bundle services the Contractor shall pay the difference between rates as described in Appendix H-1 Section L and the amount covered by a third-party resource.

c. Not utilize the Mobile Crisis Intervention Uncompensated Care Payment except to pay for AMCI and YMCI, CCS, and up to three units of outpatient CBHC bundle services delivered to Individuals without Mobile Crisis Coverage.

2. Payment Methodology

a. The Contractor shall provide EOHHS with an invoice on expenditures at a frequency and format specified by EOHHS in **Appendix E-4**.

b. Based on the Contractor's invoice for expenditures, EOHHS shall make

c. payments in accordance with **Appendix H-1**.

d. Notwithstanding any other provision of this Contract, EOHHS shall not be required to make any payments for AMCI and YMCI services until it has received funding from the Behavioral Health Access and Crisis Intervention Trust Fund in the amounts necessary to make any such payments.

S. Payment Provisions for Crisis Evaluation Services in the Emergency Department Provided to Uninsured Individuals and Persons with Medicare Only

1. General Provisions

The Contractor shall:

a. For crisis evaluation services in the emergency department provided to Uninsured Individuals and Persons with Medicare Only, require hospitals to bill other insurances (TPL), where available and consistent with **Section 2.18**.

b. Pay hospitals the rate for crisis evaluation services in the emergency department established by the EOHHS and, as further directed by EOHHS, implement all policies and procedures with regard to payments and payment methodologies to hospitals for crisis evaluation services in the emergency department for Uninsured Individuals and Persons with Medicare Only.

c. Not utilize the Emergency Department Crisis Evaluation Payment except to pay for crisis evaluation services delivered to Uninsured Individuals and Persons with Medicare Only in an emergency department.

2. Payment Methodology

a. The Contractor shall provide EOHHS with an invoice on expenditures at a frequency and format specified by EOHHS in **Appendix E-4**.

b. Based on the Contractor's invoice for expenditures, EOHHS shall make payments in accordance with **Appendix H-1**.

c. Notwithstanding any other provision of this Contract, EOHHS shall not be required to make any payments for crisis evaluation services in the emergency department until it has received funding from the Behavioral Health Access and Crisis Intervention Trust Fund in the amounts necessary to make any such payments.

T. Payments Related to the Middlesex Restoration Center Planning Grants

EOHHS shall issue payments to the Contractor for work pursuant to **Section 2.7.M** as set forth in **Appendix H-1.** The Contractor shall**:**

1. Expend the amount described in **Appendix H-1**, to provide grants to Community Behavioral Health Centers who fulfill the expectations described in **Section 2.7.O**.

2. Recoup any payments made to an awarded Community Behavioral Health Center that fails to fulfill the requirements of the grant, as further specified by EOHHS.

U. Payment Provisions for Adult Community Crisis Stabilization and Crisis Follow-Up services Provided to Individuals with Third Party Payor Coverage (Effective January 3, 2023)

1. For Adult Community Crisis Stabilization services and Mobile Crisis Intervention, require CBHCs to bill other insurances (TPL), where available and consistent with **Section 2.18**.

2. For the period of June 23, 2023, to September 30, 2023, the Contractor shall perform Third-Party Liability (TPL) benefit coordination and recovery for the services provided to Individuals with coverage by Third Party Payors for Adult Community Crisis Stabilization services and Mobile Crisis Intervention follow-up services.

V. Payment Provision for urgent outpatient CBHC bundle services for Uninsured Individuals and Persons with Medicare Only

1. General Provision

The Contractor shall:

a. For outpatient CBHC bundle services provided to Uninsured Individuals and persons covered by Medicare only who are experiencing a behavioral health crisis, require CBHCs to bill other insurance (TPL), where available and consistent with Section 2.18 and the Health Safety Net in accordance with applicable law.

1) The Contractor shall ensure that providers make diligent efforts to identify and obtain payment from all other liable parties, including insurers;

2) If a third-party resource is identified, the Contractor shall ensure that the Provider bills all third-party resources before resubmitting a Claim to the Contractor;

3) The Contractor shall not pay Providers who do not make diligent efforts to obtain payment from other liable parties.

b. Pay CBHCs the rate for outpatient CBHC bundle services established by EOHHS and, as further directed by EOHHS, implement all policies and procedures with regard to payments and payment methodologies to outpatient CBHC bundle services for Uninsured Individuals and persons with Medicare only who are experiencing a behavioral health crisis delivered under the Contract.

1) For outpatient CBHC bundle services for persons with Medicare only who are experiencing a behavioral health crisis, the Contractor shall pay the difference between rates as described in **Appendix H-1 Section M.1** and the amount covered by a third-party resource.

c. Not utilize the Outpatient Crisis Payment except to pay up to three units of outpatient CBHC bundle services delivered to Uninsured Individuals and persons with Medicare only who are experiencing a behavioral health crisis.

2. Payment Methodology

a. The Contractor shall provide EOHHS with an invoice on expenditures at a frequency and format specified by EOHHS in **Appendix E-4**.

1) Based on the Contractor's invoice for expenditures, EOHHS shall make payments in accordance with Appendix H-1.

2) Notwithstanding any other provision of this Contract, EOHHS shall not be required to make any payments for outpatient CBHC bundle services until it has received funding from the Behavioral Health Access and Crisis Intervention Trust Fund in the amounts necessary to make any such payments.

W. HRSN Supplemental Services Payment Pursuant to **Section 2.6.D.12.g**

1. The non-risk arrangement for payment of HRSN Supplemental Services shall be as follows:

a. On a quarterly basis, or at a frequency to be specified by EOHHS, EOHHS shall pay the Contractor a prospective lump sum amount for HRSN Supplemental Services, as described in **Section 2.6.D.12** and set forth in **Appendix H-1**, for the upcoming quarter or other applicable time period. Such amount shall be based on enrollment of Covered Individuals enrolled in a PCACO and be for the provision of HRSN Supplemental Services and the administrative amount of such services.

b. For each Contract Year, EOHHS shall perform an annual reconciliation after the end of the Contract Year to correct the amount of any payments described above. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies. As directed by EOHHS, the Contractor shall remit to EOHHS the full amount of any overpayment EOHHS made to the Contractor for HRSN Supplemental Services for the Contract Year, as identified by EOHHS. Such payments shall be made either through a check or, at the discretion of EOHHS, through addition to or recoupment from future HRSN Supplemental Services payments and/or reconciliation payments described in **Section 4.2**.

X. Children's Behavioral Health Initiative Provider Payments

For Contract Year 2025, as part of efforts to support the CBHI and CSA provider networks, EOHHS shall provide funding to the Contractor in support of CBHI provider infrastructure and workforce support. The Contractor shall disperse the funding to CBHI and CSA providers as directed by EOHHS.

Y. Community Behavioral Health Center Incentive Program pursuant to **Section 2.8.K**

1. At a frequency specified by EOHHS, EOHHS shall pay the Contractor an amount

equal to the sum of provider payments described in Section 2.8.K for the applicable time period.

2. For each Contract Year, EOHHS shall perform an annual reconciliation after the end of the Contract Year to correct the amount of any payments described in Section 2.8.K. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies.

Section 4.3 Payment Reconciliation Process

A. Enrollment-related Reconciliations

1. EOHHS shall perform the following monthly reconciliations with a lookback period determined by EOHHS and adjust the Estimated Capitation Payment as below:

   a. Covered Individuals Who Change Rating Categories During the Payment Months included in the lookback period.

      EOHHS shall, in the month following the Payment Months in the lookback period, recover from the Contractor the total Estimated Capitation Payment issued to the Contractor for Covered Individuals who change Rating Categories during any of the Payment Months in the lookback period, and issue pro-rated monthly Estimated Capitation Payments that reflect the actual number of Covered Individual Days in any of the months in the lookback period for each of the affected Rating Categories.

   b. Covered Individuals Who Disenroll During the Payment Month

      EOHHS shall, in the month following the Payment Months in the lookback period, recover from the Contractor the total Estimated Capitation Payments issued to the Contractor for Covered Individuals who disenroll from the Contractor's Plan during any of the Payment Months in the lookback period, and issue pro-rated monthly capitation payments to reflect the actual number of Covered Individual days in any of the months in the lookback period.

   c. Covered Individuals Who Enroll During a Payment Month

      For Covered Individuals who enroll in the Contractor's Plan during the Payment Months in the lookback period but after the Estimated Capitation Payment has been issued to the Contractor for any of such Payment Months in the lookback period, EOHHS shall, in the month following the Payment Month, issue pro-rated monthly Estimated Capitation Payments to reflect the actual number of Covered Individual Days with respect to such Covered Individuals for any of the payment months in the lookback

period.

2. Estimated Monthly BH Covered Services Administrative Reconciliation Process

   a. EOHHS shall perform a monthly reconciliation of the Estimated Monthly Payment for Administrative Component of the BH Covered Services Capitation Rate calculated according to **Section 4.3.A.2** against the actual number of Covered Individuals as determined by EOHHS, in accordance with the following methodology. EOHHS shall:

      1) Multiply the actual number of Covered Individuals for the previous month, by the PMPM BH Administrative rate and the Care Management administrative rate amount; this is the Actual Monthly Administrative Component of the BH Covered Services Capitation Rate.

      2) Compare the Estimated Monthly Administrative Component of the BH Covered Services paid for the month against the Actual Monthly Administrative Component of the BH Covered Services Capitation Rate.

3. Estimated PCC PSS Payment Process

   a. Each month EOHHS shall issue monthly payments to the Contractor for PCC Plan Support Services, in accordance with the following methodology. EOHHS shall:

      1) Determine the number of PCC Enrollees for the month using the monthly enrollment file used to generate prospective capitation.

      2) Multiply the number of Enrollees for the month, as determined by EOHHS, by the applicable PMPM Plan management support rate; this payment will be the final Monthly PCC Plan Support Services Payment Amount applicable to the number of enrollees for the month.

4. The Contractor shall provide any information necessary to complete monthly and annual payment reconciliations in the time frame and format specified by EOHHS for Estimated BH Covered Services Capitation Rates, Estimated Monthly Administrative Component of the BH Covered Services, and Estimated PCC PSS Payments.

   a. Based on the comparisons described in **subsection 1, 2 , and 3** above, EOHHS shall determine each month whether overpayments or underpayments were made to the Contractor.

      1) EOHHS shall remit to the Contractor the full amount of any underpayments made for the month. Such payments shall be made

through an adjustment to future Estimated Monthly BH Covered Services Capitation Rates, Estimated Monthly Administrative Component of the BH Covered Services, and future Estimated PCC PSS Payments as applicable, or by another mechanism, as determined by EOHHS.

2) The Contractor shall remit to EOHHS the full amount of any overpayments made for the month. Such payments shall be made through an adjustment to Estimated Covered Services Capitation Rates, Estimated Monthly Administrative Component of the BH Covered Services, and future Estimated PCC PSS Payments, as applicable, or by another mechanism, as determined by EOHHS.

B. Reconciliation Process for AMCI, YMCI, and Community Crisis Stabilization services Provided to Uninsured Individuals and Persons with Medicare Only

1. By 210 days after the end of each Contract Year, the Contractor shall provide EOHHS with a report (see **Appendix E-1**) of the Contractor's actual expenditures for AMCI, YMCI, and CCS services provided to Uninsured Individuals and persons with Medicare only, based on Claims paid through no later than 180 days, including its best estimate of IBNR Claims and any applicable IBNR completion factor reported to EOHHS.

2. EOHHS shall conduct a year-end reconciliation of the Contractor's estimated expenditures on AMCI, YMCI, and CCS services provided to Uninsured Individuals and persons with Medicare only delivered under the Contract against actual expenditures, including IBNR.

3. If actual expenditures are less than the Contractor's estimates, EOHHS shall recoup the difference from the Contractor.

4. If actual expenditures are greater than the Contractor's estimate, EOHHS shall pay the difference to the Contractor.

5. The Contractor and EOHHS shall perform the reconciliation set forth in this section for ESP services provided to Uninsured Individuals and individuals with Medicare only on January 1 and 2, 2023 and as further specified by EOHHS.

C. EOHHS shall perform an annual reconciliation of the Estimated Capitation Payment to adjust for any enrollment discrepancies not included in the monthly reconciliation with the lookback period determined by EOHHS. Such annual reconciliations shall account for enrollment discrepancies related to Covered Individuals who have not resided in Massachusetts according to an EOHHS-specified federal report, Covered Individuals who have become deceased, and Covered Individuals who are Incarcerated, including but not limited to Pre-release Covered Individuals. The Contractor shall work with EOHHS to resolve any discrepancies in any calculations;

D. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies pursuant to the reconciliations in this **Section**. The Contractor shall remit to EOHHS the full amount of any overpayments identified by EOHHS. The Contractor shall report any such overpayments to EOHHS within 60 calendar days of when the Contractor identifies the overpayment. Such payments shall be made either through a check or, at the discretion of EOHHS, through recoupment from future capitation and/or reconciliation payments as described in **Section 4**.

1. Overpayments – Overpayments shall constitute the amount actually paid to the Contractor for all Rating Categories in excess of the amount that should have been paid in accordance with EOHHS's reconciliation.

2. Underpayments – Underpayments shall constitute the amount not paid to the Contractor for all Rating Categories that should have been paid in accordance with EOHHS's reconciliation.

Section 4.4 BH Covered Services Continuing Services Reconciliation

EOHHS shall perform a year-end Continuing Services reconciliation as follows:

A. The Contractor shall process and pay its Providers' Claims for all Continuing Services at the Contractor's contracted rate with its Providers.

B. EOHHS shall perform a reconciliation following the end of the Contract Year to determine those Continuing Service claims paid by the Contractor for which the Contractor's Adverse Action was upheld by BOH and which were provided following the conclusion of the Internal Appeal ("approved Continuing Service claims"); provided that the Contractor submits to EOHHS by 210 days following the end of the Contract Year all data regarding such services, as required in **Appendix E-1**.

C. EOHHS shall pay the Contractor no later than 60 days following the reconciliation set forth in **subsection B** the total value of the approved Continuing Service claims referenced in **subsection B** that were provided in the applicable Contract Year; provided that the Contractor timely submitted all data required by EOHHS pursuant to **Appendix E-1**.

D. Approved Continuing Service claims shall include, at a minimum, the following information:

1. Covered Individuals information, by MID, including date of birth, sex, dates of enrollment, the dates on which the Continuing Services were provided, and current enrollment status;

2. Costs incurred, by MID, including dates of service; and

3. Such other information as may be required pursuant to any EOHHS request for information.

E. The reconciliation payment procedures may include an audit, to be performed by EOHHS or its authorized agent, to verify all claims for the Covered Individuals by the Contractor. The findings of such audit shall determine the amount, if any, that the Contractor shall be reimbursed by EOHHS. If an audit is not conducted, EOHHS shall reimburse the Contractor as otherwise provided herein.

Section 4.5 In-State Acute Hospital Add-on/Pursuant to Section 2.7.F.3.n

A. At a frequency to be specified by EOHHS, EOHHS shall pay the Contractor an amount equal to the sum of provider payments described in **Section 2.7.F.3.n** for the applicable time period.

B. For each Contract Year, EOHHS shall perform an annual reconciliation after the end of the Contract Year, of the directed payments described in **Section 2.7.F.3.n**. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies. The Contractor shall remit to EOHHS the full amount of any overpayments identified by EOHHS. Such payments shall be made either through a check or, at the discretion of EOHHS, through recoupment from future capitation and/or reconciliation payments described in **Section 4.5**.

Section 4.6 Performance Incentive Arrangements

A. EOHHS may establish annual performance standards and financial sanctions or incentive arrangements in **Appendix G** for the Contractor related to its performance of Contractor responsibilities. EOHHS shall determine whether the Contractor has met, exceeded, or fallen below any and all such performance standards and shall provide the Contractor with written notice of such determinations.

B. In no case shall total payments to the Contractor exceed 105% of the Contractor-specific Capitation payments, as determined by EOHHS.

C. All Performance Incentive arrangements shall meet the following requirements:

1. Performance Incentives shall be for a fixed period of time, which shall be described in the specific Performance Incentive;

2. No Performance Incentive shall be renewed automatically;

3. All Performance Incentives shall be made available to both public and private contractors;

4. No Performance Incentive shall be conditioned on intergovernmental transfer agreements;

5. All Performance Incentives shall be necessary for the specified activities, targets, and performance measures or quality-based outcomes that support program initiatives as specified by the state's quality strategy under 42 CFR 438.340; and

6. The Contractor's performance under any Performance Incentive shall be measured during the Contract Year in which the Performance Incentive is effective.

D. Finders' Fee Performance Incentive

If, as further described in **Section 2.3.D.3.e.ii**, EOHHS determines the Contractor meets the requirements to receive a finders' fee performance incentive, the amount of the incentive payment shall be equal to 50% of the Contractor's pro rata amount of the net state share of the total settlement or verdict amount, based on the Contractor's percentage of the single damages from covered conduct over the relevant time period as determined by EOHHS. The net state share is the gross amount of the verdict or settlement minus any amounts owed as a repayment of federal financial participation to the federal government or other restitution called for in the verdict or settlement.

E. Quality and Incentive Arrangement

1. EOHHS shall pay the Contractor a payment based on the Contractor's Quality Score as set forth in **Appendix G**. For Contract Year 2023 - 2024, such payment shall equal no more than $1,500,000. Starting in Contract Year 2025, and for each subsequent Contract Year:

   a. Such payment shall not exceed 0.75 percent of total capitation revenue; and

   b. The total amount of the Quality Incentive Program referenced in this section and the Quality and Equity Incentive Program referenced in **Appendix G** shall not exceed the amount stipulated in **Appendix H-1**.

2. The Contractor shall make all appropriate efforts to meet a set of performance targets for individual Quality Measures as set forth in **Appendix G**.

3. EOHHS shall calculate, annually, the Contractor's Quality Score based on the Contractor's performance with respect to the Quality Measures set forth in **Appendix G**.

   a. Such score shall be based on the Contractor's meeting or improvement towards meeting the targets and a statewide performance metric, as further specified by EOHHS and as set forth in **Appendix G**.

   b. Such score shall be a number between zero (0) and one (1).

4. For such calculations described above, EOHHS shall use data reported by the Contractor, or other data as further specified by EOHHS.

5. Based on the Contractor's performance, EOHHS shall pay the Contractor in accordance with **Section 4.6.A**.

F. Quality and Equity Incentive Program Arrangement

EOHHS shall pay the Contractor a payment based on the Contractor's Health Equity Score set forth in **Appendix G**. Such payment shall equal no more than 0.75 percent of total capitation.

1. The Contractor shall make all appropriate efforts to meet a set of performance targets for individual Health Equity measures as set forth in Appendix G.

2. EOHHS shall calculate, annually, the Contractor's Health Equity Score based on the Contractor's performance with respect to the Health Equity measures set forth in Appendix G. This calculation will consider:

   a. Collection of complete and accurate self-reported social risk factor data for its Covered Individuals, which may include race, ethnicity, language, disability status, sexual orientation, and gender identity;

   b. Identification and monitoring of health care inequities through stratified reporting of performance metrics as further specified by EOHHS; and

   c. Reduction of identified disparities through targeted and evidence-based interventions as demonstrated through performance metrics as further specified by EOHHS.

   d. Such scores shall be a number between zero (0) and one hundred (100).

3. For calculations described above, EOHHS shall use data reported by the Contractor or other data as further specified by the EOHHS.

4. Based on the Contractor's performance, EOHHS shall pay the Contractor in accordance with Section 4.6.A.

Section 4.7 Risk-Sharing Arrangements

A. General Provisions

1. There may be distinct financial risk-sharing arrangements for the Behavioral Health Covered Services Component of the Capitation Rates paid for under the Rates for RC I excluding Children under 21 with TPL; RC I Children under 21 with TPL only; RC II excluding Children under 21 with TPL; RC II Children under 21 with TPL only; and RC IX and RC X, as applicable, as set forth in **Appendix H-1**.

2. The arrangement described in this **Section 4.6** may result in payment by the Contractor to EOHHS or by EOHHS to the Contractor.

3. All payments to be made by the Contractor to EOHHS or by EOHHS to the Contractor shall be calculated and determined by EOHHS based on the

Contractor's expenditures related to Covered Individuals, as determined by EOHHS.

4. The Contractor's Behavioral Health Covered Services Capitation Rate revenue shall mean the sum of the applicable 12 Actual Monthly Behavioral Health Covered Services Capitation Rate payments for the Contract Year, as determined in accordance with **Section 4.2.A**. This calculation shall be used to determine the Contractor's revenue for the Behavioral Health Covered Services Capitation Rate.

5. By 210 days after the end of each Contract Year, the Contractor shall provide EOHHS with a report of actual expenditures for all of the services included in the Behavioral Health Covered Services Capitation Rate, subtracting any TPL recoveries retained by the Contractor pursuant to **Section 2.18**. The report of expenditures shall be based on all Claims paid through no fewer than 180 days, including the Contractor's best estimate of Claims incurred but not reported (IBNR) and any applicable IBNR completion factor reported to EOHHS with the IBNR methodology report (see **Appendix E-1**). In the event that the above final report of actual expenditures includes an IBNR completion factor greater than 1 percent for total BH Covered Services, EOHHS reserves the right to conduct an audit of the Contractor's IBNR methodology.

6. EOHHS shall in its sole discretion make the final determination of IBNR, using the Contractor's report of actual expenditures to inform that determination.

7. EOHHS shall compare the actual PMPM Behavioral Health Covered Services Capitation Rate payments for the Contract Year to the Contractor's actual expenditures. Based on such comparison, and calculating any difference, EOHHS shall determine in accordance with **Section 4.4** whether overpayments or underpayments were made to the Contractor.

    a. If underpayments were made, EOHHS shall pay the Contractor a final payment for the preceding Contract Year in accordance with the methodology.

    b. If overpayments were made the Contractor shall pay EOHHS a final payment for the preceding Contract Year in accordance with the methodology.

8. Notwithstanding the generality of the foregoing, if EOHHS determines that risk sharing arrangements result in payments that exceed the approved capitation rates and the excess payments exceed that total amount MassHealth would have paid on a fee for service basis for the BH Covered Services actually furnished to Covered Individuals, EOHHS may re-price any or all of the Contractor's paid Claims so that the total final payments to the Contractor based on risk sharing arrangements do not exceed the amount MassHealth would have paid for the actual services provided to Covered Individuals on a Fee-For-Service basis.

B. Primary Care ACO

1. There may be distinct risk-sharing arrangements for the services delivered to a Covered Individual enrolled in a Primary Care ACO as set forth in **Appendix H-1**.

2. The arrangement described in this Section may result in payment by the Contractor to EOHHS or by EOHHS to the Contractor.

3. All payments to be made by the Contractor to EOHHS or by EOHHS to the Contractor shall be calculated and determined by EOHHS based on the Contractor's expenditures related to Covered Individuals enrolled in a Primary Care ACO, as determined by EOHHS.

Section 4.8 Reinsurance

The Contractor may purchase reinsurance from a company authorized to do business in Massachusetts, to cover medical costs that exceed a threshold per Covered Individual for all rating categories for the duration of the Contract period. Such reinsurance policy is not required and is at the Contractor's discretion.

Section 4.9 Option to Audit

EOHHS, or its authorized agent, may perform an audit to verify any claims data submitted by the Contractor. The findings of such audit shall determine the amount, if any, that the Contractor shall be reimbursed or that EOHHS shall recover from the Contractor. If an audit is not conducted, EOHHS shall, within a reasonable time after receipt of claims data from the Contractor and in accordance with any applicable timeframe described in the Contract, reimburse to the Contractor or recover from the Contractor as provided in the reconciliation processes described in this **Section 4**.

Section 4.10 Behavioral Health Quality Incentive Payment

A. At a frequency to be specified by EOHHS, EOHHS shall pay the Contractor an amount equal to the sum of the provider payments described in **Section 4.10** for the applicable time period.

B. For each Contract Year, EOHHS shall perform an annual reconciliation after the end of the Contract Year to correct the amount of payments described in **Section 2.7.F.4**. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies.

Section 4.11 Clinical Quality Incentive for Acute Hospitals

A. At a frequency to be specified by EOHHS, EOHHS shall pay the Contractor an amount equal to the sum of the provider payments described in **Section 2.7.F.5** for the applicable time period.

B. For the performance period, EOHHS shall perform a reconciliation after the end of the performance period to correct the amount of payments described in **Section 2.7.F.5**. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies.

Section 4.12 Community Behavioral Health Incentive Program

A. At a frequency to be specified by EOHHS, EOHHS shall pay the Contractor an amount equal to the sum of provider payments described in **Section 2.8.F.10** for the applicable time period.

B. For each Contract Year, EOHHS shall perform an annual reconciliation to correct the amount of payments described in **Section 2.8.F.10**. EOHHS shall remit to the Contractor the full amount of any underpayments it identifies.

Section 5. ADDITIONAL TERMS AND CONDITIONS

Section 5.1 Administration

A. Notification of Administrative Changes

The Contractor shall notify EOHHS in writing of all changes affecting the delivery of care, the administration of its program, or its performance of Contract requirements. The Contractor shall notify EOHHS in writing no later than 60 days prior to any material change to the manner in which services are rendered to Covered Individuals, including but not limited to reprocurement or termination of a Material Subcontractor. The Contractor shall notify EOHHS in writing, of all other changes no later than five business days prior to the effective date of such change. The Contractor shall notify EOHHS in writing no later than 90 days prior to the effective date of any material administrative and operational change with respect to the Contractor**,** including but not limited to a change to the Contractor's corporate structure, ownership, or tax identification number.

B. Assignment or Transfer

The Contractor shall not assign or transfer any right or interest in this Contract to any successor entity or other entity, including any entity that results from a merger of the Contractor and another entity, without the prior written consent of EOHHS. The Contractor shall include in such request for approval a detailed plan for EOHHS to review. The purpose of the plan review is to ensure uninterrupted services to Covered Individuals, evaluate the new entity's ability to support the Provider Network, ensure that services to Covered Individuals are not diminished and that major components of the organization and EOHHS programs are not adversely affected by the assignment or transfer of this Contract.

C. Independent Contractors

The Contractor shall ensure that its employees, subcontractors, and any other of its agents in the performance of the Contract act in an independent capacity, and not as officers or employees of EOHHS or the Commonwealth of Massachusetts.

D. Subrogation

Subject to EOHHS's lien and third party recovery rights, the Contractor shall:

1. Be subrogated and succeed to any right of recovery of a Covered Individual against any person or organization, for any services, supplies, or both provided under this Contract up to the amount of the benefits provided hereunder; and

2. Require that the Covered Individual pay to the Contractor all such amounts recovered by suit, settlement, or otherwise from any third person or his or her insurer to the extent of the benefits provided hereunder, up to the value of the benefits provided hereunder, pursuant to the third-party liability benefit

coordination plan to be implemented under the provisions of **Section 2.18**. The Contractor may ask the Covered Individual:

a. To take such action, furnish such information and assistance, and execute such instruments as the Contractor may require to facilitate enforcement of its rights hereunder, and to take no action prejudicing the rights and interest of the Contractor hereunder; and

b. To notify the Contractor hereunder and to authorize the Contractor to make such investigations and take such action as the Contractor may deem appropriate to protect its rights hereunder whether or not such notice is given.

E. Advance Directives

The Contractor shall comply with (1) the requirements of 42 CFR Part 489, Subpart I and 42 CFR 422.128, relating to the maintenance of written policies and procedures regarding advance directives; and (2) the requirements of 130 CMR 450.112 and 42 CFR 438.3(j). The Contractor shall provide adult Enrollees with written information on advance directives policies, including a description of applicable state law. The information must reflect changes in State law as soon as possible, but no later than 90 days after the effective date of the change.

F. Compliance with Certification, Program Integrity and Prohibited Affiliation Requirements

As a condition of receiving payment under this Contract, the Contractor must comply with all applicable certification, program integrity and prohibited affiliation requirements at 42 CFR 438.600 et seq., and as described in this Contract**.**

G. Prohibited Affiliations and Exclusion of Entities

1. In accordance with 42 U.S.C. § 1396u-2(d)(1) and 42 CFR 438.610, the Contractor shall not knowingly have an employment, consulting, provider, subcontractor, or other agreement for the provision of items and services that are significant and material to the Contractor's obligations under the Contract with any person, or affiliate of such person, who is debarred, suspended or otherwise excluded from certain procurement and non-procurement activities, under federal or state law, regulation, executive order or guidelines. Further, no such person may have beneficial ownership of more than five percent of the Contractor's equity nor be permitted to serve as a director, officer, or partner of the Contractor. The Contractor shall provide written disclosure to EOHHS of any prohibited affiliations identified by the Contractor.

2. The Contractor shall be excluded from participating in MassHealth if it meets any of the conditions set forth in 42 CFR 438.808(b).

H. Subcapitation and Physician Incentive Plans

1. The Contractor may, subject to EOHHS's prior review and approval and all applicable state and federal rules and regulations, including but not limited to the provisions of 42 CFR 438.3(i), 42 CFR 422.208 and 422.210, negotiate and enter into arrangements to pay Network Providers on a subcapitated basis or operate a physician incentive plan.

2. The Contractor shall not engage in risk-sharing payment methodologies (i.e., non-Fee-for-Service arrangements) with its Network Providers without first submitting the proposed payment methodology to EOHHS for review and approval. Any Network Provider payment methodology that the Contractor proposes to EOHHS must satisfy the following minimum requirements:

   a. Balance cost incentives with access and quality incentives; and

   b. Ensure that those Network Providers for whom the Contractor proposes to use such payment methodologies are able to demonstrate the managerial, operational and financial capability to manage the proposed risk arrangement.

3. The Contractor shall comply, and shall ensure that its subcontractors comply, with all applicable requirements governing subcapitation arrangements and physician incentive plans. In accordance with the requirements of 42 U.S.C. § 1396b(m)(2)(A)(x), 42 CFR Parts 417, 422, 434, 438, and 1003, the Contractor shall ensure that:

   a. No specific payment is made directly or indirectly to a Provider, physician, or physician group as an inducement to reduce or limit Medically Necessary services furnished to a Covered Individual; and

   b. The applicable stop-loss protection, Covered Individual survey, and disclosure requirements of 42 CFR Part 417 are met.

4. Provider Incentive Plans

   a. Incentive payment contracts between the Contractor and Network Providers shall:

      1) Have a defined performance period that can be tied to the applicable MLR reporting periods;

      2) Be signed and dated by all appropriate parties before the commencement of the applicable performance period;

      3) Include clearly-defined, objectively measurable, and well-documented clinical or quality improvement standards that the Network Provider must meet to receive the incentive payment; and

4) Specify a dollar amount or a percentage of a verifiable dollar amount that can be clearly linked to successful completion of the metrics defined in the incentive payment contract, including a date of payment

b. The Contractor shall:

1) As directed by EOHHS, maintain documentation to support the provider incentive payments;

2) Not use attestations as supporting documentation for data that factor into the MLR calculation; and

3) Make incentive payment contracts, and any documentation required under this section, available to EOHHS upon request.

I. National Provider Identifier

The Contractor shall require each Provider providing Covered Services to Covered Individuals under this Contract to have a unique identifier in accordance with the system established under 42 U.S.C. §1320d-2(b). The Contractor shall provide such unique identifier to EOHHS for each of its Providers in the format and time frame established by EOHHS.

J. Provider-Covered Individual Communications

1. In accordance with 42 USC 1396u-2(b)(3) and 42 CFR 438.102, the Contractor may not prohibit, or otherwise restrict, a health care professional acting within the lawful scope of practice, from advising or advocating on behalf of a Covered Individual who is his or her patient, for the following:

a. The Covered Individual's health status, medical care, or treatment options, including any alternative treatment that may be self-administered;

b. Any information the Covered Individual needs in order to decide among all relevant treatment options;

c. The risks, benefits, and consequences of treatment or non-treatment; and

d. The Covered Individual's right to participate in decisions regarding his or her health care, including the right to refuse treatment, and to express preferences about future treatment decisions.

2. Notwithstanding the provisions of **Section 5.1.J.1** above, and subject to the requirements set forth below, the Contractor is not required to provide, reimburse for, or provide coverage of, a counseling or referral service if the Contractor objects to the service on moral or religious grounds. The Contractor must furnish information about any service the Contractor does not cover due to moral or religious grounds as follows.

a. EOHHS:

1) With its application for a Medicaid contract; and

2) At least 60 days prior to adopting the policy during the term of the Contract.

b. To Potential Covered Individuals, via enrollment/Marketing materials, at least 30 days prior to adopting the policy during the term of the Contract.

c. To Covered Individuals, at least 30 days prior to adopting the policy during the term of the Contract and in the Covered Individual handbook. The Contractor shall also describe in the Covered Individual handbook that the Covered Individual may access such services by contacting MassHealth directly and provide contact information.

3. The Contractor shall accept a reduction in the Capitation Rate for any service it does not provide, reimburse for, or provide coverage of due to moral or religious grounds.

K. Covered Individuals - No Liability for Payment

1. The Contractor shall:

a. Ensure, in accordance with 42 USC §1396 u-2(b)(6) and 42 CFR 438.106, that a Covered Individual will not be held liable:

1) For debts of the Contractor, in the event of the Contractor's insolvency;

2) For services (other than Excluded Services) provided to the Covered Individual in the event that:

a) The Contractor fails to receive payment from EOHHS for such services; or

b) A Provider fails to receive payment from EOHHS or the Contractor for such services, including but not limited to payments that are in excess of the amount the covered individual would owe if the Contractor covered the service directly.

b. Not charge Covered Individuals coinsurance, co-payments, deductibles, financial penalties or any other amount in full or part, for any service provided under this Contract.

c. Not deny any service provided under this Contract to a Covered Individual who, prior to becoming MassHealth eligible, incurred a debt that has not been paid.

d. Ensure Provider compliance with all Covered Individual payment restrictions, including balance billing and co-payment provisions, and develop and implement a plan to sanction any Provider that does not comply with such provisions.

e. Return to the Covered Individual the amount of any liability inappropriately imposed on and paid by the Covered Individual.

L. Covered Individual Rights

1. The Contractor must have written policies regarding Covered Individual rights and must comply with any applicable federal and state laws that pertain to Covered Individual rights;

2. The Contractor must ensure that its staff and affiliated Providers take those rights into account when furnishing services to Covered Individuals;

3. Covered Individual rights shall include:

a. The right to receive the information required pursuant to this Contract;

b. The right to be treated with respect and with due consideration for his or her dignity and privacy;

c. The right to receive information on available treatment options and alternatives, presented in a manner appropriate to the Covered Individual's condition and ability to understand;

d. The right to receive a second opinion on a medical procedure and have the Contractor pay for such second opinion consultation visit;

e. The right to participate in decisions regarding his or her health care, including the right to refuse treatment;

f. The right to be free from any form of restraint or seclusion used as a means of coercion, discipline, convenience or retaliation;

g. The right to freely exercise his or her rights without adversely affecting the way the Contractor and its Providers treat the Covered Individual;

h. The right to request and receive a copy of his or her medical records and request that they be amended or corrected, as specified in 45 CFR 164.524 and 164.526; and

i. The right to be furnished ACO Covered Services in accordance with this Contract.

M. Coverage of Emergency, Screening and Post-Stabilization Services

1. The Contractor must cover and pay for Behavioral Health Covered Services for treatment of a Behavioral Health Emergency medical condition in accordance with 42 CFR 438.114 and M.G.L. c. 118E, § 17A.

2. The Contractor must cover and pay for Behavioral Health Covered Services for treatment of a Behavioral Health Emergency medical condition regardless of whether the Provider that furnishes the services has a contract with the Contractor.

3. The Contractor may not deny payment for Behavioral Health Covered Services for treatment of a Behavioral Health Emergency medical condition, including cases in which the absence of immediate medical attention would not have:

    a. placed the health of the individual (or, with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy;

    b. resulted in serious impairment to bodily functions; or

    c. resulted in serious dysfunction of any bodily organ or part.

4. The Contractor may not deny payment for Behavioral Health Covered Services for treatment of a Behavioral Health Emergency medical condition if a representative of the Contractor instructed the Covered Individual to seek Emergency services.

5. The Contractor may not limit what constitutes a Behavioral Health Emergency medical condition on the basis of lists of diagnoses or symptoms;

6. The Contractor may require Network Providers to notify the Covered Individual's PCC of the Covered Individual's screening and treatment, but may not refuse to cover MassHealth Behavioral Health Covered Services for treatment of a Behavioral Health Emergency medical condition based on their failure to do so;

7. A Covered Individual who has an Emergency medical condition may not be held liable for payment of subsequent screening and treatment needed to diagnose the specific condition or stabilize the patient;

8. The attending emergency physician, or the Provider actually treating the Covered Individual, is responsible for transfer or discharge, and that determination is binding on the Contractor, if such transfer or discharge order:

    a. is consistent with generally accepted principles of professional medical practice; and

    b. is a covered benefit under the Contract.

9. The Contractor shall cover and pay for Post-stabilization Care Services that are MassHealth Covered Services in accordance with 42 CFR 438.114, 42 CFR 422.113(c), and M.G.L. c. 118E, § 17A.

N. Restraint and Seclusion

The Contractor shall require any Provider that is a psychiatric residential treatment facility providing inpatient psychiatric services to individuals under age 21, to comply with all requirements relating to restraint and seclusion as set forth in 42 CFR 441.151 subpart D, and 42 CFR 483 subpart G and in **DMH's Human Rights and Restraint and Seclusion Policy**.

O. Disclosure Requirements

1. Except as otherwise provided elsewhere in this Contract, the Contractor shall within two business days disclose to EOHHS any known non-compliance by the Contractor with any provision of this Contract, or any state or federal law or regulation governing this Contract.

2. The Contractor shall make the following federally required disclosures in accordance with 42. CFR § 455.100-106, 42 CFR 455.436, 42 CFR 1002.3. and 42 U.S.C. § 1396b(m)(4) in the form and format specified by EOHHS, at any time upon a written request by EOHHS, and as follows:

a. Ownership and Control

Upon execution, renewal or extension of this Contract and within 35 days of any change in ownership, the Contractor shall furnish full and complete information to EOHHS as required by 42 CFR 455.104 regarding ownership and control, with respect to both the Contractor and Material Subcontractors.

b. Business Transactions

Pursuant to 42 CFR 455.105, within 35 days of a written request by EOHHS and/or the U.S. Department of Health and Human Services, the Contractor shall furnish full and complete information to the requester regarding business transactions.

c. Criminal Convictions

Pursuant to 42 CFR 455.106, upon any renewal or extension of this Contract and at any time upon a written request by EOHHS, the Contractor shall furnish full and complete information to EOHHS regarding persons convicted of crimes.

d. Other Disclosures

The Contractor shall comply with all reporting and disclosure requirements of 42 USC § 1396b(m)(4)(A) if the Contractor is not a federally qualified health maintenance organization under the Public Health Service Act. Pursuant to 42 U.S.C. § 1396b(m)(4)(B), the

Contractor shall make any information reported pursuant to 42 U.S.C. § 1396b(m)(4)(A) available to Covered Individuals upon reasonable request.

3. The Contractor shall ensure that its Network Provider enrollment forms require Provider applicants to disclose complete ownership, control, and relationship information, and that Network Applicants and Network Providers fully and accurately complete the required portions of the EOHHS form developed for such purpose. Further, the Contractor shall require persons with an ownership or control interest, or persons who are agents or managing employees of Network Providers, to utilize the EOHHS form developed for such purpose to fully and accurately disclose health care-related criminal convictions, and to notify EOHHS of such disclosures within 20 working days.

4. Unless otherwise instructed by EOHHS, for the purposes of making the disclosures to EOHHS set forth in **Section 5.1.O**, the Contractor shall fully and accurately complete the EOHHS form developed for such purpose, attached hereto as **Appendix B-3**. EOHHS may update or replace this Appendix without the need for a Contract amendment.

5. The Contractor shall search the federal HHS-OIG's List of Excluded Individuals/Entities (LEIE) and the System Award Management website for the names of Network providers upon enrollment, reenrollment, credentialing or re-credentialing, as further described in **Section 2.8.H**. In addition, the Contractor shall conduct such searches for the names of Network providers, persons with ownership or control interest in the Contractor, and agents or managing employees of the Contractor at least monthly to ensure that EOHHS does not pay for services provided by excluded persons or entities.

6. EOHHS may immediately terminate this Contract in whole or in part if the Contractor fails to comply with this **Section 5.1** or in response to the information contained in the Contractor's disclosures under this **Section 5.1**. In addition, the Contractor shall not be entitled to payment for any MassHealth services for which EOHHS determines federal reimbursement is not available. Any such payments shall constitute an overpayment as defined in 130 CMR 450.235. Under such circumstances, EOHHS may also exercise its authority under 130 CMR 450.238, et seq. to impose sanctions.

Section 5.2 Data Privacy and Security (including Health Insurance Portability and Accountability Act (HIPAA))

A. The Contractor shall be required to comply with M.G.L. c. 66A, M.G.L. c. 93H, the Health Insurance Portability and Accountability Act ("HIPAA") privacy and security regulations at 45 CFR Parts 160, 162 and 164 (the "HIPAA Rules"), as applicable to a business associate (as such term is used therein), Commonwealth Security Policies issued by the Executive Office of Technology Services and Security and any other applicable

laws, regulations, policies, and procedures pertaining to the privacy or security of confidential information that is used, accessed, received, created, maintained, disclosed, transmitted or otherwise obtained by such Contractor or its agents or subcontractors in the course of providing the services described herein, and the Contractor shall be required to enter into any contract or agreement deemed necessary or appropriate by EOHHS to comply with such obligations. For purposes of the foregoing, "confidential information" includes personal data (as such term is used in M.G.L. 66A), personal information (as such term is used in M.G.L. 93H), protected health information (as such term is used in the HIPAA Rules), EOHHS security procedures, business operations information, proprietary information or other information treated that is treated as confidential under applicable law, regulation, policy or contract. Further, EOHHS reserves the right to add any requirement during the course of the Contract that it determines it must include in the contract in order for the department to comply with the HIPAA Rules, M.G.L. c. 66A, 801 CMR 3.00, M.G.L. c. 93H, 201 CMR 17, 42 CFR Part 431, Subpart F, 42 CFR Part 2, 45 CFR §155.260 and other applicable laws, regulations, and policies.

B. Covered Entities

EOHHS and the Contractor acknowledge that they are covered entities, as defined at 45 CFR 160.103.

C. Statutory Requirements

The Contractor shall comply with all applicable requirements regarding the privacy, security, use and disclosure of personal data (including protected health information, such as medical records and any other health and enrollment information), including, but not limited to, requirements set forth in M.G.L. c. 66A, 42 CFR 431, Subpart F, and 45 CFR Parts 160, 162 and 164.

D. Contractor's Compliance with HIPAA

The Contractor represents and warrants that:

1. It shall conform to the requirements of all applicable Health Insurance Portability and Accountability Act (HIPAA) requirements and regulations;

2. It shall work cooperatively with EOHHS on all activities related to ongoing compliance with HIPAA requirements, as directed by EOHHS; and

3. It shall execute, at EOHHS's direction, a Trading Partner Agreement and any other agreements EOHHS determines are necessary to comply with HIPAA requirements.

E. Research Data

The Contractor shall seek and obtain EOHHS prior written authorization for the use of any data pertaining to this Contract for research or any other purposes not directly related to the Contractor's performance under this Contract. EOHHS may approve or deny such data requests at its sole discretion. To obtain EOHHS authorization to access data for an activity that is not directly related to the performance of this Contract, the Contractor shall:

1. Submit to EOHHS, at the direction of and in a form and format specified by EOHHS, an application to participate in an external study and application for release of MassHealth data, as appropriate, for prior review and approval;
2. If approved by EOHHS, enter into the appropriate data use agreement as directed by EOHHS; and
3. Submit to EOHHS, prior to publication, the results of any external research projects for which the Contractor has received EOHHS approval to share MassHealth data.

F. Requesting Member-Level Data or Reports

If the Contractor wishes to receive member-level data or reports that may be available from EOHHS under the Contract, the Contractor may be required to submit a request to EOHHS and execute a data use agreement containing any representations and/or privacy and security requirements applicable to the data and/or report(s) that EOHHS may determine necessary or appropriate.

G. Business Associate Activities

The Contractor acknowledges and agrees that it is acting as EOHHS' Business Associate, as such term is defined under HIPAA, in providing services pursuant to **Sections 2.4.B, 2.4.C, 2.5, 2.6.D.2, 2.7.H, 2.7.J, 2.7P, 2.10, 2.11, 2.14.I, 2.19, and 2.13** (to the extent that **Section 2.13** activities involve functions performed by the Contractor on EOHHS' behalf) and such additional Sections of the Contract as EOHHS shall identify in the Contract or shall identify in either written amendments to the Contract or written work plans or instructions during the course of the Contract (such services, "Business Associate Activities").

With respect to these Business Associate Activities, the Contractor agrees to protect information received in connection with its provision of these services under this Contract, including PI, pursuant to applicable federal and state laws, EOHHS agreements, and policies, including, but not limited to, M.G.L. c. 66A, 801 CMR 3.00, M.G.L. c. 93H, 201 CMR 17, the HIPAA Rules (inclusive of 45 CFR §§ 160, 162, and 164), 42 CFR Part 431, Subpart F, 42 CFR Part 2, 45 CFR §155.260 as further described in the Data Management and Confidentiality Agreement (DMCA), attached hereto in **Appendix K** and incorporated herein.

For the avoidance of doubt, the Contractor's obligations with respect to the Business Associate Activities are in addition to those outlined in this **Section 5.2**, which stem from its status as a Covered Entity under HIPAA.

H. EOHHS reserves the right to add any requirement during the course of the Contract that it reasonably determines it must include in the Contract in order for EOHHS to comply with any applicable state or federal law or regulation, or any contractual obligation to which EOHHS is subject, relating to privacy and/or security, including but not limited to the Privacy and Security Rules, and the Contractor shall promptly execute and comply with any amendment to the Contract that EOHHS deems necessary or appropriate in connection therewith.

I. Security Controls Compliance and Audit Tasks

1. As of the effective date of the contract, the Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PI, and that prevent use or disclosure of such PI, other than as provided for by this Agreement. Such safeguards shall be consistent with state and federal laws applicable to the privacy and security of personal and other confidential information, related requirements, including a HIPAA, MGL 66A (FIPA), 42 CFR 431, Subpart F, 42 CFR Part 2 ("Standards").

   a. In the event the Contractor is unable to fully comply with the Standards on the effective date, Contractor must submit to EOHHS a gap analysis detailing with which parts of the Standards the Contractor is unable to comply and a Plan of Actions and Milestones ("POAM"), providing an overview of the reasonable effort and time required to comply with the Standards.

      1) The gap analysis should identify, at a high-level:

         a) which of the Standards' controls Contractor believes they do not comply with; and

         b) how the Contractor is non-compliant.

      2) The POAM must, at a minimum, describe:

         a) which of the Standards' controls Contractor believes they do not comply with;

         b) how the Contractor is non-compliant;

         c) why the Contractor believes they are non-compliant;

d) a ranking of the severity of each gap to Contractor's ability to protect the confidentiality, integrity, or availability per the rating scheme outlined in the Standards; and

e) a status as of the date of submission of the POAM of remediation efforts for the gaps and/or an explanation of compensating controls or workarounds for the gap that in the Contractor's opinion lessen or eliminate the severity of the gap.

3) EOHHS may review the gap analysis and POAM with the Contractor and will provide a timeline for implementation of the Standards and/or correction of any deficiencies that are in EOHHS' opinion material that is mutually acceptable to the parties ("Implementation Timeline"). The POAM will be updated to include the agreed-upon Implementation Timeline. EOHHS may meet with Contractor from time to time and/or as deadlines to correct deficiencies approach and/or come due and review the POAM, Implementation Timeline, and any other documentation requested by EOHHS with Contractor to determine Contractor's compliance with such documents and assess what further actions need to be taken.

b. On an annual basis, Contractor must internally review their compliance with the Standards and submit an updated POAM to EOHHS pursuant to the process outlined in **Section 5.2.I.1.A**.

c. Contractor understands that it is solely responsible for meeting the Standards and for managing its information security program. EOHHS's review of the gap analysis and/or POAM, or any other discussions of or related to the gap analysis and/or POAM, shall not constitute approval by EOHHS of their contents and will not otherwise operate to indemnify, remove liability, or otherwise absolve Contractor of any responsibility for non-compliance with the Standards.

d. In the event Contractor is unable to fully comply with the Standards by the Effective Date, Contractor shall prioritize (in no particular order) implementation of Standards controls dealing with computer access authentication, data encryption, mobile device encryption, physical access controls, appropriate employee training, and information flow identification and enforcement.

e. If Contractor hosts any Commonwealth Data or other data on behalf of EOHHS ("Hosted Data"), in addition to the foregoing security requirements, as of the Effective Date, Contractor must either be capable of providing or have subcontracted with a hosting company to provide a

server environment has received a FEDRAMP Authorization to Operate at the Moderate level (the "Hosting Standards"). Contractor must ensure that all Hosted Data is located within the continental United States. Additionally, Contractor must ensure that it and/or EOHHS have at least logical control over Hosted Data.

2. Once every three years, starting on the third year after the Effective Date, and at no additional cost to EOHHS, Contractor shall engage an independent third-party auditor to conduct an audit of Contractor's compliance with the Standards and Hosting Standards. Such audit shall include, but not be limited to, an audit of the Contractor's facilities where work is performed on behalf of EOHHS and its hosting facilities where Hosted Data resides. At the conclusion of such audit, the Contractor shall provide EOHHS with the audit results and findings.

    a. At EOHHS's option and cost, EOHHS may enlist their own independent third-party auditor to conduct such audits. Contractor must permit auditor access to its facilities and must cooperate with the auditor to ensure successful completion of the audit.

    b. In the event the results of the third-party audit demonstrate that Contractor does not fully comply with the Standards or the Hosting Standards, Contractor must submit an updated POAM pursuant to the process outlined in **Section 5.2.I.1.A** that includes and addresses such deficiencies.

3. On at least an annual basis and at no additional cost to EOHHS, Contractor shall conduct a vulnerability assessment of Contractor's computing and hosting environments with respect to the services provided under this Contract. Such vulnerability assessment shall include a penetration test, using industry-standard methodology, of Contractor's computing environment. Contractor must provide EOHHS the findings of the vulnerability assessment and penetration test. If the findings demonstrate security vulnerabilities in Contractor's computing environment, Contractor must submit an updated POAM pursuant to the process outlined in **Section 5.2.I.1.A** that addresses such deficiencies.

4. Notwithstanding the foregoing, nothing contained in this **Section 5.2.I** shall abrogate or restrict EOHHS' ability to audit and inspect Contractor's facility, hosting facility or books and records, including but not limited to Contractor's Information Security Plan, business continuity plan, disaster recovery plan, or other documentation required to be maintained pursuant to the Standards and Hosting Standards or otherwise in this Contract. Such audit and/or inspection shall be conducted with reasonable notice and during Contractor's standard business hours.

5. In the event EOHHS is assessed any fine, penalty, or monetary damages as a result of a finding or judgment based in whole or in part on Contractor's non-compliance with the Standards, inability to meet any part of the Implementation

Timeline, inability to abide by the POAM, or any misstatements or omissions in the POAM (collectively "Liabilities"), Contractor will indemnify EOHHS for any such Liabilities and EOHHS will be entitled to reimbursement from the Contractor for any such Liabilities. If, in EOHHS' determination, Contractor demonstrates an inability to meet any part of the Implementation Timeline, inability to abide by the POAM, or any misstatements or omissions in the POAM (including material divergence between the POAM representations and the finding of an independent third party audit), EOHHS may pursue remedies specified elsewhere in this Contract including, but not limited to, seeking monetary damages and/or terminating the Contract in whole or in part.

J. Security Controls Compliance and Audit Deliverables

The Contractor shall deliver to the Commonwealth the following Deliverables subject to acceptance or rejection by EOHHS as described in the Agreement:

1. Gap analysis including at a minimum the following:
   a. A list of gaps (if any)
   b. The cause of those gaps
2. POAM including at a minimum the following:
   a. A list of gaps (if any)
   b. The cause of those gaps
   c. Why the Contractor believes those gaps exist
   d. A raking of the gap severity
   e. An ongoing and cumulative set of status updates for remediation and/or implementation of a compensating control or workaround
3. Information Security Standards including, at a minimum, the Contractor's information security standards generally applicable to the organization.
4. FEDRAMP ATO Documentation including at a minimum a demonstration that the hosting environment has a FEDRAMP Moderate ATO.
5. Third Party Audit Reports including at a minimum all reports generated for the Contractor that will demonstrate a generally effective control environment for the work performed for EOHHS.

Section 5.3 General Terms and Conditions

A. Compliance with Laws

1. The Contractor shall comply with all applicable statutes, orders, and regulations promulgated by any federal, state, municipal, or other governmental authority relating to the performance of this Contract as they become effective. Without limiting the generality of the foregoing, the Contractor shall comply, to the extent applicable, with Title VI of the Civil Rights Act of 1964, as implemented by regulations at 45 CFR Part 80; Title IX of the Education Amendments of 1972; the Age Discrimination Act of 1975, as implemented by regulations at 45 CFR Part 91; the Rehabilitation Act of 1973; the Americans with Disabilities Act; the Assisted Suicide Funding Restriction Act of 1997; Titles XIX and XXI of the Social Security Act and waivers thereof; Chapter 141 of the Acts of 2000 and applicable regulations; Chapter 58 of the Acts of 2006 and applicable regulations; 42 CFR Part 438; The Paul Wellstone and Pete Domenici Mental Health Parity and Addiction Equity Act of 2008 (commonly referred to as the Mental Health Parity Law) and applicable regulations; and relevant provisions of the Patient Protection and Affordable Care Act and Health Care and Education Reconciliation Act of 2010, including but not limited to Section 1557 of such Act, to the extent such provisions apply and other laws regarding privacy and confidentiality, and as applicable, the Clean Air Act, Federal Water Pollution Control Act, and the Byrd Anti-Lobbying Amendment, and, as applicable, the CMS Interoperability and Patient Access Final Rule (CMS 9115-F).

2. In accordance with 130 CMR 450.123(B), the Contractor shall review its administrative and other practices, including the administrative and other practices of any contracted Behavioral Health organization, for the prior calendar year for compliance with the relevant provisions of the federal Mental Health Parity Law, regulations and guidance and submit a certification to EOHHS in accordance with 130 CMR 450.123(B)(1)-(3) and any additional instructions provided by EOHHS.

3. The Contractor shall be liable for any and all loss of Federal Financial Participation (FFP) incurred by the Commonwealth that results from the Contractor's failure to comply with any requirement of federal law or regulation.

B. Loss of Licensure/Accreditation

The Contractor shall report to EOHHS if at any time during the Contract the Contractor or any of its providers or material subcontractor loses, or is at risk of losing, any applicable license, state approval or accreditation. Such loss may be grounds for termination of the Contract under the provisions of **Section 5.5**.

C. Indemnification

The Contractor shall indemnify and hold harmless EOHHS and the Commonwealth from and against any and all liability, loss, damage, costs, or expenses which EOHHS or the Commonwealth may sustain, incur, or be required to pay, arising out of or in connection with the Contractor's violation of any federal or state law or regulation or any negligent

action or inaction or willful misconduct of the Contractor, or any person employed by the Contractor, provided that:

1. The Contractor is notified of any claims made directly to EOHHS within a reasonable time from when EOHHS becomes aware of the claim; and

2. The Contractor is afforded an opportunity to participate in the defense of such claims.

D. Prohibition Against Discrimination

1. In accordance with 42 U.S.C. § 1396u-2(b)(7) and 42 CFR 438.12, the Contractor shall not discriminate with respect to participation, reimbursement, or indemnification as to any Network Provider who is acting within the scope of the Network Provider's license or certification under applicable state law, solely on the basis of such license or certification. If the Contractor declines to include individual or groups of Providers in its network, it must give the affected Providers written notice of the reasons for its decision. This Section shall not be construed to prohibit the Contractor from including Network Providers only to the extent necessary to meet the needs of Covered Individuals or from using different reimbursement for different Network Providers, or from establishing any measure designed to maintain quality and control costs consistent with the responsibilities of the Contractor.

2. In accordance with 42 U.S.C. § 1396u-2 and 42 CFR 438.3(d), M.G.L. c. 151B, § 4(10), and all other applicable state or federal laws and regulations, the Contractor shall not discriminate and will not use any policy or practice that has the effect of discriminating against a Member eligible to enroll in the Contractor's MassHealth plan on the basis of health status, need for health care, race, color, national origin, sex, sexual orientation, gender identity, or disability.

3. If a complaint or claim against the Contractor is presented to the MCAD, the Contractor shall cooperate with MCAD in the investigation and disposition of such complaint or claim.

E. Information Sharing

During the course of a Covered Individual's enrollment or upon transfer or termination of enrollment, whether voluntary or involuntary, and subject to all applicable federal and state laws, the Contractor shall arrange for the transfer, at no cost to EOHHS or the Covered Individual, of medical information regarding such Covered Individual to any subsequent provider of medical services to such Covered Individual, as may be requested by the Covered Individual or such provider or be directed by EOHHS, the Covered Individual, regulatory agencies of the Commonwealth, or the United States Government. With respect to Covered Individuals who are children in the care or custody of the Commonwealth, the Contractor shall provide, upon reasonable request of the state agency

with custody of the Covered Individual, a copy of said Enrollee's medical records and any care management documentation in a timely manner.

F. Other Contracts

Upon EOHHS request, the Contractor shall provide a complete list of any managed Behavioral Health care contracts it or its corporate parent or subsidiary holds within Massachusetts in addition to this Contract. EOHHS shall not disclose non-public information that the Contractor may consider proprietary, except as required by law.

Nothing contained in this Contract shall be construed to prevent the Contractor from operating other comprehensive health care plans or providing health care services to persons other than those covered hereunder. The Contractor shall also provide EOHHS with a complete list of such plans and services, upon request. EOHHS shall not disclose any non-public information which the Contractor may consider proprietary, except as required by law. Nothing in this Contract shall be construed to prevent EOHHS from contracting with other comprehensive health care plans, or any other provider.

G. Title and Intellectual Property Rights

1. Definition of Property

The term "Property" as used herein includes the following forms of property: (1) confidential, proprietary, and trade secret information; (2) trademarks, trade names, discoveries, inventions processes, methods and improvements, whether or not patentable or subject to copyright protection and whether or not reduced to tangible form or reduced to practice; and (3) works of authorship, wherein such forms of property are required by Contractor to develop, test, and install the any product to be developed that may consist of computer programs (in object and source code form), scripts, data, documentation, text, photographs, video, pictures, sound recordings, training materials, images, techniques, methods, program images, text visible on the Internet, illustrations, graphics, pages, storyboards, writings, drawings, sketches, models, samples, data, other technical or business information, reports, and other works of authorship fixed in any tangible medium.

2. Contractor Property and License

Contractor will retain all right, title and interest in and to all Property developed by it, i) for clients other than the Commonwealth, and ii) for internal purposes and not yet delivered to any client, including all copyright, patent, trade secret, trademark and other intellectual property rights created by Contractor in connection with such work (hereinafter the "Contractor Property"). EOHHS acknowledges that its possession, installation or use of Contractor Property will not transfer to it any title to such property. "Contractor Property" also includes Contractor's proprietary tools, methodologies and materials developed prior to the performance of Services and used by Contractor in the performance of its

business and specifically set forth in this Contract and which do not contain, and are not derived from, EOHHS's Confidential Information, EOHHS's Property or the Commonwealth Data.

Except as expressly authorized herein, EOHHS will not copy, modify, distribute or transfer by any means, display, sublicense, rent, reverse engineer, decompile or disassemble Contractor Property.

Contractor grants to EOHHS, a fully-paid, royalty-free, non-exclusive, non-transferable, worldwide, irrevocable, perpetual, assignable license to the Contractor Property to make, have made, use, reproduce, distribute, modify, publicly display, publicly perform, digitally perform, transmit, copy, sublicense to any EOHHS subcontractor for purposes of creating, implementing, maintaining or enhancing a Deliverable, and create derivative works based upon Contractor Property, in any media now known or hereafter known, only to the extent the Contractor Property is embodied in the Deliverables, or otherwise required to exploit the Deliverables. During the Term of this Agreement and immediately upon any expiration or termination thereof for any reason, Contractor will provide to EOHHS the most current copies of any Contractor Property to which EOHHS has rights pursuant to the foregoing, including any related documentation.

Notwithstanding anything contained herein to the contrary, and notwithstanding EOHHS's use of Contractor Property under the license created herein, Contractor shall have all the rights and incidents of ownership with respect to Contractor Property, including the right to use such property for any purpose whatsoever and to grant licenses in the same to third parties. Contractor shall not encumber or otherwise transfer any rights that would preclude a free and clear license grant to the Commonwealth.

3. Commonwealth Property

In conformance with the Commonwealth Terms and Conditions, all Deliverables created under this Agreement whether made by Contractor, subcontractor or both are the property of EOHHS, except for the Contractor Property embodied in the Deliverable. Contractor irrevocably and unconditionally sells, transfers and assigns to EOHHS or its designee(s), the entire right, title, and interest in and to all intellectual property rights that it may now or hereafter possess in said Deliverables, except for the Contractor Property embodied in the Deliverables, and all derivative works thereof. This sale, transfer and assignment shall be effective immediately upon creation of each Deliverable and shall include all copyright, patent, trade secret, trademark and other intellectual property rights created by Contractor or subcontractor in connection with such work (hereinafter the "Commonwealth Property"). "Commonwealth Property" shall also include the specifications, instructions, designs, information, and/or materials, proprietary tools and methodologies including, but not limited to software and hardware,

owned, licensed or leased by EOHHS and which is provided by EOHHS to Contractor or of which Contractor otherwise becomes aware as well as EOHHS's Confidential Information, the Commonwealth Data and EOHHS's intellectual property and other information relating to its internal operations.

All material contained within a Deliverable and created under this Agreement, except for the Contractor Property embodied in a Deliverable (for which the Contractor shall grant EOHHS the license described in **Section 5.3.G.2**), are works made for hire.

Contractor agrees to execute all documents and take all actions that may be reasonably requested by EOHHS to evidence the transfer of ownership of or license to intellectual property rights described in this **Section 5.3.G**, including providing any code used exclusively to develop such Deliverables for EOHHS and the documentation for such code. The Commonwealth retains all right, title and interest in and to all derivative works of Commonwealth Property.

EOHHS hereby grants to Contractor a nonexclusive, revocable license to use, copy, modify and prepare derivative works of Commonwealth Property only during the term and only for the purpose of performing services and developing Deliverables for the EOHHS under this Agreement.

Contractor agrees that it will not: (a) permit any third party to use Commonwealth Property; (b) sell, rent, license or otherwise use the Commonwealth Property for any purpose other than as expressly authorized under this Agreement; or (c) allow or cause any information accessed or made available through use of the Commonwealth Property to be published, redistributed or retransmitted or used for any purpose other than as expressly authorized under this Agreement. Contractor agrees not to, modify the Commonwealth Property in any way, enhance or otherwise create derivative works based upon the Commonwealth Property or reverse engineer, decompile or otherwise attempt to secure the source code for all or any part of the Commonwealth Property, without EOHHS's express prior consent. EOHHS reserves the right to modify or eliminate any portion of the Commonwealth Property in any way at any time. EOHHS may terminate use of the Commonwealth Property by Contractor immediately and without prior notice in the event of the failure of such person to comply with the security or confidentiality obligations hereunder. The Commonwealth Property is provided "AS IS" and EOHHS FOR ITSELF, ITS AGENCIES AND ANY RELEVANT AUTHORIZED USERS EXPRESSLY DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES CONCERNING THE COMMONWEATH PROPERTY, COMMONWEALTH DATA OR ANY THIRD PARTY CONTENT TO BE PROVIDED HEREUNDER, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT,

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR QUALITY OF SERVICES.

H. Ownership of Furnishings and Equipment

Unless t, the Contractor shall provide and retain all furnishings and equipment used in the completion of its performance under this Contract.

I. Counterparts

The Contract may be executed simultaneously in two or more counterparts, each of which will be deemed an original and all of which together will constitute one and the same instrument.

J. Entire Contract

The Contract constitutes the entire agreement of the parties with respect to the subject matter hereof, including all Attachments and Appendices hereto, and supersedes all prior agreements, representations, negotiations and undertakings not set forth or incorporated herein. The terms of the Contract shall prevail notwithstanding any variances with the terms and conditions of any verbal communication subsequently occurring, except as otherwise provided herein. This Contract, including the Commonwealth of Massachusetts Standard Contract Form and Commonwealth Terms and Conditions, shall supersede any conflicting verbal or written agreements, forms, or other documents relating to the performance of this Contract.

K. No Third Party Enforcement

No person not executing this Contract shall be entitled to enforce this Contract against a party hereto regarding such party's obligations under this Contract.

L. Intermediate Sanctions

1. In addition to termination under **Section 5.5**, EOHHS may, in its reasonable discretion, impose any or all of the sanctions in **Section 5.3.L.2** below, for any of the following circumstances. EOHHS shall only impose those sanctions it determines to be reasonable and appropriate for the specific violation(s) identified. Sanctions may be imposed if the Contractor:

    a. Fails substantially to provide Medically Necessary items and services required to be provided under this Contract or under law to Covered Individuals and Uninsured Individuals including persons covered by Medicare only;

    b. Imposes co-payments, premiums or other charges on Covered Individuals and Uninsured Individuals including persons covered by Medicare in excess of any permitted under this Contract;

c. Discriminates against Covered Individuals on the basis of race, color, gender, or national origin;

d. Discriminates among Covered Individuals on the basis of health status or need for health care services, including termination of enrollment or refusal to reenroll a Covered Individual, except as permitted under **Section 2.4.B**, or any practice that would reasonably be expected to discourage enrollment by Covered Individuals whose medical condition or history indicates probable need for substantial future medical services;

e. Misrepresents or falsifies information provided to CMS or EOHHS;

f. Misrepresents or falsifies information provided to Covered Individuals, Members, Providers, or PCCs;

g. Fails to comply with requirements regarding physician incentive plans;

h. Fails to comply with requirements regarding Provider-Covered Individual communications;

i. Fails to comply with federal or state statutory or regulatory requirements related to the Contract;

j. Violates restrictions or other requirements regarding marketing;

k. Fails to comply with health improvement targets and quality improvement goal requirements set forth in **Section 2.13** of this contract;

l. Fails to comply with any corrective action plan required by EOHHS;

m. Fails to meet readiness review timeframes or address readiness deficiencies in a timely manner as required under **Section 2.2.B** and **Appendix B-1** of this Contract

n. Fails to meet deliverable timelines which deliverables shall include those reports, analyses, workplans, surveys, evaluations, metrics and other documents with submission dates explicitly defined in the Contract or, if a date is not specified, with explicit timelines or bases of specified duration provided therein;

o. Submits required reports that are either late or missing a significant amount of information or data;

p. Fails to meet any of the standards for data submission described in this contract, including accuracy, completeness, timeliness, and other standards for Encounter Data described in **Section 2.14.E** and **Appendices D-1** and **D-2**. Sanctions for such failure are further described in **Section 5.3.L.2**;

q. Fails to meet satisfactory performance based upon EOHHS' Performance Management Evaluation, in accordance with the provisions of **Section 3.1.C**;

r. Fails to comply with financial solvency requirements as set forth in **Section 2.15**;

s. Fails to comply, as determined by EOHHS from audit findings, with any provision of this Contract related to DSRAs;

t. Fails to comply with the False Claims provision of the Deficit Reduction Act of 2005

u. Fails to take all steps necessary, as determined by EOHHS, to enable EOHHS to maximize rebate collection as set forth in **Section 2.6.D.1.d**;

v. Fails to comply with any other requirement of Section 1932 of the Social Security Act, and any implementing regulations; or

w. Fails to comply with any other requirements of this Contract.

2. Such sanctions may include without limitation, any or all of the following:

a. Civil monetary penalties in accordance with 42 CFR 438.704;

b. financial penalties, including without limitation asserting EOHHS's rights under its Performance Guarantee, in accordance with the provisions of **Appendix H-2**;

c. withholding of administrative payments;

d. withholding Performance Incentive bonuses;

e. the appointment of temporary management to oversee the operation of the Contractor in those circumstances set forth in 42 U.S.C. § 1396u-2(e)(2)(B) and 42 CFR 438.706;

f. suspension of payment to the Contractor; adjusting or withholding Estimated Base Capitation Rate Payments or other Base PMPM Capitation Rate payments;

g. adjusting or withholding of Service Compensation Payments;

h. adjusting or withholding the DMH Administrative Compensation Rate or Administrative Component of the MassHealth Capitation Payments; and

3. withholding gain from any risk-sharing arrangement.

4. For any Contract responsibilities for which the Contractor utilizes a Material Subcontractor, if EOHHS identifies any deficiency in the Contractor's performance under the Contract for which the Contractor has not successfully

implemented an approved corrective action plan in accordance with **Section 5.3.M**, EOHHS may:

a. require the Contractor to terminate its agreement with the Material Subcontractor and subcontract with a Material Subcontractor deemed satisfactory by EOHHS; or

b. otherwise require the Contractor to altern the manner or method in which the Contractor performs such Contractor responsibility.

5. Civil monetary penalties shall be administered in accordance with 42 CFR 438.704 as follows:

a. The limit is $25,000 for each determination under the following:

1) failure to provide Medically Necessary items and services;

2) misrepresentation or false statement to a Covered Individual, Member, or Provider;

3) failure to comply with requirements regarding physician incentive plans; or

4) violates restrictions or other requirements regarding Marketing.

b. The limit is $100,000 for each determination under the following:

1) discrimination; or

2) misrepresentation or false statements to CMS or EOHHS.

c. The limit is $15,000 for each Covered Individual EOHHS determines was terminated or not re-enrolled because of a discriminatory practice under **Section 5.3.L.1.d** above (with an overall limit of $100,000 under **Section 5.3.L.4.b** above).

d. The limit is $25,000 or double the amount of the excess charges, whichever is greater, for each determination under **Section 5.3.L.1.b** above.

6. Encounter Data and other Related Data Capitation Payment Deduction

a. For each month where the Contractor has not met data submission standards, including those for Encounter Data, as described in **Section 2.14, Appendix E,** and elsewhere in this Contract, EOHHS shall apply a Capitation Payment deduction as follows:

1) EOHHS shall deduct 2% from the Contractor's Capitation Payment for one month;

2) Once Contractor has corrected a month's data submission, in EOHHS's reasonable determination, EOHHS shall pay the Contractor the amount of the deduction applied for such month;

3) If EOHHS subsequently detects additional deficiencies in such corrected data submission, EOHHS may apply the deduction again to a subsequent month's Capitation Payment;

4) EOHHS shall administer such deductions so that EOHHS shall at no time have applied more than five such deductions. Deductions that are paid back as described in **Section 5.3.L.5.a** above shall not count towards such five deduction limit; and

5) Notwithstanding the deductions described in this Section, EOHHS may take corrective action for any failure by Contractor to comply with the data submission requirements of this Contract;

b. If the Contractor does not meet Encounter Data and other data or documentation submission deadlines for risk sharing arrangements as specified in **Section 4.6,** EOHHS may apply a Capitation Payment deduction equal to $400,000.00, if EOHHS chooses to incorporate such Encounter Data and other data and documentation into the risk sharing arrangement calculations set forth in **Section 4.6** for that particular Contract Year. EOHHS will not impose such Capitation Payment deduction if EOHHS chooses not to incorporate such Encounter Data and other data and documentation into such risk sharing arrangement calculations for that particular Contract Year pursuant to **Section 4.6**.

7. For each instance where the Contractor has failed to submit on time its Financial Encounter Validation Report as set forth in **Appendix E-4**, EOHHS may apply a Capitation Payment deduction as follows:

a. EOHHS may deduct $500.00 for each business day the Financial Encounter Validation Report is late from the Contractor's next Capitation Payment, unless:

1) the Contractor has requested an extension at least three business days prior to the report's due date, including with its request the reason for the needed extension and an action plan and timeline for when the Contractor is able to submit such report; and

2) EOHHS has granted the Contractor's request

b. If EOHHS grants the Contractor's extension request, EOHHS may deduct $500.00 for each business day the Contractor's Financial Encounter Validation report is late past the new deadline EOHHS granted under the

Contractor's extension request from the Contractor's next Capitation Payment.

8. The intermediate sanctions provisions contained in this Contract are pursuant to state authority, unless otherwise specifically provided.

9. Denial of Payment Sanction

In accordance with 42 CFR 438.726(b) and 42 CFR 438.730(e), EOHHS shall deny payments under this Contract to the Contractor for New Covered Individuals if CMS denies payment to EOHHS for the same New Covered Individuals in the following situations:

a. If a CMS determination that the Contractor has acted or failed to act as described in **Section 5.3.L.1.** of this Contract is affirmed on review pursuant to 42 CFR 438.730(d).

b. If a CMS determination that the Contractor has acted or failed to act as described in **Section 5.3.L.1.** of this Contract is not timely contested by the Contractor under 42 CFR 438.730(c).

For the purposes of this **Section 5.3.L.9,** New Covered Individual shall be defined as a Covered Individual that applies for enrollment after the Effective Date of this Sanction (the date determined in accordance with 42 CFR 438.730(f)).

c. Before imposing any of the intermediate sanctions specified in this **Section 5.3.L**, EOHHS shall give the Contractor written notice that explains the basis and nature of the sanctions not less than 14 calendar days before imposing such sanction.

10. Overpayment Capitation Deduction

a. In accordance with **Section 2.3.D.3.d**, if the Contractor identifies an overpayment prior to EOHHS and does not recover such overpayment within 180 days after identification, without providing sufficient justification, as determined by EOHHS, in the Summary of Provider Overpayments report to EOHHS, EOHHS may apply a Capitation Payment deduction in an amount equal to the overpayment identified but not collected;

b. In accordance with **Section 2.3.D.3.d** if EOHHS identifies an overpayment prior to the Contractor such that the Contractor did not identify and report such overpayment to EOHHS in accordance with all applicable Contract requirements, including but not limited to the Summary of Provider Overpayments Report, within 180 days of the date(s) of service associated with any Claim(s) included in the overpayment:

1) In the event the Contractor recovers such overpayment as agreed upon by EOHHS and the Contractor within 90 days of the Contractor's response to EOHHS's notification of the overpayment, EOHHS may apply a Capitation Payment deduction equal to 80% of the agreed-upon overpayment amount. No Capitation Payment deductions shall apply to any amount of a recovery to be retained under the False Claims Act cases or through other investigations.

2) In the event the Contractor does not recover such overpayment first identified by EOHHS within 90 days of the Contractor's response to EOHHS's notification of the overpayment, without providing sufficient justification to EOHHS for any initial overpayment amounts identified but not recovered as determined by the sole discretion of EOHHS, EOHHS may apply a Capitation Payment deduction equal to the amount of the overpayment identified but not collected. No Capitation Payment deductions shall apply to any amount of a recovery to be retained under the False Claims Act cases or through other investigations.

c. EOHHS shall calculate, following the end of the Contract Year, any and all Capitation Payment deductions for any prior Contract Year pursuant to this **Section 5.3.L**.

d. Notwithstanding the Capitation Payment deductions described in this Section, EOHHS may take corrective action for a failure by the Contractor to take all steps necessary, as determined by EOHHS, to report overpayments as specified in this Contract, including those requirements set forth in **Section 2.3.D.3.d**.

M. Corrective Action Plan

If, at any time, EOHHS determines that the Contractor is deficient in the performance of its obligations under the Contract, EOHHS may require the Contractor to develop and submit a corrective action plan to correct such deficiency. EOHHS shall approve, disapprove, or require modifications to the corrective action plan based on its reasonable judgment as to whether the corrective action plan will correct the deficiency. The Contractor shall, upon EOHHS approval, immediately implement the corrective action plan, as approved or modified by EOHHS. The Contractor's failure to implement any corrective action plan may, in the sole discretion of EOHHS, be considered breach of Contract and subject to any and all contractual remedies including: those under the Contractor's Performance Guarantees in accordance with **Appendix H-2**; termination of the Contract with or without notice; or other intermediate sanctions as described in **Section 5.3.L**.

N. Section Headings

The headings of the Sections of the Contract are for convenience only and do not affect the construction hereof.

O. Administrative Procedures Not Covered

EOHHS may from time-to-time issue memoranda clarifying, elaborating upon, explaining, or otherwise relating to Contract administration and other management matters.

P. Effect of Invalidity of Clauses

If any clause or provision of the Contract is in conflict with any state or federal law or regulation, that clause or provision shall be null and void; any such invalidity shall not affect the validity of the remainder of the Contract.

Q. Conflict of Interest

Neither the Contractor nor any Material Subcontractor shall, for the duration of the Contract, have any interest that will conflict, as determined by EOHHS, with the performance of services under the Contract, or that may be otherwise anticompetitive. Without limiting the generality of the foregoing, EOHHS requires that neither the Contractor nor any Material Subcontractor have any financial, legal, contractual or other business interest in any entity performing health plan enrollment functions for EOHHS, the CSC Enrollment Vendor and subcontractor(s) if any).

R. Insurance for Contractor's Employees

1. The Contractor shall agree to maintain at the Contractor's expense all insurance required by law for its employees, including worker's compensation and unemployment compensation, and shall provide EOHHS with certification of same upon request. The Contractor, and its professional personnel providing services to Covered Individuals, shall obtain and maintain appropriate professional liability insurance coverage. The Contractor shall, at EOHHS's request, provide certification of professional liability insurance coverage.

2. The Contractor shall offer health insurance to its employees sufficient to ensure that it is not obligated to provide a share payment under Chapter 58.

S. Waiver

The exercise or non-exercise of any authority under this Contract by either party, including, but not limited to, EOHHS's review and approval of materials submitted in relation to the Contract, shall not relieve the other party of any obligations set forth herein, nor be construed as a waiver of any of the other party's obligations or as acceptance by EOHHS of any unsatisfactory practices or breaches by the other party.

Section 5.4 Record Retention, Inspection and Audit

The Contractor shall make available the administrative and medical records maintained by the Contractor and its subcontractors, including but not limited to Network Providers, to EOHHS and its agents, designees or contractors, any other authorized representatives of the Commonwealth of Massachusetts or the United States Government, or their designees or contractors, at such times, places, and in such manner as such entities may reasonably request for the purposes of financial and/or medical audits, programmatic review, inspections, and examinations, provided that such activities shall be conducted during the normal business hours of the Contractor. Such records shall be maintained and available to EOHHS for seven (7) years. Such administrative and medical records shall include but not be limited to care management documentation, financial statements, Provider Contracts, contracts with subcontractors, including financial provisions of such Provider Contracts and subcontractor contracts. The Contractor further agrees that the Secretary of the U.S. Department of Health and Human Services or his designee, the Governor or his designee, and the State Auditor or his designee may inspect and audit any financial records of the Contractor or its subcontractors.

Notwithstanding the generality of the foregoing, pursuant to 42 CFR 438.3(h), EOHHS, other representatives from the Commonwealth of Massachusetts, CMS, the Office of the Inspector General, the Comptroller General, and their designees, may, at any time, inspect and audit any records or documents of the Contractor or its subcontractors, and may, at any time, inspect the premises, physical facilities, and equipment where activities or work related to this Contract is conducted. The right to audit under this Section exists for 10 years from the last day of this Contract or from the date of completion of any audit, whichever is later. The Contractor shall maintain all records and documents relating to activities or work under this Contract for a period of no less than 10 years.

In cases where such an audit or review results in EOHHS believing an overpayment has been made, EOHHS may seek to pursue recovery of overpayments. EOHHS will notify the Contractor in writing of the facts upon which it bases its belief, identifying the amount believed to have been overpaid and the reasons for concluding that such amount constitutes an overpayment. In the event the overpayment amount is based on a determination by a federal or state agency (other than EOHHS) of an overpayment by EOHHS, EOHHS will so inform the Contractor and, in such cases, the Contractor may contest only the factual assertion that the federal or state agency made such a determination. The Contractor may not contest in any proceeding before or against EOHHS the amount or basis for such determination.

Section 5.5 Termination of Contract

A. Termination without Prior Notice

EOHHS may terminate the Contract immediately and without prior written notice, upon any of the following events. EOHHS shall provide written notice to the Contractor upon such termination:

1. The Contractor's application for or consent to the appointment of a receiver, trustee, or liquidator for itself or any of its property.

2. The Contractor's admission in writing that it is unable to pay its debts as they mature.

3. The Contractor's assignment for the benefit of creditors.

4. Commencement of a proceeding under any bankruptcy, reorganization, insolvency, or readjustment of debt provision of federal or state law or answer admitting the material allegations of a petition filed against the Contractor in any such proceeding.

5. Commencement of an involuntary proceeding against the Contractor or Material Subcontractor under any bankruptcy, reorganization, insolvency, or readjustment of debt provision of federal or state law, which is not dismissed within 60 days.

6. The Contractor incurs loss of any of the following: (1) licensure at any of the Contractor's facilities; (2) state approval of the Contractor; or (3) NCQA accreditation;

7. Cessation in whole or in part of state or federal funding for this Contract, provided that termination for this reason shall occur no earlier than the last day of the month in which such funding ceases;

8. EOHHS determines in its reasonable discretion that the health, safety or welfare of its Covered Individuals requires immediate termination of the Contract.

9. The Contractor is non-compliant with **Section 5.1.G**, and the Secretary of Health and Human Services, in accordance with 42 CFR 438.610(c), directs EOHHS to terminate, or does not permit EOHHS to extend, renew or otherwise continue this Contract.

10. The Contractor is non-compliant with **Section 5.1.O**.

B. Termination with Prior Notice

1. Either party may terminate the Contract upon breach by a party of any duty or obligation hereunder, which breach continues unremedied for 30 days after written notice thereof by the other party.

2. EOHHS may terminate the Contract after written notice thereof to the Contractor in the event the Contractor fails to accept EOHHS's proposed offer of payment for any financial provision identified in **Section 4** of this Contract.

3. EOHHS may terminate the Contract if the EOHHS determines that state or federal health care reform initiatives or state or federal health care cost containment initiative makes termination of the Contract necessary or advisable as determined by EOHHS

C. Continued Obligations of the Parties

1. In the event of termination, expiration or non-renewal of the Contract, the obligations of the parties hereunder with regard to each Covered Individual at the time of termination, expiration, or non-renewal shall continue until the Covered Individual has been disenrolled; provided, however, that EOHHS shall exercise best efforts to promptly complete all disenrollment activities within six months from the date of termination, expiration or non-renewal.

2. In the event that the Contract is terminated, expires, or is not renewed for any reason:

    a. EOHHS shall be responsible for notifying all Covered Individuals covered by this Contract of the date of termination and the process by which they will continue to receive medical care;

    b. The Contractor shall promptly return to EOHHS all payments advanced to the Contractor for coverage of Covered Individuals for periods after the effective date of their disenrollment; and

    c. The Contractor shall supply to EOHHS all information necessary for the reimbursement of any outstanding claims determined by EOHHS to be due to the Contractor, and any such claims shall be paid to the Contractor accordingly.

3. For termination of the Contract for failure by the Contractor to agree to any Capitation Rate, the Contractor shall accept the lesser of the most recently agreed to Capitation Rates or the new Capitation Rate for each RC as payment in full for BH Covered Services and all other services required under this Contract delivered to Covered Individuals until all Covered Individuals have been disenrolled from the Contractor's Plan; and

4. For expiration or non-renewal of the Contract following a reprocurement of the PCC Plan's BH Program, the financial terms in effect for the current Contract Year shall remain in effect until all Covered Individuals have been disenrolled, except that there shall be no Performance Incentives in EOHHS's sole discretion.

D. Termination Authority

The termination provisions contained in this Contract are pursuant to state authority, unless otherwise specifically provided.

E. Termination Pursuant to 42 CFR 438.708

1. EOHHS may terminate this Contract pursuant to its authority under 42 CFR 438.708

2. If EOHHS terminates this Contract pursuant to its authority under 42 CFR 438.708, EOHHS shall provide the Contractor with a pre-termination hearing in accordance with 42 CFR 438.710 as follows:

a. EOHHS shall give the Contractor written notice of intent to terminate, the reason for termination, and the time and place of the hearing;

b. After the hearing, EOHHS shall give the Contractor written notice of the decision affirming or reversing the proposed termination of the Contract and, for an affirming decision, the effective date of termination; and

c. If the decision is affirmed, EOHHS shall give Covered Individuals notice of the termination and information on their options for receiving MassHealth services following the effective date of termination in accordance with 42 CFR 438.710(b)(2)(iii) and **Section 5.5.C.2**. of this Contract.

3. If EOHHS terminates this Contract, EOHHS and the Contractor shall comply with all Continuing Obligations set forth in **Section 5.5.C** of this Contract;

Section 5.6 Contract Term

The Contract is effective upon execution, through December 31, 2027, unless otherwise terminated or extended in accordance with this Section or at such other time that EOHHS may implement changes that render the performance of the Contract unnecessary. At EOHHS's option, the Contract may be extended in any increments through December 31, 2032, and upon terms to be negotiated by the parties. EOHHS reserves the right to further extend the Contract for any reasonable increment it determines necessary to complete a subsequent procurement. Extension of this Contract is subject to mutual agreement on terms by both parties, further legislative appropriations, continued legislative authorization, and EOHHS' determination of satisfactory performance.

Section 5.7 Additional Modifications to the Contract Scope

EOHHS shall have the option at its sole discretion to modify, reduce or terminate any activity related to the Contract whenever, in the judgment of EOHHS, the goals of the project have been modified or altered in any way that necessitates such changes. In the event of the reduction of the scope of work for any tasks or portions thereof, EOHHS will provide written notice to the Contractor. In the event of a change in the scope of work of any tasks or portions thereof, EOHHS will initiate negotiations with the Contractor.

Section 5.8 Amendments

A. The parties agree to negotiate in good faith to cure any omissions, ambiguities, or manifest errors herein. By mutual agreement, the parties may amend this Contract where such amendment does not violate state or federal statutory, regulatory, or waiver provisions, provided that such amendment is in writing, signed by authorized representatives of both parties, and attached hereto. Further, the Contractor agrees to take such action as is necessary to amend this Contract in order for EOHHS to comply with all applicable state and federal laws, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Balanced Budget Amendments of 1997 (BBA) and any regulations promulgated thereunder, the Deficit Reduction Act, and Health Care Reform, as well as any regulations, policy guidance, and policies and procedures related to any such applicable state and federal laws. EOHHS additionally reserves the right, at its sole discretion, to amend the Contract to implement judicial orders, settlement agreements, or any state or federal initiatives or changes affecting EOHHS or the Contract. EOHHS may terminate this Contract immediately upon written notice in the event the Contractor fails to agree to any such amendment.

B. EOHHS and Contractor mutually acknowledge that unforeseen policy, operational, methodological, or other issues may arise throughout the course of this Contract. Accordingly, EOHHS and Contractor agree to work together in good faith to address any such circumstances and resolve them, and, if necessary, will enter into amendments to this Contract on mutually agreeable terms.

C. Notwithstanding the generality of the foregoing, EOHHS reserves the right to amend the Contract to implement new initiatives or to modify initiatives related to:

1. new MassHealth programs;
2. expansion of or changes to existing MassHealth programs;
3. other programs as specified by EOHHS;
4. programs resulting from state or federal legislation, including but not limited to the Patient Protection and Affordable Care Act (ACA) of 2010 (Public Law 111–148 March 23, 2010), regulations, initiatives, or judicial decisions that may affect in whole or in part any components of the PCC Plan or the BHP;
5. requiring or allowing individuals age 65 and over, with or without Medicare and individuals age 21 or over with Medicare to enroll in the PCC Plan or the BHP; and
6. changes the managed care options available to any or all MassHealth Coverage Types, in whole or in part, or excluding any or all MassHealth Coverage Types from either mandatory or voluntary Managed Care.

7. The parties shall negotiate in good faith to implement any such initiatives proposed by EOHHS. The Contractor's responsibilities, including staffing, space, and all other budgetary requirements, are subject to change due to implementation of such initiatives. EOHHS reserves the right to modify the Contract, including the budget and reimbursements, due to program modifications. In addition, the Contractor may request an opportunity to enter into negotiations with EOHHS over amendments to the Contract related to new initiatives or modified initiatives as described in this Section. EOHHS may grant such a request in its sole discretion.

D. EOHHS reserves the right to enroll additional MassHealth Members over the term of the Contract, or to reduce current enrollment levels. Possible EOHHS initiatives that could change enrollment include but are not limited to:

1. Increased or decreased MassHealth membership pursuant to any MassHealth waiver;

2. Expanded eligibility coverage for children under age 19 or adults over 65;

3. Any other state or federal changes that result in an increase or decrease in MassHealth-eligible individuals, including changes to comply with the ACA, such as an adjustment to the minimum federal poverty eligibility level, or a change in the MassHealth Managed Care enrollment policy or criteria for participation; and

4. Changes in EOHHS's methodology by which assignments are made to MassHealth Managed Care plans.

E. The Contractor shall propose to EOHHS for approval during the term of the Contract new initiatives and reimbursement mechanisms designed to further integrate PCC Plan administrative functions with BH management and performance. Such proposals shall include, upon EOHHS request, detailed work plans and timelines. EOHHS may at its sole discretion accept, reject or modify any proposed initiative.

Section 5.9 Order of Precedence

The Contractor's response to EOHHS's Request for Responses (RFR) that served as the basis for this Contract is incorporated by reference into the Contract. Any ambiguity or inconsistency between these documents shall be resolved by applying the following order of precedence:

A. this Contract, including any amendments thereto;

B. EOHHS's Request for Responses (RFR) for a Vendor to Provide Comprehensive Behavioral Health Program and Management Support Services , issued on March 17, 2022, including any amendments thereto; and

C. the Contractor's response to the RFR identified below submitted on June 6, 2022.

Section 5.10 Managed Care Activities Vacated by the Court

Should any part of the scope of work under this Contract relate to an EOHHS program that is no longer authorized by law (e.g., which has been vacated by a court of law, or for which CMS has withdrawn federal authority, or which is the subject of a legislative repeal), the Contractor must do no work on that part after the effective date of the loss of program authority. EOHHS must adjust the capitation rates for at risk services to remove costs that are specific to any program or activity that is no longer authorized by law. If the Contractor works on a program or activity no longer authorized by law after the date the legal authority for the work ends, the Contractor will not be paid for that work. If EOHHS paid the Contractor in advance to work on a no-longer-authorized program or activity and under the terms of this contract the work was to be performed after the date the legal authority ended, the payment for that work should be returned to the EOHHS. However, if the Contractor worked on a program or activity prior to the date legal authority ended for that program or activity, and EOHHS included the cost of performing that work in its payments to the Contractor, the Contractor may keep the payment for that work even if the payment was made after the date the program or activity lost legal authority.

Section 5.11 Written Notices

Notices to the parties as to any Contract matter will be sufficient if given in writing and sent by certified mail, postage prepaid, or delivered in hand as follows:

To EOHHS:

Associate Chief of Behavioral Health
Executive Office of Health and Human Services
1 Ashburton Place, 11th floor
Boston, MA 02108

With copies to:

General Counsel
Executive Office of Health and Human Services
1 Ashburton Place, 11th floor
Boston, MA 02108

Rashiem Grant, Contract Manager
Executive Office of Health and Human Services
Accounting Unit, 7th floor
600 Washington Street
Boston, MA 02111-1712

And, in addition, for notices required by the provisions of **Section 5.2**, a copy to:

EOHHS Privacy Office
One Ashburton Place, 11th Floor
Boston, MA 02111

To the Contractor:

Massachusetts Behavioral Health Partnership
200 State Street
Boston, MA 02109
Attention: Chief Executive Officer

With copies to:

Carelon Behavioral Care, Inc.
200 State Street,
Suite 302
Boston, MA 02109
Attention: General Counsel

APPENDIX A-1
BEHAVIORAL HEALTH COVERED SERVICES

✓ Denotes a covered service

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
Inpatient Services - 24-hour services, delivered in a licensed or state-operated hospital setting, that provide clinical intervention for mental health or substance use diagnoses, or both. This service does not include continuing inpatient psychiatric care delivered at a facility that provides such services, as further specified by EOHHS. **(See details below)**					
1. **Inpatient Mental Health Services -** hospital services to evaluate and treat an acute psychiatric condition which 1) has a relatively sudden onset; 2) has a short, severe course; 3) poses a significant danger to self or others; or 4) has resulted in marked psychosocial dysfunction or grave mental disability. Such services include (1) specialized inpatient psychiatric services provided to children or adolescents with neurodevelopmental disorders who have severe behavioral manifestations of Autism Spectrum Disorders (ASD)/Intellectual Disabilities (ID) and co-occurring mental health conditions, and shall be provided in accordance with the MassHealth Acute Hospital Request for Applications (Acute Hospital RFA) and the MassHealth Psychiatric Hospital Request for Applications (Psychiatric Hospital RFA); and (2) for dates of service on or after October 1, 2023, specialized inpatient psychiatric services provided to Covered Individuals with an eating disorder diagnosis and severe associated psychiatric and medical needs in specialized eating disorder psychiatric settings, and shall be provided in accordance with the Acute Hospital RFA and the	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
MassHealth Psychiatric Hospital Request for Applications (Psychiatric Hospital RFA).					
2. **Inpatient Substance Use Disorder Services (Level 4) –** Intensive inpatient services provided in a hospital setting, able to treat Covered Individuals with acute medically complex withdrawal management needs, as well as co-occurring biomedical and/or psychiatric conditions. Services are delivered by an interdisciplinary staff of addiction credentialed physician and other appropriate credentialed treatment professionals with the full resources of a general acute care or psychiatric hospital available.	✓	✓	✓		
3. **Observation/Holding Beds –** hospital services, for a period of up to 24 hours, in order to assess, stabilize, and identify appropriate resources for Covered Individuals.	✓	✓	✓		
4. **Administratively Necessary Day (AND) Services –** a day(s) of inpatient hospitalization provided to Covered Individuals when said Covered Individuals are clinically ready for discharge, but an appropriate setting is not available. Services shall include appropriate continuing clinical services.	✓	✓	✓		
Diversionary Services - those mental health and substance use disorder services that are provided as clinically appropriate alternatives to Behavioral Health Inpatient Services, or to support a Covered Individual returning to the community following a 24-hour acute placement; or to provide intensive support to maintain functioning in the community. There are two categories of Diversionary Services, those provided in a 24-hour facility, and those which are provided in a non-24-hour setting or facility. **(See detailed services below)**					

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
24-Hour Diversionary Services					
a. **Youth and Adult Community Crisis Stabilization** – services provided as an alternative to hospitalization, including short-term psychiatric treatment in structured, community-based therapeutic environments. Community Crisis Stabilization provides continuous 24-hour observation and supervision for Covered Individuals who do not require or are transitioning from Inpatient Services.	✓	✓	✓		
b. **Community-Based Acute Treatment for Children and Adolescents (CBAT) –** mental health services provided in a staff-secure setting on a 24-hour basis, with sufficient clinical staffing to insure safety for the child or adolescent, while providing intensive therapeutic services including, but not limited to, medication monitoring; psychiatric assessment; nursing availability; Specialing (as needed); individual, group and family therapy; case management; family assessment and consultation; discharge planning; and psychological testing, as needed. This service may be used as an alternative to or transition from Inpatient services. CBAT includes, but is not limited to, Intensive Community-Based Acute Treatment for Children and Adolescents (ICBAT).	✓	✓			
c. **Medically Monitored Intensive Services --Acute Treatment Services (ATS) for Substance Use Disorders (Level 3.7) –** 24-hour, seven days week, medically monitored addiction treatment services that provide evaluation and withdrawal management. Withdrawal management services are delivered by nursing and counseling staff under a physician-approved	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
protocol and physician-monitored procedures and include: bio-psychosocial assessment; induction to FDA approved medications for addictions when appropriate, individual and group counseling; psychoeducational groups; and discharge planning. Pregnant women receive specialized services to ensure substance use disorder treatment and obstetrical care. Covered Individuals with Co-Occurring Disorders receive specialized services to ensure treatment for their co-occurring psychiatric conditions. These services may be provided in licensed freestanding or hospital-based programs.					
d. Clinical Stabilization Services for Substance Use Disorders (Level 3.5) – 24-hour treatment services which can be used independently or following Acute Treatment Services for substance use disorders including comprehensive bio-psychosocial assessments and treatment planning, therapeutic milieu, intensive psycho education and counseling, outreach to families and significant others; linkage to medications for addiction therapy, connection to primary care and community supports and aftercare planning for individuals beginning to engage in recovery from addiction. Covered Individuals with Co-Occurring Disorders receive coordination of transportation and referrals to mental health providers to ensure treatment for their co-occurring psychiatric conditions. Pregnant women receive coordination of their obstetrical care.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
e. Individualized Treatment Stabilization Services (ITS) Tier 1 – A program that provides integrated ASAM Level 3.7 (ATS) and ASAM Level 3.5 (CSS) services in a single unit or location for stabilization and continuity of care. ITS Tier 1 programs must meet all expectations for both service models, including licensure requirements. ITS Tier 1 serves members who are involuntarily committed to treatment due to the severity and level of impairment caused by their SUD. ITS Tier 1 includes all requirements of ASAM Level 3.7 (ATS) and ASAM Level 3.5 (CSS) and psychopharmacology services, a minimum of six hours of clinical services 7 days a week, treatment for mental health and co-occurring disorders, clinical programming must include evidence-based practices such as cognitive behavioral therapy (CBT) and acceptance and commitment therapy (ACT), as well as other targeted behavioral interventions that promote skill-building and the facilitation of access to recovery support navigator services and peer recovery coach services.	✓	✓	✓		
f. Individualized Treatment Stabilization Services (ITS) Tier 2 – An integrated program that provides enhanced ASAM Level 3.7 (ATS) and ASAM Level 3.5 (CSS) services in a single unit or location for stabilization and continuity of care. ITS Tier 2 must meet all expectations for both service models. ITS Tier 2 serves members who have co-occurring disorders and multiple unsuccessful treatment episodes at lower levels of care who would benefit from fewer transitions between levels of care and enhanced engagement interventions. ITS Tier 2 includes all requirements of ASAM Level 3.7 (ATS) and ASAM Level 3.5	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
(CSS) and psychopharmacology services, a minimum of six hours of clinical services 7 days a week, treatment for mental health and co-occurring disorders, clinical programming must include evidence-based practices such as cognitive behavioral therapy (CBT) and acceptance and commitment therapy (ACT), as well as other targeted behavioral interventions that promote skill-building and the facilitation of access to recovery support navigator services and peer recovery coach services.					
g. Youth Withdrawal Management and Stabilization Services – Integrated ASAM 3.7 (ATS) and ASAM 3.5 (CSS) providing developmentally appropriate services to adolescents ages 13-17 years of age. Youth withdrawal management and stabilization services shall be located separately from any adult services. Youth withdrawal management services must individually assess youth according to ASAM criteria and implement treatment plans to meet the youths' needs. For ASAM level 3.7 service must include 24-hour, seven-days a week, medically monitored addiction treatment services that provide evaluation and withdrawal management. Withdrawal management services are delivered by nursing and counseling staff under a physician-approved protocol and physician-monitored procedures and include: bio-psychosocial assessment; induction to FDA approved medications for addictions when appropriate, individual and group counseling; psychoeducational groups; and discharge planning. Pregnant women receive specialized services to ensure substance use disorder treatment and obstetrical care. Covered Individuals	✓	✓			

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
with Co-Occurring Disorders receive specialized services to ensure treatment for their co-occurring psychiatric conditions. ASAM 3.5 (CSS) 24-hour treatment services which can be used independently or following Acute Treatment Services for substance use disorders including comprehensive bio-psychosocial assessments and treatment planning, therapeutic milieu, intensive psycho education and counseling, outreach to families and significant others; linkage to medications for addiction therapy, connection to primary care and community supports and aftercare planning for individuals beginning to engage in recovery from addiction. Covered Individuals with Co-Occurring Disorders receive coordination of transportation and referrals to mental health providers to ensure treatment for their co-occurring psychiatric conditions. Pregnant women receive coordination of their obstetrical care.					
h. **Transitional Care Unit (TCU)** – a community based therapeutic program offering high levels of supervision, structure and intensity of service within an unlocked setting. The program serves children and adolescents, under age 19, who are in the custody of the Department of Children and Families (DCF), who have been determined to need group care or foster care and no longer meet the clinical criteria for continued stay at an acute level of care. The TCU offers comprehensive services, including but not limited to, a therapeutic milieu, psychiatry, aggressive case management, and multidisciplinary, multi-modal therapies.	✓	✓			
Residential Rehabilitation Services for Substance Use Disorders (Level 3.1)					

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
a. **Adult Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) -** 24-hour residential environment that provides a structured and comprehensive rehabilitative environment that supports each resident's independence and resilience and recovery from alcohol and/or other drug problems. Scheduled, goal-oriented rehabilitative services are provided in conjunction with ongoing support and assistance for developing and maintaining interpersonal skills necessary to achieve recovery. Members receive at least five hours of individual or group therapy each week in addition to case management, psychoeducation and milieu based rehabilitative activities. Residential programs licensed and approved to serve pregnant and post-partum women provide assessment and management of gynecological and/or obstetric and other prenatal needs, as well as treatment plans addressing parenting skills education, child development education, parent support, family planning, nutrition, as well as opportunities for parent/child relational and developmental groups. Covered Individuals with Co-Occurring Disorders receive coordination of transportation and referrals to mental health providers to ensure treatment for their co-occurring psychiatric conditions.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
b. Family Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) - 24-hour residential environment for families in which a parent has a substance use disorder and either is pregnant, has custody of at least one child or has a physical reunification plan with at least one child within 30 days of admission. Scheduled, goal-oriented rehabilitative services intended to support parents and children are provided in conjunction with ongoing support and assistance for developing and maintaining interpersonal and parenting skills necessary to achieve recovery and support family reunification and stability. Covered Individuals receive at least five hours of individual or group therapy each week in addition to case management, psychoeducation and milieu based rehabilitative activities.	✓	✓	✓		
c. Transitional Age Youth and Young Adult Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) - 24-hour developmentally appropriate residential environment designed specifically for either Transitional Age Youth ages 16-21 or Young Adults ages 18-25 that provides a structured and comprehensive rehabilitative environment that supports each resident's independence and resilience and recovery from alcohol and/or other drug problems. Scheduled, goal-oriented rehabilitative services are provided in conjunction with ongoing support and assistance for developing and maintaining interpersonal skills necessary to achieve recovery. Covered Individuals	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
receive at least five hours of individual or group therapy each week in addition to case management, psychoeducation and milieu based rehabilitative activities. Covered Individuals with Co-Occurring Disorders receive coordination of transportation and referrals to mental health providers to ensure treatment for their co-occurring psychiatric conditions.					
d. Youth Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) - 24-hour developmentally appropriate residential environment with enhanced staffing and support designed specifically for youth ages 13-17 that provides a structured and comprehensive rehabilitative environment that supports each resident's independence and resilience and recovery from alcohol and/or other drug problems. Scheduled, goal-oriented rehabilitative services are provided in conjunction with ongoing support and assistance for developing and maintaining interpersonal skills necessary to achieve recovery. Covered Individuals receive at least five hours of individual or group therapy each week in addition to case management, psychoeducation and milieu based rehabilitative activities. Covered Individuals with Co-Occurring Disorders receive coordination of transportation and referrals to mental health providers to ensure treatment for their co-occurring psychiatric conditions.	✓	✓			

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
e. **Co-Occurring Enhanced Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) -** 24-hour, safe, structured environment, located in the community, which supports Covered Individual's recovery from addiction and moderate to severe mental health conditions while reintegrating into the community and returning to social, vocation/employment, and/or educational roles. Scheduled, goal-oriented clinical services are provided in conjunction with psychiatry and medication management to support stabilization and development of skills necessary to achieve recovery. Clinical services are provided a minimum of five hours a week and additional outpatient levels of care may be accessed concurrently as appropriate. Programs will ensure that Members have access to prescribers of psychiatric and addiction medications.	✓	✓	✓		
f. Pregnancy Enhanced Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) - 24-hour developmentally appropriate residential environment designed specifically for people who are pregnant that provides a structured and comprehensive rehabilitative environment that supports each resident's independence and resilience and recovery from alcohol and/or other drug problems. Scheduled, goal-oriented rehabilitative services are provided in conjunction with ongoing support and assistance for developing and maintaining interpersonal skills necessary to achieve recovery. Members receive at least five hours of individual or group therapy each week in	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
addition to case management, psychoeducation and milieu based rehabilitative activities. Residential programs must provide assessment and management of gynecological and/or obstetric and other prenatal needs, as well as treatment plans addressing parenting skills education, child development education, parent support, family planning, nutrition, as well as opportunities for parent/child relational and developmental groups. This enhancement applies to Adult Residential Rehabilitation Services and Co-Occurring Enhanced Residential Rehabilitation Services.					
g. Postpartum Enhanced Residential Rehabilitation Services for Substance Use Disorders (Level 3.1) - 24-hour developmentally appropriate residential environment designed specifically for people who are postpartum up to 12 months inclusive of all pregnancy outcomes, that provides a structured and comprehensive rehabilitative environment that supports each resident's independence and resilience and recovery from alcohol and/or other drug problems. Scheduled, goal-oriented rehabilitative services are provided in conjunction with ongoing support and assistance for developing and maintaining interpersonal skills necessary to achieve recovery. Members receive at least five hours of individual or group therapy each week in addition to case management, psychoeducation and milieu based rehabilitative activities. Residential programs must provide assessment and management of gynecological and/or obstetric and other postpartum needs, as well as	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
treatment plans addressing parenting skills education, child development education, parent support, family planning, nutrition, as well as opportunities for parent/child relational and developmental groups. This enhancement applies to Adult Residential Rehabilitation Services and Co-Occurring Enhanced Residential Rehabilitation Services.					
Non-24-Hour Diversionary Services					
1. **Community Support Program (CSP) and Specialized CSP -** an array of services delivered by a community-based, mobile, multi-disciplinary team of professionals and paraprofessionals. These programs provide essential services to Covered Individuals with a long standing history of a psychiatric or substance use disorder and to their families, or to Covered Individuals who are at varying degrees of increased medical risk, or to children/adolescents who have behavioral health issues challenging their optimal level of functioning in the home/community setting for whom CBHI services are not appropriate. Services include outreach and supportive services, delivered in a community setting, which will vary with respect to hours, type and intensity of services depending on the changing needs of the Covered Individual. Specialized CSP programs serve populations with particular needs. **Specialized CSP Programs:** **a. CSP for Justice Involved –** a Specialized CSP service to address the health-related social needs of Covered Individuals with Justice Involvement who have a barrier to accessing or consistently utilizing medical and behavioral health services, as	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
defined by EOHHS. CSP-JI includes behavioral health and community tenure sustainment supports. **b. CSP for Homeless Individuals –** a Specialized CSP service to address the health-related social needs of Covered Individuals who (1) are experiencing Homelessness and are frequent users of acute health MassHealth services, as defined by EOHHS, or (2) are experiencing chronic homelessness, as defined by the US Department of Housing and Urban Development. **c. CSP – Tenancy Preservation Program -** a Specialized CSP service to address the health-related social needs of Covered Individuals who are At Risk of Homelessness and facing Eviction as a result of behavior related to a disability. CSP-TPP works with the member, the Housing Court, and the member's landlord to preserve tenancies by connecting the member to community-based services in order to address the underlying issues causing the lease violation. The primary goal of the CSP-TPP is to preserve the tenancy and the secondary goals are to put in place services that address those issues that put the Covered Individual's housing in jeopardy to ensure that the Covered Individual's housing remains stable.					
2. **Partial Hospitalization (PHP) –** an alternative to Inpatient Mental Health Services, PHP services offer short-term day mental health programming available seven days per week. These services consist of therapeutically intensive acute treatment within a stable therapeutic milieu and include daily psychiatric management.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
3. **Psychiatric Day Treatment –** services which constitute a program of a planned combination of diagnostic, treatment and rehabilitative services provided to a person with mental illness who needs more active or inclusive treatment than is typically available through a weekly visit to a mental health center, individual Provider's office or hospital outpatient department, but who does not need 24-hour hospitalization.	✓	✓	✓		
4. **Structured Outpatient Addiction Program (SOAP) –** clinically intensive, structured day and/or evening substance use disorder services. These programs can be utilized as a transition service in the continuum of care for a Covered Individual being discharged from Acute Substance Abuse Treatment, or can be utilized by individuals, who need Outpatient Services, but who also need more structured treatment for a substance use disorder without 24-hour monitoring. These programs incorporate the evidence-based practice of Motivational Interviewing into clinical programming to promote individualized treatment planning. **Specialized SOAP Services** **Enhanced Structured Outpatient Addiction Program (E-SOAP) -** specialized SOAP services and staffing for targeted populations including pregnant and postpartum Covered Individuals, adolescents and Covered Individuals who are experiencing homelessness or at risk of homelessness.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
5. **Intensive Outpatient Program (IOP) -** a clinically intensive service designed to improve functional status, provide stabilization in the community, divert an admission to an Inpatient Service, or facilitate a rapid and stable reintegration into the community following a discharge from an inpatient service. The IOP provides time-limited, comprehensive, and coordinated multidisciplinary treatment.	✓	✓	✓		
6. **Recovery Coaching –** a non-clinical service provided by individuals currently in recovery from a substance use disorder who have been certified as Recovery Coaches and who have been trained to help people with addiction gain hope, explore recovery and achieve life goals. The focus of the Recovery Coach role is to create a relationship between equals that is non-clinical and focused on removing obstacles to recovery; facilitate initiation and engagement to treatment and serve as a guide and motivating factor for the Covered Individual to maintain recovery and community tenure. **Specialized Recovery Coach Services** Effective September 1, 2025, Recovery Coach for Pregnant and Postpartum Members- A specialized peer recovery coach who provides non-clinical peer recovery supports to individual in or seeking recovery who are pregnant or have been pregnant in the last 12 months.	✓	✓	✓		
7. **Recovery Support Navigators (RSN) –** a specialized care coordination service intended to engage Covered Individuals with Substance Use Disorder in accessing and continuing Substance Use Disorder treatment. RSNs may be located in a variety of Substance Use Disorder treatment environments, as well as hospital medical	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
or surgical inpatient and emergency department settings, doing outreach and building relationships with individuals in programs, including withdrawal management and step-down services. If a **Covered Individual** accepts RSN services upon leaving a Substance Use Disorder treatment program, the RSN will work with the individual on accessing appropriate treatment and staying motivated for treatment and recovery. These services shall be provided in accordance with the Mass Health Acute Hospital Request for Applications (Acute Hospital RFA) when provided in hospital settings. **Specialized Recovery Support Navigators** Effective September 1, 2025, Recovery Support Navigator for Pregnant or Postpartum Members- A specialized Recovery Support Navigator that provides services to individuals who are pregnant or have been pregnant in the last 12 months.					
8. **Program of Assertive Community Treatment (PACT) –** a multi-disciplinary team approach to providing acute, active, ongoing, and long-term community-based psychiatric treatment, assertive outreach, rehabilitation and support. The program team provides assistance to Covered Individuals to maximize their recovery, ensure consumer-directed goal setting, assist individuals in gaining a sense of hope and empowerment, and provide assistance in helping the individuals served become better integrated into the community. Services are provided in the community and are available, as needed by the individual, 24 hours a day, seven days a week, 365 days a year. PACT includes PACT 50; PACT 80; and Forensic PACT.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
Outpatient Services - mental health and substance use disorder services provided in person in an ambulatory care setting such as a Community Behavioral Health Center (CBHC), mental health center or substance use disorder clinic, hospital outpatient department, community health center, or practitioner's office. The services may be provided at a Covered Individual's home or school.					
Standard outpatient Services – those Outpatient Services most often provided in an ambulatory setting.					
1. **Family Consultation -** a meeting of at least 15 minutes' duration, either in person or by telephone, with family members or others who are significant to the Covered Individual and clinically relevant to a Covered Individual's treatment to: identify and plan for additional services; coordinate a treatment plan; review the individual's progress; or revise the treatment plan, as required.	✓	✓	✓		
2. **Case Consultation -** an in-person or by telephone meeting of at least 15 minutes' duration, between the treating Provider and other behavioral health clinicians or the Covered Individual's primary care physician, concerning a Covered Individual who is a client of the Provider, to: identify and plan for additional services; coordinate a treatment plan; review the individual's progress; and revise the treatment plan, as required. Case Consultation shall not include clinical supervision or consultation with other clinicians within the same provider organization.	✓	✓	✓		
3. **Diagnostic Evaluation -** an assessment of an Covered Individual's level of functioning, including physical, psychological, social, educational and environmental strengths and challenges for the purpose of diagnosis and designing a treatment plan.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
4. **Psychiatric Consultation on an Inpatient Medical Unit -** an in-person meeting of at least 15 minutes' duration between a psychiatrist or Advanced Practice Registered Nurse Clinical Specialist and a Covered Individual at the request of the medical unit to assess the Covered Individual's mental status and consult on a behavioral health or psychopharmacological plan with the medical staff on the unit.	✓	✓	✓		
5. **Medication Visit -** an individual visit specifically for psychopharmacological evaluation, prescription, review, and/or monitoring by a psychiatrist or R.N. Clinical Specialist for efficacy and side effects.	✓	✓	✓		
6. **Medication Administration –** shall mean the injection of intramuscular psychotherapeutic medication by qualified personnel.	✓	✓	✓		
7. **Couples/Family Treatment -** the use of psychotherapeutic and counseling techniques in the treatment of a Covered Individual and his/her partner and/or family simultaneously in the same session.	✓	✓	✓		
8. **Group Treatment –** the use of psychotherapeutic or counseling techniques in the treatment of a group, most of whom are not related by blood, marriage, or legal guardianship. Group Treatment includes, but is not limited to, Dialectical Behavioral Therapy.	✓	✓	✓		
9. **Individual Treatment -** the use of psychotherapeutic or counseling techniques in the treatment of an individual on a one-to-one basis. Individual Treatment includes, but is not limited to, Dialectical Behavioral Therapy.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
10. **Inpatient-Outpatient Bridge Visit -** a single-session consultation conducted by an outpatient provider while a Covered Individual remains on an Inpatient psychiatric unit. The Inpatient-Outpatient Bridge Visit involves the outpatient Provider meeting with the Covered Individual and the inpatient team or designated inpatient treatment team clinician.	✓	✓	✓		
11. **Assessment for Safe and Appropriate Placement (ASAP) -** an assessment, required by MGL 119 Sec. 33B, conducted by a diagnostician with specialized training and experience in the evaluation and treatment of sexually abusive youth or arsonists, to evaluate individuals who are in the care and custody of DCF and who have been adjudicated delinquent for a sexual offense or the commission of arson, or have admitted to such behavior, or are the subject of a documented or substantiated report of such behavior, and who are being discharged from Inpatient Psychiatric Unit or Hospital or Community-Based Acute Treatment for Children/Adolescents or Intensive Community Based Acute Treatment for Children/Adolescents to a family home care setting. Services are provided through a contracted ASAP provider.	✓	✓			
12. **Collateral Contact –** a communication of at least 15 minutes' duration between a Provider and individuals who are involved in the care or treatment of a Covered Individual under 21 years of age, including, but not limited to, school and day care personnel, state agency staff, and human services agency staff.	✓	✓			

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
13. **Acupuncture Treatment -** the insertion of metal needles through the skin at certain points on the body, with or without the use of herbs, an electric current, heat to the needles or skin, or both, as an aid to persons who are withdrawing from dependence on substances or in recovery from addiction.	✓	✓	✓		
14. **Opioid Treatment Services —** supervised assessment and treatment of an individual, using FDA approved medications (including methadone, buprenorphine/naloxone, and naltrexone) along with a comprehensive range of medical and rehabilitative services, when clinically necessary, to alleviate the adverse medical, psychological or physical effects incident to opiate addiction. This term encompasses induction of Medication for Opioid Use Disorder (MOUD) detoxification treatment and maintenance treatment. MOUD services may also be provided by outpatient hospital emergency departments in accordance with the MassHealth Hospital Request for Applications (Acute Hospital RFA) as further specified by EOHHS.	✓	✓	✓		
15. **Ambulatory Withdrawal Management -** outpatient services for Members who are experiencing a serious episode of excessive substance use or withdrawal complications. Ambulatory Withdrawal Management is provided under the direction of a physician and is designed to stabilize the Member's medical condition under circumstances where neither life nor significant bodily functions are threatened. The severity of the individual's symptoms will determine the setting, as well as the amount of nursing and physician supervision necessary during the course of treatment.	✓	✓	✓		

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
16. **Psychological Testing -** the use of standardized test instruments to assess a Covered Individual's cognitive, emotional, neuropsychological, verbal, and defensive functioning on the central assumption that individuals have identifiable and measurable differences that can be elicited by means of objective testing. See 130 CMR 411.000.	✓	✓	✓		
17. **Applied Behavior Analysis for members under 21 years of age (ABA Services) –** a MassHealth service that focuses on the analysis, design, implementation, and evaluation of social and other environmental modifications to produce meaningful changes in human behavior. This service provides for the performance of behavioral assessments; interpretation of behavior analytic data; development of a highly specific treatment plan; supervision and coordination of interventions; and training other interveners to address specific objectives or performance goals in order to treat challenging behaviors that interfere with a youth's successful functioning. See 101 CMR 358.00.	✓	✓			
18. **Early Intensive Behavioral Intervention (EIBI) –** a service provided to children under three years of age who have a diagnosis of autism spectrum disorder (ASD) and meet clinical eligibility criteria. Such services shall be provided only by DPH-approved, Early Intensive Behavioral Intervention Service Providers.	✓	✓			
19. **Preventive Behavioral Health Services -** short-term interventions in supportive group, individual, or family settings, recommended by a physician or other licensed practitioner, practicing within their scope of licensure, that cultivate coping skills and strategies for symptoms of depression, anxiety, and other social/emotional	✓	✓			

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
concerns, which may prevent the development of behavioral health conditions for members who are under 21 years old who have a positive behavioral health screen (or, in the case of an infant, a caregiver with a positive post-partum depression screening), even if the member does not meet criteria for behavioral health diagnosis. Preventive behavioral health services are available in group sessions when delivered in community-based outpatient settings, and in individual, family, and group sessions when provided by a behavioral health clinician practicing in an integrated pediatric primary care setting.					
20. **Certified Peer Specialist (CPS) –** A service utilizing peers with lived experience in sustained recovery and wellness while living with mental health conditions and trauma to promote member's empowerment, self-determination, self-advocacy and resiliency. CPSs, employed by CBHCs and CMHCs, are specially trained and certified to support members in their goals and empower their decision making regarding their recovery.	✓	✓	✓		
Intensive Home or Community-Based Services for Youth – mental health and substance use disorder services provided to Covered Individuals in a community-based setting such as home, school, or community service agency. The services provided are more intensive than services that may be provided through a standard outpatient service. **(See detailed services below)**					
1. **Family-based Intensive Treatment –** Effective October 1, 2025, a service for individuals younger than 21 years of age with serious emotional disturbance to maintain the youth at home safely and support outpatient and community-based levels of care. The services include assessment of the members, development and review of an individualized treatment plan, development and review of safety or crisis planning tools, intensive therapeutic	✓				

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
interventions for the youth and family, referral and coordination of other services and supports, skills training, and coaching. Family-based intensive treatment is provided by eligible providers using a team-based approach.					
2. **Family Support and Training –** a service provided to the parent /caregiver of a youth (under the age of 21), in any setting where the youth reside, such as the home and other community settings. Family Support and Training is a service that provides a structured, one-to-one, strength-based relationship between a Family Support and Training staff and a parent/caregiver. The purpose of this service is for resolving or ameliorating the youth's emotional and behavioral needs by improving the capacity of the parent /caregiver to parent the youth so as to improve the youth's functioning. Services may include education, assistance in navigating the youth serving systems; fostering empowerment, including linkages to peer/parent support and self-help groups; assistance in identifying formal and community resources, support, coaching, and training for the parent/caregiver.	✓				
3. **Intensive Care Coordination –** a service that provides targeted case management services to individuals under 21 with a Serious Emotional Disturbance including individuals with co-occurring conditions. This service includes assessment, development of an individualized care plan, referral and related activities to implement the care plan and monitoring of the care plan.	✓				

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
4. **In-Home Behavioral Services –** this service usually includes a combination of behavior management therapy and behavior management monitoring, as follows: a. **Behavior Management Therapy** – This service includes assessment, development of the behavior plan, and supervision and coordination of interventions to address specific behavioral objectives or performance. This service addresses challenging behaviors which interfere with the youth's successful functioning. The Behavior management therapist develops and monitors specific behavioral objectives and interventions, including a crisis-response strategy, that are incorporated into the youth's treatment plan. The therapist may also provide short-term counseling and assistance, depending on the youth's performance and level of intervention required. Phone contact and consultation may be provided as part of the intervention. b. **Behavior Management Monitoring –** This service includes implementation of the behavior plan, monitoring the youth's behavior, reinforcing implementation of the plan by parents or other caregivers and reporting to the behavior management therapist on implementation of the plan and progress toward behavioral objectives or performance goals. Phone contact and consultation may be provided as part of the intervention.	✓				

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
5. **In-Home Therapy Services -** This service is a therapeutic clinical intervention and ongoing training and therapeutic support, as follows: a. **The Therapeutic Clinical Intervention** is a structured, consistent, therapeutic relationship between a licensed clinician and the youth and family for the purpose of treating the youth's mental health needs including improving the family's ability to provide effective support for the youth to promote healthy functioning of the youth within the family. The clinician develops a treatment plan and, using established psychotherapeutic techniques, works with the entire family or a subset of the family, to enhance problem-solving, limit-setting, communication, emotional support or other family or individual functions. The Therapeutic Clinical Intervention is provided by a qualified licensed clinician who will often work in a team that includes one or more qualified paraprofessionals. b. **Ongoing Therapeutic Training and Support** is a service provided by a paraprofessional to support implementation of the licensed clinician's treatment plan to achieve the goals of the treatment plan. The paraprofessional assists a licensed clinician in implementing the therapeutic objectives of the treatment plan designed to address the youth's mental health and emotional challenges. This service includes teaching the youth to understand, direct, interpret, manage and control feelings and emotional responses to situations, and to assist the family in	✓	✓			

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
supporting the youth in addressing his or her emotional and mental health needs. Phone contact and consultation may be provided as part of the intervention.					
6. **Therapeutic Mentoring Services -** this service provides a structured, one-to-one mentoring relationship between a therapeutic mentor and a youth for the purpose of addressing daily living, social and communication needs. Each youth will have goals and objectives that are designed to support age-appropriate social functioning or ameliorate deficits in the youth's age-appropriate social functioning. These goals and objectives are developed by the youth, as appropriate, and his/her treatment team and are incorporated into the treatment plan. The service includes supporting, coaching and training the youth in age-appropriate behaviors, interpersonal communication, problem-solving and conflict resolution and relating appropriately to other youths, as well as adults, in recreational and social activities. The therapeutic mentor works with the youth in such settings as their home, school or social or recreational activities.	✓				
Crisis Services - Crisis Services are available seven days per week, 24 hours per day to provide treatment of any individual who is experiencing a mental health crisis. **(See detailed services below)**					

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
1. **Adult Mobile Crisis Intervention (AMCI) -** a short-term mobile, on-site, face-to-face therapeutic service provided for members 21 years of age or older experiencing a behavioral health crisis and for the purpose of identifying, assessing, treating, and stabilizing the situation and reducing the immediate risk of danger to the member or others consistent with the member's risk management/safety plan, if any. Services are available 24 hours a day, seven days a week. AMCI shall include at a minimum: crisis assessment, intervention and stabilization. a. **Assessment** - a face-to-face evaluation of an individual presenting with a behavioral health emergency, including assessment of the need for hospitalization, conducted by appropriate clinical personnel; b. **Intervention** –the provision of psychotherapeutic and crisis counseling services to an individual for the purpose of stabilizing an emergency; and c. **Stabilization** – short-term behavioral health treatment in a structured environment with continuous observation and supervision of individuals who do not require hospital level of care. In addition, medication evaluation and specialing services shall be provided if Medically Necessary.	✓	✓	✓	✓	✓ **(initial crisis encounter only)**

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
2. **Youth Mobile Crisis Intervention (YMCI) -** a short term mobile, on-site, and face-to-face therapeutic service provided for youth experiencing a behavioral health crisis and for the purpose of identifying, assessing, treating, and stabilizing the situation and reducing the immediate risk of danger to the youth or others consistent with the youth's risk management/safety plan, if any. Services are available 24 hours a day, 7 days a week.	✓	✓		✓	✓ **(initial crisis encounter only)**
3. **Behavioral Health Crisis Evaluation Services in Acute Medical Setting** - Crisis evaluations provided in medical and surgical inpatient and emergency department settings include the crisis assessment, crisis interventions, and disposition coordination and reporting and community collaboration activities for members presenting to the ED in a behavioral health crisis. Elements of crisis evaluations include**:** a. **Comprehensive Behavioral Health Crisis Assessment –** Behavioral Health crisis assessment by a qualified behavioral health professional to individuals within 60 minutes of time of the member's readiness to receive such an assessment. Behavioral Health Crisis Evaluation team must include: qualified behavioral health professional, a complex behavioral health care clinician, and other master's and bachelor's-level clinicians and staff sufficient to meet the needs of members served which may include certified peer specialists and recovery coaches. b. **Crisis Interventions –** Observation, treatment, and support to individuals experiencing a behavioral health crisis.	✓	✓	✓	✓	

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
c. **Discharge Planning and Care Coordination –** A disposition plan that includes discharge planning to identify and secure an appropriate level of care and goals for that level of care. d. **Reporting and Community Collaboration –** Required reporting of individuals awaiting inpatient psychiatric hospitalization and the establishment of referral relationships with community providers. These services shall be provided in accordance with the Acute Hospital RFA.					
4. **Behavioral Health Crisis Management Services in Acute Medical Settings -** crisis management services provided in medical and surgical inpatient and emergency department settings include ongoing crisis interventions, ongoing determination and coordination of appropriate disposition, and ongoing required reporting and community collaboration activities. Elements of crisis management include: a. **Crisis Interventions –** Observation, treatment, and support to individuals experiencing a behavioral health crisis. b. **Discharge Planning and Care Coordination –** A disposition plan that includes discharge planning to identify and secure an appropriate level of care and goals for that level of care. c. Ongoing required reporting and community collaboration These services shall be provided in accordance with the Acute Hospital RFA.	✓	✓	✓	✓	
Other Behavioral Health Services - Behavioral Health Services that may be provided as part of treatment in more than one setting type.					

Service	Coverage Types				
	MassHealth Standard & CommonHealth Covered Individuals	MassHealth Family Assistance Covered Individuals	CarePlus Covered Individuals	Uninsured Individuals, and Persons Covered by Medicare Only	Individuals without Mobile Crisis Coverage
Electro-Convulsive Therapy (ECT) - a therapeutic service which initiates seizure activity with an electric impulse while the individual is under anesthesia. It is administered in a facility that is licensed to provide this service by DMH.	✓	✓	✓		
Repetitive Transcranial Magnetic Stimulation (rTMS) - a noninvasive form of neurostimulation in which rapidly changing magnetic fields are applied to the surface of the scalp through a copper wire coil connected to a magnetic stimulator. The therapeutic service is used to treat depression that has not responded to standard treatment such as medications and psychotherapy.	✓	✓	✓		
Specialing - therapeutic services provided to a Covered Individual in a variety of 24-hour settings, on a one-to-one basis, to maintain the individual's safety.	✓	✓	✓		

APPENDIX A-2
Required Network Provider Lists

Exhibit 1: Community Behavioral Health Center (CBHC) List

CBHC	CATCHMENT AREA
North Suffolk Mental Health Association	Greater Boston
Cambridge Health Alliance	Boston/Cambridge
Cambridge Health Alliance	Malden/Medford/Revere
Boston Medical Center	Boston/Brookline
Riverside Community Care	Norwood
Aspire Health Alliance	South Shore
The Brien Center	Berkshires
Clinical Support Options	Greenfield
Clinical Support Options	Northampton
Behavioral Health Network (BHN)	Southern Pioneer
Center for Human Development	Southern Pioneer
Advocates	Metrowest
Clinical Support Options	North County
Community Healthlink	North County
Riverside Community Care	South County
Community Healthlink	Worcester
Eliot Community Health Services	North Essex
Beth Israel Lahey Behavioral Services	Lawrence
Vinfen	Lowell
Eliot Community Health Services	Tri-city
Child and Family Services	Southern Coast

CBHC	CATCHMENT AREA
High Point Treatment Center	Brockton
Bay Cove Human Services	Cape Cod
Fairwinds- Nantucket's Counseling Center	Nantucket
Child and Family Services	Fall River
Community Counseling of Bristol County	Taunton Attleboro

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Exhibit 2: State-Operated Community Mental Health Centers (SOCMHCs)

Brockton Multi-Service Center 165 Quincy Street Brockton, MA 02402
John C. Corrigan Mental Health Center 49 Hillside Street Fall River, MA 02729
Mass. Mental Health Center 75 Fenwood Road Boston, MA 02115
Pocasset Mental Health Center 830 Country Road Pocasset, MA 02559

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Exhibit 3: State Operated Facilities Providing Inpatient Mental Health Services, Outpatient Behavioral Health Services, and Diversionary Behavioral Health Services

Type of Service/Appendix C Category	Provider Name	Location	NPI	Claim Form[1]	Service
Hospital Based Services	Cape Cod and Islands Mental Health Center	Pocasset	1851477491	UB04	Inpatient Services
Hospital Based Services	Corrigan Mental Health Center	Fall River	1700964947	UB04	Inpatient Services
Hospital Based Services	Corrigan Mental Health Center	Fall River	1194803288	UB04	Outpatient Services*
Hospital Based Services	Cape Cod and Islands Mental Health Center	Pocasset	1851477491	1500	Professional Services
Hospital Based Services	Corrigan Mental Health Center	Fall River	1700964947	1500	Professional Services
Diversionary Services	Substance Abuse Program "WRAP"	Taunton	1508212416	1500	Acute Treatment Services
Diversionary Services	Substance Abuse Program "WRAP"	Taunton	1508212416	1500	Clinical Support Services
Clinic services	Brockton Multi-Service Center	Brockton	1326155458	1500	Clinic
Clinic services	Mass Mental Health Center	Boston	1073638805	1500	Clinic

[REMAINDER OF PAGE INTENTIONALLY BLANK]

[1] Professional services are also billed for these programs on a 1500 claim form.

Exhibit 4: [Reserved]

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Exhibit 5: [Reserved]

Exhibit 6: Providers of Psychiatric Inpatient Child Services and Psychiatric Inpatient Adolescent Services List

Hospital Name	Address	Psychiatric Inpatient Child Provider	Psychiatric Inpatient Adolescent Provider
Arbour Hospital	49 Robinwood Ave Jamaica Plain, MA 02130		✓
Beverly Hospital	85 Herrick Street Beverly, MA 01915	✓	✓
Boston Children's Hospital	300 Longwood Avenue Boston, MA 02115	✓	✓
Boston Children's Hospital - Waltham	9 Hope Avenue Waltham, MA 02454	✓	✓
Bournewood Health Systems	300 South Street Brookline, MA 02467		✓
CHA Somerville Campus	230 Highland Avenue Somerville, MA 02143	✓	✓
Franciscan Children's	30 Warren Street Brighton, MA 02135	✓	✓
Fuller Hospital	200 May Street South Attleboro, MA 02703		✓
Hospital for Behavioral Medicine	100 Century Drive Worcester, MA 01606	✓	✓
McLean Southeast at Oak Street	52 Oak Street Middleborough, MA 02346		✓
MetroWest Medical Center - Leonard Morse Hospital	67 Union Street Natick, MA 01760-6089	✓	✓
MiraVista Behavioral Health Center	1233 Main Street Holyoke, MA 01040		✓
Monte Nido Walden	10 Carematrix Drive Dedham, MA 02026		✓
Pembroke Hospital	199 Oak Street Pembroke, MA 02359		✓
Southcoast Behavioral Health	581 Faunce Corner Road N. Dartmouth, MA 02714	✓	✓
Salem Hospital	81 Highland Avenue Salem, MA 01970	✓	✓
TaraVista Behavioral Health Center	85 Patton Road Devens, MA 01434		✓
Valley Springs Behavioral Health Hospital	45 Lower Westfield Road Holyoke, MA 01040	✓	✓
Westborough Behavioral Healthcare Hospital	300 Friberg Parkway Westborough, MA 01581	✓	✓

Exhibit 7: Providers of Inpatient Substance Use Disorder Services (Level 4) List

Program Name	Address
Adcare Hospital of Worcester, Inc.	107 Lincoln Street Worcester, MA 01605
Faulkner - Addiction Recovery Program Inpatient	1153 Centre Street 6-North Boston, MA 02130
Harrington Healthcare Co-Occurring Disorders Unit	340 Thompson Road Webster, MA 01570
McLean Hospital HCQ	115 Mill Street Belmont, MA 02478
Boston Medical Center (BMC) – Brighton	736 Cambridge St., CCP 10 Boston, MA 02135

Exhibit 8: Providers of Individualized Treatment Services and Youth Withdrawal Management and Stabilization Services List

Program Name	Address
Providers of Individualized Treatment Services	
Recovery Centers of America at Danvers	75 Lindal St Danvers, MA 01923
New View (Behavioral Health Network)	21 Kenwood St Greenfield, MA 01301
Recovery From Addictions Program (DMH)	60 Hodges St Taunton, MA 02780
High Point Treatment Inc	108 North Front Street New Bedford, MA 02740 10 Meadowbrook Rd. Brockton MA 02301 1223 State Rd. Plymouth MA 02360
Providers of Youth Withdrawal Management and Stabilization Services	
Southcoast Behavioral Health	581 Faunce Corner Road Dartmouth, MA 02747

Exhibit 9: Community Service Agency (CSA) Provider List

COMMUNITY SERVICE AGENCY	CATCHMENT AREA(s): CITY/TOWN
Bay State Community Services (Braintree) 400 Washington Street, Suite 106 Braintree, MA 02184	Braintree; Cohasset; Hingham; Hull; Milton; Norwell; Quincy; Randolph; Scituate; Weymouth
Bay State Community Services (Plymouth) 430 Court Street, Suite 3 Plymouth, MA 02360	Acushnet; Carver; Dartmouth; Duxbury; Fairhaven; Halifax; Hanover; Hanson; Kingston; Marion; Marshfield; Mattapoisett; New Bedford; Pembroke; Plymouth; Plympton; Rochester; Wareham
Behavioral Health Network (Leominster) 40 Spruce Street Leominster, MA 01453	Ashby; Ayer; Barre; Berlin; Bolton; Clinton; Fitchburg; Groton; Hardwick; Harvard; Lancaster; Leominster; Lunenburg; New Braintree; Oakham; Pepperell; Princeton; Rutland; Shirley; Sterling; Townsend
Behavioral Health Network (Springfield) 395 Liberty Street Springfield, MA 01104	Agawam; Blandford; Chester; East Longmeadow; Granville; Hampden; Huntington; Indian Orchard; Longmeadow; Montgomery; Russell; Southwick; Springfield; Tolland; Westfield; West Springfield; Wilbraham
Behavioral Health Network (Ware) 82 Main Street Ware, MA 01082	Belchertown; Bondsville; Chicopee; Granby; Holyoke; Ludlow; Monson; Palmer; South Hadley; Southampton; Thorndike; Three Rivers; Ware
Behavioral Health Network (Worcester) 335 Chandler Street Worcester, MA 01602	Auburn; Boylston; Grafton; Holden; Leicester; Millbury; Paxton; Shrewsbury; Spencer; West Boylston; Worcester
The Brien Center 66 West Street, Suite L2 Pittsfield, MA 01201	Adams; Alford; Becket; Cheshire; Clarksburg; Dalton; Egrement; Florida; Great Barrington; Hancock; Hinsdale; Lanesboro; Lee; Lenox; Monroe; Monterey; Mount Washington; New Ashford; New Marlboro; North Adams; Otis; Peru; Pittsfield; Richmond; Sandisfield; Savoy; Sheffield; Stockbridge; Tyringham; Washington; West Stockbridge; Williamstown; Windsor
Brockton Area Multi-Services, Inc. (BAMSI) 300 Battles Street Brockton, MA 02301	Abington; Avon; Bridgewater; Brockton; East Bridgewater; Easton; Holbrook; Rockland; Stoughton; West Bridgewater; Whitman
Child & Family Services (Fall River) 160 Osborn Street Fall River, MA 02724	Fall River; Freetown; Somerset; Swansea; Westport
Child & Family Services (New Bedford) 3057 Acushnet Avenue New Bedford, MA 02745	Acushnet; Carver; Dartmouth; Duxbury; Fairhaven; Halifax; Hanover; Hanson; Kingston; Marion; Marshfield; Mattapoisett; New Bedford; Pembroke; Plymouth; Plympton; Rochester; Wareham
Children's Services of Roxbury 520 Dudley Street Roxbury, MA 02119	Boston; Dorchester; South Boston; Roxbury; West Roxbury; Jamaica Plain; Mattapan; Roslindale; Hyde Park; Lower Mills; Brighton; Brookline

COMMUNITY SERVICE AGENCY	CATCHMENT AREA(s): CITY/TOWN
Clinical & Support Options (Gardener) 205 School Street, Suite 301 Gardner, MA 01440	Ashburnham; Gardner; Hubbardston; Templeton; Westminster; Winchendon
Clinical & Support Options (Greenfield) One Arch Place Greenfield, MA 01301	Ashfield; Athol; Bernardston; Buckland; Charlemont; Colrain; Conway; Deerfield; Erving; Gill; Greenfield; Hawley; Heath; Leverett; Leyden; Millers Falls; Montague; New Salem; Northfield; Orange; Petersham; Phillipston; Rowe; Royalston; Shelburne; Shutesbury; Sunderland; Turners Falls; Warwick; Wendell; Whately
Clinical & Support Options (Northampton) 8 Atwood Drive Northampton, MA 01062	Amherst; Chesterfield; Cummington; Easthampton; Florence; Goshen; Hadley; Hatfield; Middlefield; Northampton; Pelham; Plainfield; Westhampton; Williamsburg; Worthington
Clinical & Support Options (Pittsfield) 877 South Street Pittsfield, MA 01201	Adams; Alford; Becket; Cheshire; Clarksburg; Dalton; Egrement; Florida; Great Barrington; Hancock; Hinsdale; Lanesboro; Lee; Lenox; Monroe; Monterey; Mount Washington; New Ashford; New Marlboro; North Adams; Otis; Peru; Pittsfield; Richmond; Sandisfield; Savoy; Sheffield; Stockbridge; Tyringham; Washington; West Stockbridge; Williamstown; Windsor
Eliot Community Human Services (Danvers) 75 Sylvan Street Danvers, MA 01923	Amesbury; Beverly; Boxford; Danvers; Essex; Georgetown; Gloucester; Groveland; Hamilton; Haverhill; Ipswich; Manchester by the Sea; Marblehead; Merrimac; Middleton; Newbury; Newburyport; Peabody; Rockport; Rowley; Salisbury; Topsfield; Wenham; West Newbury
Eliot Community Human Services (Saugus) 1711 Broadway Saugus, MA 01906	Lynn; Lynnfield; Melrose; Nahant; North Reading; Reading; Salem; Saugus; Stoneham; Swampscott; Wakefield
Gandara 80 Commercial Street Holyoke, MA 01040	Statewide Specialty
The Home for Little Wanderers (Chelsea) 95 4th Street Chelsea, MA 02150	Chelsea; Revere; East Boston; Winthrop; Charlestown
The Home for Little Wanderers (Roslindale) 780 American Legion Hwy Roslindale, MA 02131	Boston; Dorchester; South Boston; Roxbury; West Roxbury; Jamaica Plain; Mattapan; Roslindale; Hyde Park; Lower Mills; Brighton; Brookline
The Home for Little Wanderers (Somerville) 17 Inner Belt Road Somerville, MA 02143	Cambridge; Somerville
Justice Resource Institute (Gloucester) 3 Blackburn Center Gloucester, MA 01930	Amesbury; Beverly; Boxford; Danvers; Essex; Georgetown; Gloucester; Groveland; Hamilton; Haverhill; Ipswich; Manchester by the Sea; Marblehead; Merrimac; Middleton; Newbury;

COMMUNITY SERVICE AGENCY	CATCHMENT AREA(s): CITY/TOWN
	Newburyport; Peabody; Rockport; Rowley; Salisbury; Topsfield; Wenham; West Newbury
Justice Resource Institute (Jamaica Plain) 3313 Washington Street Jamaica Plain, MA 02130	Boston; Dorchester; South Boston; Roxbury; West Roxbury; Jamaica Plain; Mattapan; Roslindale; Hyde Park; Lower Mills; Brighton; Brookline
Justice Resource Institute (Lawrence) 15 Union Street, Suite 215 Lawrence, MA 01840	Andover; Lawrence; Methuen; North Andover
Justice Resource Institute (Nantucket) 19 Old South Road Nantucket, MA 02554	Nantucket
Justice Resource Institute (Taunton) 35 Summer Street, Suite 104 Taunton, MA 02360	Attleboro; Berkley; Dighton; Lakeville; Mansfield; Middleborough; North Attleboro; Norton; Raynham; Rehoboth; Seekonk; Taunton
Justice Resource Institute (Yarmouthport) 221 Willow Street, 2nd Floor Yarmouthport, MA 02780	Barnstable; Bourne; Brewster; Chatham; Chilmark; Cotuit; Dennis; Eastham; Falmouth; Harwich; Hyannis; Mashpee; Orleans; Osterville; Provincetown; Sandwich; Truro; Wellfleet; Woods Hole; Yarmouth
Justice Resource Institute (Yarmouthport) 221 Willow Street, 2nd Floor Yarmouthport, MA 02780	Martha's Vineyard
The Learning Center for the Deaf, Walden Community Services 848 Central Street Framingham, MA 01701	Statewide Specialty
LUK, inc. (Fitchburg) 545 Westminster Street Fitchburg, MA 01420	Ashby; Ayer; Barre; Berlin; Bolton; Clinton; Fitchburg; Groton; Hardwick; Harvard; Lancaster; Leominster; Lunenburg; New Braintree; Oakham; Pepperell; Princeton; Rutland; Shirley; Sterling; Townsend
LUK, inc. (Worcester) 40 Southbridge Street Worcester, MA 01608	Auburn; Boylston; Grafton; Holden; Leicester; Millbury; Paxton; Shrewsbury; Spencer; West Boylston; Worcester
North Suffolk Community Services 265 Beach Street Revere, MA 02150	Everett; Malden; Medford
Riverside Community Care 237 Highland Ave Needham, MA 02494	Canton; Dedham; Dover; Foxboro; Medfield; Millis; Needham; Newton; Norfolk; Norwood; Plainville; Sharon; Walpole; Wellesley; Weston; Westwood; Wrentham
Wayside Youth & Family Support Network (Framingham) 88 Lincoln Street Framingham, MA 01701	Acton; Ashland; Arlington; Bedford; Belmont; Boxborough; Burlington; Carlisle; Concord; Framingham; Holliston; Hopkinton; Hudson; Lexington; Lincoln; Littleton; Maynard; Marlborough; Natick; Northborough; Sherborn;

COMMUNITY SERVICE AGENCY	CATCHMENT AREA(s): CITY/TOWN
	Southborough; Stow; Sudbury; Waltham; Watertown; Wayland; Westborough; Wilmington; Winchester; Woburn
Wayside Youth & Family Support Network (Lowell) 73 East Merrimack Street Lowell, MA 01852	Billerica; Chelmsford; Dracut; Dunstable; Lowell; Tewksbury; Tyngsboro; Westford
Wayside Youth & Family Support Network (Milford) 10 Asylum Street Milford, MA 01757	Bellingham; Blackstone; Brimfield; Brookfield; Charlton; Douglas; Dudley; East Brookfield; Franklin; Holland; Hopedale; Medway; Mendon; Milford; Millville; Northbridge; North Brookfield; Oxford; Southbridge; Sturbridge; Sutton; Upton; Uxbridge; Wales; Warren; Webster; West Brookfield

APPENDIX B-1
CONTRACT IMPLEMENTATION, READINESS REVIEW REQUIREMENTS AND DELIVERABLES

The Contractor will work with EOHHS during the transition and readiness review period.

The Contractor must provide a corrective action plan in response to any readiness review deficiency no later than 10 calendar days after notification of any such deficiency by EOHHS unless the Contractor documents to EOHHS' satisfaction that the deficiency has been corrected within 10 calendar days of notification of the deficiency.

In the event that the Contractor fails to submit all deliverables in accordance with the milestones and timeframes required by EOHHS or does not fully meet readiness review requirements established by EOHHS, EOHHS may, at its discretion, postpone the Contract Operational Start Date. EOHHS may also impose sanctions in accordance with the Contract for each day beyond January 1, 2023, that the Contractor is not operational.

The following table identifies specific readiness review requirements.

All Deliverables shall be provided in a format required or approved by EOHHS. EOHHS reserves the right to update this Appendix to delineate additional deliverables for the Contractor prior to the Operational Start Date. The Contractor shall refer to **Appendix E-1** for ongoing deliverables.

CONTRACT IMPLEMENTATION AND READINESS REVIEW DELIVERABLES

Operational Readiness Requirement	Contract Section	Due Date
Administration and Contract Management		
1. Designate and identify Key Personnel pursuant to Section 2.3.A.3. Provide résumés of each Key Personnel and the percent of allocated time each Key Personnel is dedicated to the Contract.	**2.3.A.3**	No later than the Operational Start Date. Additionally, the Contractor must notify EOHHS within five (5) business days of learning that any Key Personnel position is or will be vacant.
2. Submit a plan and description for training staff on contractual, state, and federal requirements specific to individual job functions required by this Contract.	**2.3.A.4**	No later than 30 days after the Operational Start Date.
3. Provide plan for Advisory Committees and Councils pursuant to Section 2.3.B.	**2.3.B**	No later than 30 days after the Operational Start Date
4. Submit policies and procedures for network management and oversight of Community Behavioral Health Centers (CBHCs) and Behavioral Health Urgent Care providers .	**2.3.D.1**	No later than the Operational Start Date
5. Provide all documentation required in Appendix B-2: Material Subcontractor Checklist for each new Material Subcontractor.	**2.3.D.2**	No later than the Operational Start Date or the date the Contractor expects to initially execute Material Subcontract, whichever is later.
6. Submit a compliance plan designed to guard against fraud, waste and abuse in accordance with 42 CFR 438.608.	**2.3.D.3.b**	No later than 30 days after the Operational Start Date
7. Submit an anti-fraud, waste, and abuse plan to detect and prevent fraud and abuse by Network Providers and Covered Individuals.	**2.3.D.3.c**	No later than 30 days after the Operational Start Date
Enrollment and Education Activities		
8. Submit plan for conducting Enrollee outreach, orientation and education.	**2.4.C**	No later than the Operational Start Date
9. Submit orientation and outreach materials and phone scripts.	**2.4.C**	No later than 30 days after the Operational Start Date
Care Delivery, Care Coordination, and Care Management		
10. Submit work plan for Integrated Care Management and Practice Based Care Management Programs.	**2.5.C**	No later than the Operational Start Date
11. Submit plan to support EOHHS' efforts to reduce the number of and time spent by Covered Individuals awaiting disposition in Emergency Departments.	**2.5.K**	No later than the Operational Start Date.
Covered Services		
12. Submit plan for providing utilization management services	**2.6.C**	No later than 30 days after the Operational Start Date

Operational Readiness Requirement	Contract Section	Due Date
Provider Contracts and Related Responsibilities		
13. Submit Network Provider directory website link	**2.7.G**	No later than 30 days after the Operational Start Date.
14. Submit the names, titles, roles, contact information, percent of FTE time, and role functions for those staff dedicated to support the CBHC system and Behavioral Health Urgent Care once fully operational.	**2.7.H**	No later than the Operational Start Date
15. Submit a readiness plan to oversee compliance with the program specifications of the new CBHC model of care	**2.7.H.8**	No later than the Operational Start Date
Provider Network and Network Management		
16. Submit updates to Provider Network list, if any.	**2.8.A.4**	No later than 30 days after the Operational Start Date.
17. Submit template of provider agreements that include provisions specified in the Contract.	**2.8.A, 2.8.F**	No later than 30 days after the Operational Start Date
18. Submit Network Provider policies and procedures manual, including credentialing criteria and waiver processes for credentialing criteria.	**2.8.D**	No later than 30 days after the Operational Start Date
Covered Individual Services		
19. Submit Covered Individual handbook for EOHHS approval if changed since most recent submission.	**2.10.A.3**	No later than 30 days after the Operational Start Date.
Inquiries, Ombudsman Services, Grievances, and Appeals		
20. Submit policies and procedures for the filling by Covered Individuals or Appeals representatives and the receipt, timely resolution, and documentation by the Contractor for any and all Grievances and Internal Appeals	**2.12.B**	No later than the Operational Start Date
Quality Management and Quality Improvement		
21. Submit current description of Quality Management/Quality Improvement (QM/QI) program that delineates structure, goals and objectives of Contractor's QM/QI initiatives.	**2.13.B.4**	No later than the Operational Start Date.
Data Management, Information Systems, and Reporting Requirements		
22. Demonstrate capability to accept all Contract-related files and data delivered by EOHHS in the format specified by	**2.14.A**	No later than the Operational Start Date

Operational Readiness Requirement	Contract Section	Due Date
EOHHS.		
23. Demonstrate compliance with Information System Design Requirements detailed in Section 2.14.F.	**2.14.F**	No later than the Operational Start Date
24. Submit plan, policies, and procedures for training, staffing, and maintaining all toll-free service call centers, in accordance with the Contract. At a minimum, documentation should include: 1) plan for ensuring sufficient capacity to handle incoming calls, 2) contingency plan to address overflow calls and maintain call center access standards set forth in the Contract and 3) specific training and staffing to support 24-7 toll-free crisis response line to respond to behavioral health care service needs.	**2.14.J**	No later than 30 days after the Operational Start Date.
Third-Party Liability Benefit Coordination		
25. Submit work plan for Third Party Liability benefit coordination and recovery.	**2.18.A**	No later than the Operational Start Date.
PCC Plan Management Support		
26. Submit operating policies and procedures for the PCC Plan Management Support Services program	**2.19.A**	No later than 30 days after the Operational Start Date

APPENDIX B-2
MATERIAL SUBCONTRACTOR CHECKLIST

Below is a list of questions related to [***insert name of MCE***]'s preparedness for entering into a contract with a Material Subcontractor [***Insert name and type of subcontractor***]. The Contractor shall provide a written response to these questions as soon as possible, but no later than 60 days prior to implementation.

Name of MCE:

Date of Submission:

SECTION 1.
Please answer all questions completely.

GENERAL INFORMATION

1. What is the name of the Material Subcontractor?
2. What is the type and scope of service to be provided by the Subcontractor (e.g., claims processing, care management,)?
3. What is the expected effective date of the Subcontract?
4. What is the expected date on which the Subcontractor will begin to deliver services, if different from the expected effective date of the Subcontract (due to ramp up time or other implementation factors)?
5. What are the key reasons for choosing to contract with Subcontractor to perform these activities?
6. What are the key reasons for selection of this Subcontractor?
7. What are the primary services that this Subcontractor will perform, including the business functions, and/or the range of health conditions on which this Subcontractor will focus?
8. What specific services will the Subcontractor provide that the MCE is not able to provide? If comparable services are to be provided by the MCE, how will the services provided by this Subcontractor differ from those provided by MCE and why are such redundancies necessary?
9. Confirm that the MCE has ensured and explain how the MCE has ensured that the Subcontractor is financially sound.

SUBCONTRACTOR REIMBURSEMENT

10. How will the Subcontractor be reimbursed? If reimbursement is on a PMPM, will the reimbursement be based on enrollees referred or enrollees served? If based on enrollees served, please provide a definition of "served" in this respect.
11. Please provide a summary of the ROI review conducted to justify the anticipated gains and potential cost savings as an offset to the increased administrative expenditure.

MCE STAFF TRAINING AND COORDINATION

12. How and when will MCE Covered Individual Services and all other MCE business units' staff be trained about the Subcontractor? Submit copies of the relevant training materials.

13. Will the MCE designate staff to interact with the Subcontractor? If so, which staff and how many will be designated? Will interactions take place in-person or remotely or both?
14. Please specify the nature of coordination and communication that will occur between the Subcontractor and MCE staff.
15. With which of the MCE's other Subcontractors will this Subcontractor interact directly, as applicable? Please describe the nature of communication and coordination, and transfer of information, between this Subcontractor and other Subcontractors, for each of the above listed interactions. Include the role of the MCE for each.

NOTIFICATION OF AND EFFECTS ON COVERED INDIVIDUALS (IF APPLICABLE)

16. How many Covered Individuals in total will the Subcontractor serve? How will Covered Individuals be identified for this service?
17. Will the Subcontractor operations be visible or transparent to Covered Individuals?
18. How and when will existing Covered Individuals be notified of the role and availability of the Subcontractor? Submit draft copies of the relevant notification letters/materials.
19. Will new Covered Individual identification cards be sent? If so, how and when?
20. Identify any differences in access to BH Covered Services that may result from having this Subcontractor and, if access is more limited, the nature and timing of outreach to Covered Individuals.
21. Describe any other anticipated effects of the Subcontractor on Covered Individuals' engagement with the Contractor.

NOTIFICATION OF AND EFFECTS ON PROVIDERS (IF APPLICABLE)

22. Will the Subcontractor operations be visible or transparent to Providers?
23. How and when will the MCE provider network be informed about the Subcontractor? Please submit copies of the relevant notification and training materials.
24. How will the MCE ensure that PCPs are aware and approving of any information that the Subcontractor presents to Covered Individuals?
25. Identify any differences in access to Provider services that may result from having this Subcontractor and, if access is more limited, the nature and timing of outreach to Providers.
26. Describe any other anticipated effects of the Subcontractor on Providers.

SYSTEMS/ DATA

27. Will the Subcontractor have retrospective or live access to any MCE systems? If so, which system(s)?
28. Describe data elements to be shared between the Subcontractor and the MCE.
29. Describe the process for data sharing between the Subcontractor and the MCE.
30. How will data generated by the Subcontractor be integrated into MCE system(s), if applicable? How will data in the MCE system be transferred to the Subcontractor, if applicable? What will be

the frequency of such integration? How will data integrity be ensured? Explain the arrangement that will ensure the Covered Individual has the full range of recourse via the grievance and appeal system, including timely notifications and resolutions of processes.

31. Describe any expected loss of data history due to implementation of the Subcontract, if any.
32. Describe how the MCE will manage any unanticipated loss of data/information due to implementation of the Subcontract.
33. Does the MCE intend to operate redundant IT systems before a new system is relied upon solely? If so, for how long, and how will the MCE manage such redundancy of systems?
34. Describe the process that will be used to ensure that the IT system will have capacity to interface with New MMIS effectively, as applicable.

READINESS REVIEW

35. Describe the readiness review that the MCE will conduct of the Subcontractor, including timeframes.
36. Provide the MCE's contingency plan should the Subcontractor not be ready to operate by the expected implementation date. At what point will this contingency plan be implemented?
37. Has the Subcontractor worked with MassHealth or other Medicaid populations and/or within the MA market? If so, address prior experiences and measures of performance, including results of services implemented, if known.
38. Describe the training and education that the MCE will provide to the Subcontractor regarding the MCE and the MassHealth population.

EVALUATION

39. Describe how the Subcontractor's performance will be evaluated. Does the MCE plan to evaluate the Subcontractor, or will the MCE conduct the evaluation independently? If the Subcontractor will self-evaluate, what role, if any, will the MCE play in the evaluation?
40. How will the MCE ensure effective subcontractor participation in all EQRO related activities?
41. How will the MCE ensure the Subcontractor's compliance with all MassHealth MCE Program contractual provisions, including those relating to confidentiality of information and Marketing?
42. Reference any national, state, and/or local standards to which the Subcontractor will adhere.

SECTION 2.
Please answer all questions completely within the area below that are applicable to the new Subcontractor type.

CARE MANAGEMENT

1. Describe the process that will be used to transfer the active caseloads of Covered Individuals currently receiving Care Management from the MCE and/or other Subcontractor to the new Subcontractor.
2. Describe the process that will be used to ensure minimal disruption to Covered Individuals and/or care management systems. What are the respective roles of the Subcontractor and the MCE in this process, and the nature of communication and collaboration between the Subcontractor and the MCE in this process?
3. Describe the process that will be used to ensure effective communication and coordination between the Subcontractor, PCPs of Covered Individuals in care management, and the MCE. What are the respective roles of the Subcontractor and the MCE in this process, and the nature of communication and collaboration between the Subcontractor and the MCE in this process?

UTILIZATION MANAGEMENT

Describe the mechanisms it will use to ensure that subcontractor managed levels of service utilization are appropriate and simultaneously ensure high quality care in a manner that would not impede access to medically necessary care.

CLAIMS

1. Describe the process that will be used to transfer the current claims processing system to the new claims processing system.
2. Describe the process that will be used to ensure minimal disruption to claims processing and other IT functions, including timely and appropriate payment of claims. What are the respective roles of the Subcontractor and the MCE in this process, and the nature of communication and collaboration between the Subcontractor and the MCE in this process?
3. Describe the process that will be used to ensure that any prior approvals granted under the current system will be honored under the Subcontractor.
4. Describe the process that will be used to ensure that claims will not be double-paid by the current and the new Subcontractor during transition. What are the respective roles of the Subcontractor and the MCE in this process, and the nature of communication and collaboration between the Subcontractor and the MCE in this process?
5. Explain what steps will be taken to be sure the new claims system can properly perform all the interfaces with MMIS that are required.
6. Describe steps to ensure EOHHS reporting will not be negatively impacted

CALL CENTER

1. Describe the process for handling various types of calls from Covered Individuals.

2. Please describe how the process for handling various types of calls differs for Covered Individuals, prospective Covered Individuals, and/or enrollees in other product lines, if applicable
3. How will the MCE ensure that all required Covered Individual notifications occur in a timely and effective manner?

APPENDIX B-3

Disclosure Form for Entities

Commonwealth of Massachusetts | Executive Office of Health and Human Services | mass.gov

As set forth in 42 CFR §§ 455.100-106, MassHealth providers, managed care entities (MCEs), fiscal agents, and other disclosing entities seeking to provide MassHealth services (including Accountable Care Organizations (ACOs)), must disclose information regarding business ownership and control, business transactions, and criminal convictions, including submission of all relevant tax identification numbers (TINs), (e.g., social security number (SSN) or federal employer identification number (FEIN)) in order to ensure proper administration of the MassHealth program.

As set forth in 42 CFR § 455.101, MCEs include the following (as defined in 42 CFR § 438.2).

- Health Insuring Organization (HIO)
- Prepaid Inpatient Health Plan (PIHP)
- Managed Care Organization (MCO)
- Primary Care Case Manager (PCCM)
- Prepaid Ambulatory Health Plan (PAHP)

The MassHealth agency may at its discretion disapprove a provider contract, and may terminate an existing contract, if the provider fails to disclose any information in accordance with the provisions of 130 CMR 450.222, 130 CMR 450.223, or 42 CFR §§ 455.100–106, 42 CFR § 455.436, 42 CFR § 1002, or as otherwise required by state or federal law (See 130 CMR 450.227).

NOTE: All sections of this form must be completed.

Unless otherwise instructed by MassHealth, all MCEs, fiscal agents, and other disclosing entities, including ACOs, must use this form when disclosing such information to MassHealth upon:

- enrollment
- re-enrollment (following disenrollment from MassHealth)
- revalidation
- a change in managing employee(s)
- a change of ownership or control interest
- at the request of MassHealth
- any subsequent change(s) to any of the information stated on this form in accordance with 130 CMR 450.223(B)

CONTACT INFORMATION FOR INDIVIDUAL COMPLETING THIS FORM

Name	
Tel.	Email

DEFINITIONS

The following definitions provided here for reference are found at 42 CFR § 1001.2, 42 CFR § 455.101 and 130 CMR 450.221.

Agent: any person who has been delegated the authority to obligate or act on behalf of a provider.

Disclosing Entity: a Medicaid provider (other than an individual practitioner or group of practitioners), or a fiscal agent.

Familial Relationship: parent, child, sibling, or spouse.

Fiscal Agent: a contractor that processes or pays vendor claims on behalf of the Medicaid agency.

Group of Practitioners: two or more health care practitioners who practice their profession at a common location (whether or not they share common facilities, common supporting staff, or common equipment).

Immediate Family Member: a person's husband or wife; natural or adoptive parent; child or sibling; step-parent, stepchild, stepbrother or stepsister; father-, mother-, daughter-, son-, brother- or sister-in-law; grandparent or grandchild; or spouse of a grandparent or grandchild.

Indirect Ownership Interest: an ownership interest in an entity that has an ownership interest in the disclosing entity. This term includes an ownership interest in any entity that has an indirect ownership interest in the disclosing entity.

Managed Care Entity (MCE): managed care organizations (MCOs), PIHPs, PAHPs, PCCMs, and HIOs, as defined by 42 CFR §455.101.

Managing Employee: a general manager, business manager, administrator, director, or other individual who exercises operational or managerial control over, or who directly or indirectly conducts the day-to-day operation of an institution, organization, or agency.

Member of Household: with respect to a person, any individual with whom he or she is sharing a common abode as part of a single family unit, including domestic employees and others who live together as a family unit. A roomer or boarder is not considered a member of household.

Other Disclosing Entity (ODE): any other Medicaid disclosing entity and any entity that does not participate in Medicaid, but is required to disclose certain ownership and control information because of participation in any of the programs established under Title V, XVIII, or XX of the Act. This includes (a) any hospital, nursing facility, home health agency, independent clinical laboratory, renal disease facility, rural health clinic, or health maintenance organization that participates in Medicare (Title XVIII); (b) any Medicare intermediary or carrier; and (c) any entity (other than an individual practitioner or group of practitioners) that furnishes, or arranges for the furnishing of, health-related services for which it claims payment under any plan or program established under Title V or Title XX of the Act.

Ownership Interest: the possession of equity in the capital, the stock, or the profits of the disclosing entity.

Person with Ownership or Control Interest: A person or corporation that (a) has an ownership interest totaling five percent or more in a disclosing entity; (b) has an indirect ownership interest equal to five percent or more in a disclosing entity; (c) has a combination of direct and indirect ownership interests equal to five percent or more in a disclosing entity; (d) owns an interest of five percent or more in any mortgage, deed of trust, note, or other obligation secured by the disclosing entity if that interest equals at least five percent of the value of the property or assets of the disclosing entity; (e) is an officer or director of a disclosing entity that is organized as a corporation; (f) is a partner in a disclosing entity that is organized as a partnership, or (g) owns directly or indirectly an interest of five percent or more in any real property leased to a disclosing entity for use as a nursing facility, rest home, or hospital.

An individual is deemed to own any beneficial interest owned directly or indirectly by or for his or her minor children or spouse.

Significant Business Transaction: any business transaction or series of transactions that, during any one fiscal year, exceed the lesser of $25,000 or five percent (5%) of a provider's total operating expenses.

Subcontractor: (a) an individual, agency, or organization to which a disclosing entity has contracted or delegated some of its management functions or responsibilities of providing medical care to its patients; or (b) an individual, agency, or organization with which a fiscal agent has entered into a contract, agreement, purchase order, or lease (or leases of real property) to obtain space, supplies, equipment, or services provided under the Medicaid agreement.

Supplier: an individual, agency, or organization from which a provider purchases goods and services used in carrying out its responsibilities under Medicaid (e.g., a commercial laundry, a manufacturer of hospital beds, or a pharmaceutical firm).

Wholly Owned Supplier: a supplier whose total ownership interest is held by a provider or by a person, persons, or other entity with an ownership or control interest in a provider.

SECTION 1: Disclosing Entity Service Location / "Doing Business As" (SL/DBA) Name

Enter the SL/DBA name, address, and all other information requested below, applicable to this service location (SL) where services will be provided or are currently provided to MassHealth members.

Disclosing Entity SL/DBA Name		
Address (Street, Building or Suite)		
City, State & Zip Code		
NPI	PID/SL (for existing MassHealth providers)	FEIN

SECTION 2: Ownership or Control Interest in Disclosing Entity

List any individual or corporation with an ownership or control interest in the disclosing entity. Instructions for determining ownership or control percentages can be found at 42 CFR § 455.102 and 130 CMR 450.221(B). **Individuals must provide their home address. Corporations must list, as applicable, their primary business address, all business locations, corporate addresses, and P.O. Box addresses.**

Which of the Ownership or Control Interest describes you (select one): ☐ Ownership interest, ☐ Control interest, ☐ Both.

Name of Individual or Corporation	Board of directors (if individual) ☐ Yes ☐ No	Date of Birth (if individual) (MM/DD/YYYY)
Address (Home Address if Individual; Primary Business Address if Corporation)	City, State & Zip Code (9 digit)	

SSN (if individual)	FEIN (if corporation)	% of Ownership	NPI (☐ check the box if None)

For Individuals Only: If the individual listed above is related as a parent, child, sibling, or spouse to another person with an ownership or control interest in the disclosing entity, complete the following: Name of other person with ownership or control interest and relationship to the individual listed above (check one)

1. _____ ☐ parent ☐ child ☐ sibling ☐ spouse
2. _____ ☐ parent ☐ child ☐ sibling ☐ spouse
3. _____ ☐ parent ☐ child ☐ sibling ☐ spouse

For Corporations Only: Use the space below to report the address of all other business locations, corporate addresses, and P.O. box addresses.

1. _____
2. _____
3. _____

Which of the Ownership or Control Interest describes you (select one): ☐ Ownership interest, ☐ Control interest, ☐ Both.

Name of Individual or Corporation	Board of directors (if individual) ☐ Yes ☐ No	Date of Birth (if individual) (MM/DD/YYYY)
Address (Home Address if Individual; Primary Business Address if Corporation)	City, State & Zip Code (9 digit)	

SSN (if individual)	FEIN (if corporation)	% of Ownership	NPI (☐ check the box if None)

For Individuals Only: If the individual listed above is related as a parent, child, sibling, or spouse to another person with an ownership or control interest in the disclosing entity, complete the following: Name of other person with ownership or control interest and relationship to the individual listed above (check one)

1. _____ ☐ parent ☐ child ☐ sibling ☐ spouse
2. _____ ☐ parent ☐ child ☐ sibling ☐ spouse
3. _____ ☐ parent ☐ child ☐ sibling ☐ spouse

For Corporations Only: Use the space below to report the address of all other business locations, corporate addresses, and P.O. box addresses.

1. _____
2. _____
3. _____

If additional space is needed, make a copy of this page and attach it to the signed form. **NUMBER** _____ **OF** _____

All entries must be submitted using this form. Please refer to all attached pages when completing and signing this form.

SECTION 3: Ownership in Other Disclosing Entities (ODE)

Complete if any individual or corporation identified in Section 2 has an ownership or control interest in other disclosing entities.

☐ NONE (if NONE continue to Section 4)

Name (from Section 2)	Title	ODE Name
ODE Address	City, State, & Zip Code (9 digit)	
Name (from Section 2)	Title	ODE Name
ODE Address	City, State, & Zip Code (9 digit)	

SECTION 4: Ownership in Subcontractors

List any individual or corporation with an ownership or control interest in any subcontractor in which the disclosing entity has an ownership or control interest. If none, check 'None' below.

☐ NONE (if NONE continue to Section 5)

Name of individual or corporation	TIN of individual or corporation (TIN)
Owner's Address	City, State, & Zip Code (9 digit)
Subcontractor Name	Subcontractor Tax Identification Number (TIN)
Subcontractor Primary/Home Address	City, State, & Zip Code (9 digit)
Name of individual or corporation	TIN of individual or corporation (TIN)
Owner's Address	City, State, & Zip Code (9 digit)
Subcontractor Name	Subcontractor Tax Identification Number (TIN)
Subcontractor Primary/Home Address	City, State, & Zip Code (9 digit)

SECTION 5: Familial Relationship in Subcontractors

Complete if anyone identified in Section 2 is related to a person identified in Section 4 as a parent, child, sibling, or spouse. If none, check 'None' below.

☐ NONE (if NONE continue to Section 6)

Name of individual with ownership or control interest identified in Section 2
Name of individual with ownership or control interest identified in Section 4 and familial relationship to individual identified in Section 2
Name of individual with ownership or control interest identified in Section 2
Name of individual with ownership or control interest identified in Section 4 and familial relationship to individual identified in Section 2

If additional space is needed, make a copy of this page and attach it to the signed form. **NUMBER _____ OF _____**

All entries must be submitted using this form. Please refer to all attached pages when completing and signing this form.

SECTION 6: Agents and Managing Employees

Completion of all fields is required by 42 CFR § 455.104. Make copies if additional space is needed. All entries must be submitted using this form.

☐ Agent ☐ Managing employee ☐ Both

Name	Title
Home Address	City, State, & Zip Code (9 digit)
SSN	Date of Birth (MM/DD/YYYY)

☐ Agent ☐ Managing employee ☐ Both

Name	Title
Home Address	City, State, & Zip Code (9 digit)
SSN	Date of Birth (MM/DD/YYYY)

☐ Agent ☐ Managing employee ☐ Both

Name	Title
Home Address	City, State, & Zip Code (9 digit)
SSN	Date of Birth (MM/DD/YYYY)

☐ Agent ☐ Managing employee ☐ Both

Name	Title
Home Address	City, State, & Zip Code (9 digit)
SSN	Date of Birth (MM/DD/YYYY)

☐ Agent ☐ Managing employee ☐ Both

Name	Title
Home Address	City, State, & Zip Code (9 digit)
SSN	Date of Birth (MM/DD/YYYY)

☐ Agent ☐ Managing employee ☐ Both

Name	Title
Home Address	City, State, & Zip Code (9 digit)
SSN	Date of Birth (MM/DD/YYYY)

If additional space is needed, make a copy of this page and attach it to the signed form. **NUMBER _____ OF _____**

All entries must be submitted using this form. Please refer to all attached pages when completing and signing this form.

SECTION 7: Disclosures of Criminal Convictions and Relationships to Excluded Individuals and Entities

For additional information, see 42 CFR §§ 455.106 and 455.436, 42 CFR §§ 1001.1001 and 1002.3, and 130 CMR 450.212.

Respond to the following questions on behalf of:

1. the disclosing entity
2. all individuals and corporations identified in Sections 2 and 6 of this form
3. any person who formerly held an ownership or control interest in the entity but no longer holds an ownership or control interest because of a transfer of the interest to an immediate family member or a member of the person's household in anticipation of or following a conviction, imposition of a civil money penalty or assessment under Section 1128A of the Social Security Act, or imposition of an exclusion.

NOTE: All questions must be answered. If "yes" is answered to any of the questions in Section 7 below, a detailed explanation is required in Section 8 of this form, including the name Social Security Number (SSN)/Tax Identification Number (TIN) and address of the individual/entity; nature, date, and forum of the action; and any case or record number.

---

1. Have any of the individuals/entities ever been convicted of a criminal offense related to any program under Medicare, Medicaid, or Title XX services?
   ☐ Yes ☐ No

2. Have any of the individuals/entities been convicted of a criminal offense as described in sections 1128(a) and 1128(b) (1), (2), or (3) of the Social Security Act?
   ☐ Yes ☐ No

3. Have any of the individuals/entities been excluded from participation in any federal or state health program (including, but not limited to, Medicare or Medicaid)?
   ☐ Yes ☐ No

4. Have any of the individuals/entities had civil money penalties or assessments imposed under section 1128A of the Social Security Act?
   ☐ Yes ☐ No

5. Is there currently pending any proceeding(s) that could result in a conviction, sanction, or other action reportable in questions 1 – 4, above?
   ☐ Yes ☐ No

NOTE: All questions must be answered. If "Yes" is answered to any of the questions in Section 7 above, a detailed explanation is required in Section 8 of this form, including the name Social Security Number/Tax Identification Number (SSN/TIN) and address of the individual/entity; nature, date, and forum of the action; and any case or record number.

SECTION 8: Additional Explanation

If "Yes" is answered to any of the questions in Section 7, a detailed explanation is required below, including the name, Social Security Number/Tax Identification Number (SSN/TIN) and address of the individual/ entity, nature, date, and forum of the action, and any case or record number.

Attach additional pages if necessary.

If additional space is needed, make a copy of this page and attach it to the signed form. **NUMBER _____ OF _____**

All entries must be submitted using this form. Please refer to all attached pages when completing and signing this form.

SECTION 9: Attestation, Signature, and Date

All disclosing entities must complete this section.

I certify that the information on this form, and any attached statement that I have provided, has been reviewed and signed by me, and is true, accurate, and complete, to the best of my knowledge.

I understand that I sign under the pains and penalties of perjury, and may be subject to civil penalties or criminal prosecution for any falsification, omission, or concealment of any material fact contained herein.

I agree to abide by all applicable federal and state laws and regulations, as well as the rules and regulations of particular to the type of program covered by this enrollment application.

Note: Signature or date stamps, electronically generated signatures or dates, or the signature of anyone other than the disclosing entity or person legally authorized to sign on behalf of the entity are not acceptable.

In accordance with 130 CMR 450.223(B), I agree to notify the MassHealth agency in writing within 14 days of any change to any of the information submitted upon enrollment.

In accordance with 42 CFR § 455.105, I agree to disclose full and complete information regarding the following business transactions within 35 days following a request of the MassHealth agency or the Secretary of Health and Human Services:

1. Information about the ownership of any subcontractor with whom the provider, MCE, or disclosing entity has had business transactions totaling more than $25,000 during the 12-month period ending on the date of the request; and
2. Any significant business transactions between the provider and any wholly owned supplier or between the provider and any subcontractor during the 5-year period ending on the date of the request.

Signature: _____

Printed Name _____

Title _____

Date (MM/DD/YYYY) _____

Return your completed form to providersupport@mahealth.net or mail to the following:

MassHealth Customer Service Center
Attn: Provider Enrollment and Credentialing
PO Box 121205
Boston, MA 02112-1205

If you have questions about or need assistance with the completion of this form, please email the MassHealth Customer Service Center at providersupport@mahealth.net or call (800) 841-2900.

APPENDIX C

COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

Office of Medicaid
One Ashburton Place
Boston, MA 02108

FOURTH AMENDED AND RESTATED PRIMARY CARE CLINICIAN (PCC) PLAN PROVIDER CONTRACT

TABLE OF CONTENTS

Section 1. DEFINITIONS **1**

Section 2. PCC ELIGIBILITY **5**

Section 3. PCC RESPONSIBILITIES **5**

Section 3.1 Administration and Contract Management 5

Section 3.2 Provision of Medical Services 7

Section 3.3 Member Enrollment, Disenrollment, Reenrollment, and Orientation 10

Section 3.4 Privacy, Confidentiality, Security of Personal Data and HIPAA Compliance 13

Section 3.5 Enrollee Grievances 14

Section 3.6 Enrollee Rights 14

Section 3.7 Performance Improvement Management Services (PIMS) 15

Section 4. EOHHS RESPONSIBILITIES **15**

Section 4.1 Provider Application 15

Section 4.2 Administration and Contract Management 15

Section 4.3 Member Enrollment and Disenrollment Activities 16

Section 5. PAYMENT **16**

Section 5.1 PCC Enhanced Rate 16

Section 5.2 EPSDT Enhanced Rate 17

Section 5.3 Prospective Interim Payment (PIP) 17

Section 5.4 Claims Submission 18

Section 6. ADDITIONAL TERMS AND CONDITIONS **18**

Section 6.1 Compliance with Law 18

Section 6.2 Subcontracts 18

Section 6.3 Prohibited Affiliations 19

Section 6.4 Intermediate Sanctions 19

Section 6.5 Contract Termination 19

Section 6.6 Amendment 20

ATTACHMENT A: PCC Enhanced Fee Codes

WHEREAS, the Executive Office of Health and Human Services ("EOHHS") is a governmental agency responsible for the administration of the Title XIX and Title XXI ("MassHealth") Program; and

WHEREAS, the Primary Care Clinician ("PCC") has met the criteria for participation in EOHHS' Primary Care Clinician Plan; and

WHEREAS, the parties wish to amend the Contract as set forth here;

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the PCC and EOHHS agree as follows:

SECTION 1. DEFINITIONS

As used in this Contract, each of the following terms has the indicated meaning unless the context clearly requires otherwise.

Behavioral Health Program -- a managed care program administered by EOHHS through the Behavioral Health Program Contractor, for the provision of mental health and substance abuse services to Members enrolled in the PCC Plan.

Behavioral Health Program Contractor -- EOHHS' contractor responsible for providing mental health and substance abuse services to Members enrolled in the PCC Plan, for implementing quality management activities to support PCCs in delivering health care services to Enrollees, and for implementing administrative services to support EOHHS in managing its network of PCCs.

Behavioral Health Services -- MassHealth covered mental health and substance abuse treatment services.

Cold-Call Marketing -- any unsolicited personal contact by a PCC, its employees, agents, or subcontractors with a Member who is not enrolled with the PCC Plan that reasonably can be interpreted as intended to influence the Member to enroll in the PCC Plan, or to disenroll from, a MassHealth Managed Care Organization or the PCC Plan.

Early and Periodic Screening, Diagnosis and Treatment (EPSDT) -- the delivery of health care services to Members under the age of 21, in accordance with 42 U.S.C. § 1396d(a)(4), 42 CFR Part 441 Subpart B, and 130 CMR 450.140 et seq.

EPSDT Periodicity Schedule -- The EPSDT Medical Protocol and Periodicity Schedule that appears in **Appendix W** of all MassHealth provider manuals and is developed and periodically updated by MassHealth in consultation with the Massachusetts Chapter of the American Academy of Pediatrics, Massachusetts Department of Public Health, dental professionals, the Massachusetts Health Quality Partners, and other organizations concerned with children's health. The Schedule consists of screening procedures arranged according to the intervals or age levels at which each procedure is to be provided.

Easily Understood Format – the provision of information in a manner, format, and language that is easily understood, including written at no higher than a sixth-grade reading level.

Emergency Medical Condition -- a medical condition, whether physical or mental, manifesting itself by symptoms of sufficient severity, including severe pain, that the absence of prompt medical attention could reasonably be expected by a prudent layperson who possesses an average knowledge of health and medicine, to result in placing the health of the Member or another person, or in the case of a pregnant woman, the health of the woman or her unborn child, in serious jeopardy, serious impairment to body function, or serious dysfunction of any body organ or part, or, with respect to a pregnant woman, as further defined in section 1867(e)(1)(B) of the Social Security Act, 42 U.S.C. § 1395dd(e)(1)(B).

Emergency Services -- medical services that are furnished by a qualified provider and are needed to evaluate or stabilize an Emergency Medical Condition.

Enrollee -- a person determined eligible for MassHealth who is enrolled in the PCC Plan, either by choice or by assignment by EOHHS.

Executive Office of Health and Human Services (EOHHS) -- the Executive Office of Health and Human Services is the single state agency responsible for the administration of the MassHealth Program, pursuant to M.G.L. c. 118E and Title XIX and XXI of the Social Security Act and other applicable laws and waivers.

Grievance -- a complaint made by an Enrollee, which may be made either in writing or verbally, based on an issue of concern with any aspect of MassHealth or its participating provider network.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) -- federal law enacted as Pub. L. No. 104-191, and the regulations promulgated at 45 CFR Parts 160, 162 and 164, to ensure health care insurance portability, to streamline the administration of health care, and to protect the security and privacy of patient information.

Health Plan and Employer Data Information Set (HEDIS) -- a data set developed by the National Committee for Quality Assurance (NCQA), that is part of a national effort to standardize the measurement and reporting of health plan performance. EOHHS collects a subset of HEDIS measures each year to assess the performance of the PCC Plan and MassHealth-contracted Managed Care Organizations.

Individual Care Plan (ICP) – the plan of care developed by an Intensive Clinical Management clinician in conjunction with an individual's Behavioral Health Program Provider.

Individual Care Plan Report (ICPR) – a written version of the ICP that is mailed to PCCs.

Managed Care Contact -- an individual, designated by the PCC, to serve as the primary liaison between the PCC practice and EOHHS.

Marketing -- any communication from a PCC, its employees, agents or subcontractors to a Member who is not enrolled in the PCC Plan that reasonably can be interpreted as intended to influence the Member to enroll in the PCC Plan, or either to not enroll in, or to disenroll from, a MassHealth Managed Care Organization or the PCC Plan. This includes the production and dissemination by or on behalf of the PCC of any Marketing Materials. Marketing shall not include: (1) any one-to-one contact between a Provider and a Member who is a prospective, current, or former patient of that Provider regarding the provisions, terms, or requirements of MassHealth as they relate to the treatment needs of that particular Member; (2) any one-to-one contact between a Provider and a Member who was a patient of that Provider at the time the Member was enrolled in a MassHealth Managed Care Organization or the PCC Plan to inform the Member how to select the Provider going forward, if the Member so chooses, provided that the Provider informs the Member of all the MassHealth managed care plans with which the Provider is participating, including the PCC Plan and any Managed Care Organization.

Marketing Materials -- materials that are produced in any medium, by or on behalf of the PCC and can reasonably be interpreted as intended for Marketing to Members. This includes the production and dissemination by or on behalf of the PCC of any promotional material or activities by any medium including, but not limited to, oral presentations and statements, community events, print media, audio visual tapes, radio, television, billboards, Yellow Pages, and advertisements that explicitly or implicitly refer to MassHealth managed care or Title XIX of the Social Security Act, and are targeted in any way toward Members.

MassHealth -- the medical assistance or benefit programs administered by EOHHS to provide and pay for medical services to eligible Members pursuant to Title XIX of the Social Security Act (42 U.S.C. 1396), Title XXI of the Social Security Act (42 U.S.C. § 1397), M.G.L. c.118E, and other applicable laws and waivers.

MassHealth Card -- the identification card issued to persons who have been determined eligible for MassHealth.

MassHealth Coverage Type -- a scope of medical services and other benefits that is available to Members who meet specific MassHealth eligibility criteria. See 130 CMR 450.105 for a list of services covered under each coverage type.

Medically Necessary -- those MassHealth covered services that have been determined to meet the Commonwealth's definition of "medically necessary services" at 130 CMR 450.204.

Member -- a person determined by the Executive Office of Health and Human Services to be eligible for MassHealth.

Non-Symptomatic Care – an Enrollee encounter with a Provider, not associated with any presenting medical signs. Examples include well-visits and physical examinations.

Non-Urgent Symptomatic Care – an Enrollee encounter with a Provider, associated with presenting medical signs and symptoms, but not requiring immediate medical attention. Examples include recurrent headaches or fatigue.

Panel -- all MassHealth members enrolled with a particular PCC.

Performance Improvement Management Services (PIMS) -- a quality improvement program administered by EOHHS' Behavioral Health Program Contractor to help PCCs improve the rate at which certain preventive care services are provided to PCC Plan Enrollees and improve the PCC's ability to manage the care of PCC Plan Enrollees with chronic diseases.

Poststabilization Care Services -- MassHealth covered services, related to an Emergency Medical Condition, that are provided after an Enrollee is stabilized in order to maintain the stabilized condition, or when covered pursuant to 42 CFR 438.114(e) to improve or resolve the Enrollee's condition.

Primary Care -- health care services customarily furnished by or through a general practitioner, family physician, internal medicine physician, obstetrician/gynecologist, pediatrician, independent nurse practitioner or independent nurse midwife, to the extent the furnishing of those services is legally authorized in the Commonwealth. Primary Care does not include emergency or poststabilization services provided in a Hospital or other setting.

Primary Care Case Management -- a system under which the PCC contracts with the State to furnish case management services (which include the location, coordination, and monitoring of Primary Care health services) to Enrollees.

Primary Care Clinician (PCC) -- a physician, independent nurse practitioner, group practice organization, community health center, hospital-licensed health center, or acute hospital outpatient department, with a signed PCC Plan Provider application that is approved by EOHHS.

Primary Care Clinician (PCC) Plan -- the Primary Care Case Management program administered by EOHHS through which Enrollees receive coordinated Primary Care and certain other medical services.

Provider -- a MassHealth-participating individual, group, facility, agency, institution, organization, or other entity that directly provides medical or Behavioral Health Services to Members.

Recipient Eligibility Verification System (REVS) -- EOHHS' on-line Member eligibility and enrollment verification system for use by MassHealth Providers.

Recipient Identification (RID) Number -- the 10-digit identification number assigned to each Member and printed next to or below the Member's name on the Member's MassHealth Card.

Referral -- authorization for those services that a PCC does not provide directly that require the PCC's referral or authorization in accordance with the provisions of this PCC Contract and applicable MassHealth regulations at 130 CMR 450.118.

Regional Network Manager (RNM) -- an individual who is assigned to a particular region of the state to conduct Performance Improvement Management Services (PIMS) with the PCCs that have a substantial number of Enrollees on their Panel.

Urgent Care -- medical services that are not primary care and are needed to treat a medical condition that is not an emergency medical condition.

SECTION 2. PCC ELIGIBILITY

The PCC shall, at the time of executing the Contract and at all times during the Contract term, meet the PCC Provider eligibility and participation requirements established in 130 CMR 450.118.

The PCC shall notify EOHHS and withdraw as a PCC if, at any time during the Contract term, the PCC no longer meets the PCC Provider eligibility and participation requirements at 130 CMR 450.118.

SECTION 3. PCC RESPONSIBILITIES

Section 3.1 Administration and Contract Management

A. Managed Care Contact

The PCC shall identify a Managed Care Contact to represent the PCC on all matters related to the fulfillment of the PCC Contract.

B. Notification of PCC Changes

1. Notice to EOHHS

The PCC shall notify EOHHS, in writing, at least 14 days prior to any changes affecting delivery of care, the administration of its PCC practice, or its performance of PCC Contract requirements. Such changes include, but are not limited to the following:

a. Voluntarily withdrawing from the PCC Plan or the MassHealth program for any reason;

b. A change in any information contained in the PCC Plan Provider application or other application submitted by the PCC to EOHHS;

c. A change of address;

d. A change in the Managed Care Contact required in **Section 3.1.A**.; and

e. A change in the PCC's hours of operation or designation of PCC specialty.

2. Notice to PCC Plan Enrollees

The PCC shall provide notice to its PCC Plan Enrollees in advance of any changes listed in **Section 3.1.B.1.a**. and **c.** above.

C. Medical Records

The PCC shall maintain an individual medical record for each PCC Plan Enrollee based on the following guidelines:

1. The medical record shall be consistent with MassHealth regulations and generally accepted medical practice and professional standards.

2. The medical record shall fully disclose the nature and extent of the services provided to PCC Plan Enrollees.

3. The PCC shall, upon request, furnish EOHHS and any other state and federal officials and agencies that have a legal right of access, or their designees, with such information, including copies of medical records of any Enrollee for whom payment was claimed from EOHHS, in accordance with 42 U.S.C. § 1396a(a)(30)(A) and 42 U.S.C. § 1396u-2(c)(1).

4. Upon an Enrollee's request, the PCC shall provide to the Enrollee a copy of the portion of his or her medical record created or maintained by the PCC at no cost to EOHHS or the Enrollee.

D. PCC Plan Panel Capacity

Upon approval of the PCC's Provider application, EOHHS will assign an Enrollee Panel capacity at the level requested by the PCC, except that EOHHS will not approve a Panel capacity in excess of 1500 Enrollees per individual PCC provider within the PCC practice. If the PCC Provider Application did not specify a Panel capacity, EOHHS will assign an Enrollee capacity of 1500 Enrollees per PCC site.

E. Marketing

The PCC shall not, in the performance of its services under this Contract:

1. Engage in any Cold-call Marketing; or

2. Engage in any Marketing unless EOHHS approves the Marketing Materials in advance and such Marketing Materials satisfy all applicable requirements in 42 CFR 438.104(b).

F. Informational and Instructional Materials

The PCC shall provide informational materials and instructional materials relating to Enrollees in an Easily Understood Format.

Section 3.2 Provision of Medical Services

A. Provision of Care

The PCC shall:

1. Comply with generally accepted medical practice and professional standards in the delivery of medical care to Enrollees;

2. Provide or refer for all Primary Care services covered under the Enrollee's MassHealth Coverage Type, as specified in 130 CMR 450.105;

3. Inform all MassHealth Standard and CommonHealth Enrollees under age 21 about the EPSDT program, including the benefits of preventative health care, the range of services available under the EPSDT program, including behavioral health services, and where and how to obtain those services;

4. Inform all MassHealth Standard and CommonHealth Enrollees under age 21 that medically necessary services in accordance with 42 U.S.C. § 1396d(a)(4), 42 CFR Part 441 Subpart B, and 130 CMR 450.140 et seq. are available without cost, except as may be provided under federal law, and that necessary transportation and scheduling assistance is available upon request;

5. Offer to screen all MassHealth Enrollees under age 21 in accordance with the EPSDT Periodicity Schedule and 130 CMR 450.140 through 150;

6. Provide or refer all MassHealth Standard and CommonHealth Enrollees under age 21 for all medically necessary treatment services, whether or not included in their coverage type, in accordance with the EPSDT Periodicity Schedule, 130 CMR 450.140 through 149, and applicable prior authorization procedures;

7. Provide or refer all MassHealth Basic, Essential, and Family Assistance Enrollees under age 21 for medically necessary treatment services that are covered by their coverage type, as described in 130 CMR 450.105;

8. Offer to screen using the standardized behavioral health screening tools described in the EPSDT Periodicity Schedule when conducting behavioral health screens according to the EPSDT Periodicity Schedule and 130 CMR 450.140 through 150;

9. Take any other actions with respect to providing and documenting EPSDT screens, referrals, and treatment services that are required by EOHHS, as directed and notified by EOHHS;

10. Inform all Enrollees that family planning services are available to the Enrollee through any MassHealth family planning provider, and that Enrollees do not need a referral in order to receive such services;

11. Not deny any Enrollee MassHealth covered services for which the Enrollee is eligible on account of the Enrollee's inability to pay the cost sharing; and

12. Acknowledge the rights of Enrollees (see **Section 3.6**) and take these rights into account when furnishing services to Enrollees.

B. Access

The PCC shall provide reasonable and adequate hours of operation and shall ensure that the following access standards are met:

1. Non-urgent, Symptomatic Primary Care Appointments. The PCC shall ensure that Enrollees are offered a date for non-urgent, symptomatic Primary Care appointments within 10 days of the Enrollee's request.

2. Non-symptomatic Primary Care Appointments. The PCC shall ensure that Enrollees are offered a date for non-symptomatic Primary Care appointments within 45 days of the Enrollee's request unless otherwise mandated by the EPSDT Periodicity Schedule in **Appendix W** of all MassHealth provider manuals, per 130 CMR 450.141.

3. Urgent Care Appointments. The PCC shall ensure that Enrollees are offered a date for urgent care within 48 hours of the Enrollee's request.

4. Special Rules for Appointments for Enrollees Placed in the Care of Custody of the Department of Social Services (DSS). For Enrollees newly placed in the care or custody of the Department of Social Services (DSS), make best efforts to provide a DSS Health-care Screening within seven calendar days of receiving a request from a DSS case worker for such DSS Health-care Screening, and provide a Comprehensive Medical Examination within 30 calendar days of receiving a request from a DSS case worker for such a Comprehensive Medical Examination unless otherwise mandated by the EPSDT Periodicity Schedule in **Appendix W** of all MassHealth provider manuals, per 130 CMR 450.141. A DSS Comprehensive Medical Examination shall be conducted, if applicable, in accordance with the EPSDT Periodicity Schedule.

5. Emergency Services. The PCC shall provide Emergency Services immediately upon request, or instruct the Enrollee to go to the nearest emergency room or to call 911, as appropriate.

6. Poststabilization Care Services. The PCC must provide any necessary referrals for Poststabilization Care Services.

7. 24 hours/7 days per week. The PCC shall provide Enrollees with a telephone number to contact the PCC during the hours when the office is not open. The PCC shall respond to all such calls within one hour.

8. Arrangement for Care in the PCC's Absence. The PCC may arrange with another Provider to deliver health care services to Enrollees in his or her absence. If the PCC has such arrangement, the PCC shall ensure that the Provider is a MassHealth participating Provider.

C. Referral for Service

The PCC shall:

1. Inform Enrollees of those services which do not require a PCC referral (see 130 CMR 450.118);

2. Refer the Enrollee when unable to provide a MassHealth-covered service that requires a referral to an appropriate MassHealth Provider who is able to provide the service, taking into account Enrollee preferences to the extent possible;

3. Provide for arrangements with, or referrals to, sufficient numbers of physicians and other practitioners enrolled with MassHealth to ensure that MassHealth covered services can be furnished to Enrollees promptly and without compromise to quality of care;

4. Initiate a PCC referral either by:

   a. Telephone;

   b. Using the MassHealth referral form; or

   c. Using the PCC's own referral form as long as it includes the same information contained in the MassHealth referral form.

5. Make best efforts to make all PCC referrals before the Enrollee receives services that require a referral;

6. Provide the referred-to Provider with the PCC's MassHealth Provider number for use on their claim form;

7. At its discretion, provide referrals for Enrollees the PCC has not yet seen; and

8. Document each referral in the Enrollee's medical record. Documentation shall include a copy of any medical report the referred to Provider submits to the PCC.

D. Coordination of Care

The PCC shall:

1. Monitor all MassHealth-covered services, whether provided directly or through a referral to other MassHealth providers. Monitoring of services that do not require a referral is at the discretion of the PCC in keeping with generally accepted medical practice and professional standards;

2. Communicate and coordinate, to the extent permissible by law, with any provider delivering any medical or Behavioral Health Services to the PCC's Enrollees, including all specialists, home health agencies, behavioral health professionals and providers, state agency case managers, care or disease managers, school-based health centers, local education authorities (schools), and discharge planners, as appropriate and applicable. Coordination shall include, upon receipt of an Individual Care Plan (ICP) Report from the Behavioral Health Program Contractor, reviewing and acknowledging receipt of the ICP Report.

3. Enroll in the Massachusetts Department of Public Health's Immunization Program.

E. Pharmacy Management

The PCC shall participate as directed in EOHHS' pharmacy management initiatives, and shall refer to the MassHealth Drug List when prescribing Medically Necessary medications.

F. Verification of Enrollee Eligibility

The PCC shall verify each Enrollee's health care coverage and PCC Plan enrollment before providing services.

Section 3.3 Member Enrollment, Disenrollment, Reenrollment, and Orientation

A. Member Enrollment to PCC Panel

The PCC shall accept for enrollment or reenrollment all Members assigned to the PCC's panel in the order in which they are assigned without restriction unless:

1. The PCC is operating at full Panel capacity.

2. The PCC shall not accept for enrollment or reenrollment any particular Member if the PCC is not medically qualified to provide Primary Care to that Member, provided that the PCC shall not discriminate and will not use any policy or practice that has the effect of discriminating against an Enrollee with respect to enrollment, disenrollment, or reenrollment on the basis of race, color, national origin, age, physical or mental disability, marital status, sexual orientation, health care status, or need for health care services.

B. Enrollee Disenrollment

1. The PCC may not disenroll an Enrollee from its Panel. The PCC may request that EOHHS disenroll an Enrollee from its Panel, provided that the PCC may not request disenrollment because of an adverse change in the Enrollee's health status, or because of the Enrollee's utilization of medical services, diminished mental capacity, or uncooperative or disruptive behavior resulting from his or her special needs (except where his or her continued enrollment seriously impairs the PCC's ability to furnish services to either the particular Enrollee or other Enrollees). EOHHS may in its sole discretion grant this request if the PCC demonstrates, in writing, to the satisfaction of EOHHS that:

   a. The Enrollee has a pattern of noncompliant or disruptive behavior which is not the result of the Enrollee's special needs;

   b. The continued enrollment of the Enrollee with the PCC seriously impairs the PCC's ability to furnish services to either this particular Enrollee or other Enrollees; or

   c. The PCC is unable to meet the medical needs of an Enrollee.

C. Enrollee's Initial Visit and Orientation

1. PCC Plan Orientation

   The PCC shall orient all Enrollees to the PCC Plan. The PCC Plan orientation shall include, at a minimum, the following information:

   a. The Importance of Primary Care. The PCC shall explain the importance of Primary Care and the role of the PCC in managing and providing that care.

   b. Updating Enrollee Information. The PCC shall explain the importance of keeping the PCC and EOHHS updated about any change in address or telephone number.

   c. Services That Do Not Require a Referral. The PCC shall tell Enrollees about those services that do not require a PCC referral. See 130 CMR 450.118.

   d. Carrying the MassHealth Card. The PCC shall emphasize that Enrollees should carry the MassHealth Card to enable Providers to check MassHealth eligibility and identify the Enrollee's PCC.

e. Helpful Telephone Numbers for Enrollees. The PCC shall provide Enrollees with the telephone numbers, in addition to the PCC's, for the following PCC Plan services:

1) MassHealth customer service; and

2) Behavioral Health Program Contractor's customer service line.

f. PCC Practice Specifics. The PCC shall tell Enrollees about:

1) The days and hours that the PCC's practice is open;

2) How long the Enrollee should expect to wait for an appointment for Primary and Urgent Care, consistent with access requirements specified in **Section 3.2.B.**;

3) Appointment cancellation procedures;

4) Alternate phone numbers; and

5) Procedures for contacting the PCC's office after normal business hours, including who to contact, who will call the Enrollee back, and how long the Enrollee should expect to wait for a return call, consistent with access requirements specified in **Section 3.2.B.**

2. Initial Visit

a. Timing of Initial Visit

1) For New Enrollees

The PCC shall attempt to contact a new Enrollee within three weeks of enrollment in order to schedule an initial visit unless the Enrollee has previously been known to the PCC and is already in the care of the PCC. The PCC shall make best efforts to schedule the initial visit, when required, within four months of enrollment with the PCC.

2) For New PCC Plan Enrollees Previously Known to and Currently in the Care of the PCC

No initial visit is required if the PCC has performed a physical examination within the last 12 months or, in the case of an Enrollee under age 21, within the period described in the EPDST Schedule.

3) Outreach to Pregnant Enrollees

The PCC shall attempt to contact an Enrollee who is pregnant within seven days of the PCC learning of the Enrollee's pregnancy to ensure that the Enrollee is accessing prenatal care services.

b. Purpose of Initial Visit

The initial visit shall include, at a minimum:

1) A medical history intake;

2) A physical examination;

3) For Enrollees under age 21, provision of services according to the EPSDT Schedule; and

4) Medically Necessary treatment.

Section 3.4 Privacy, Confidentiality, Security of Personal Data and HIPAA Compliance

A. Covered Entities

The parties acknowledge that they are covered entities, as defined in HIPAA regulations at 45 CFR 160.103.

B. Requirements Regarding Personal Data

The PCC shall comply with all applicable requirements regarding the privacy, confidentiality, security, use and disclosure of personal data (including protected health information), including but not limited to the requirements set forth in M.G.L. c.66A, 42 CFR 431, Subpart F, and 45 CFR Parts 160, 162 and 164.

C. PCC's Compliance with HIPAA

The PCC shall:

1. Conform to all applicable HIPAA requirements and regulations no later than the compliance date of each of those requirements or regulations.

2. At all times subsequent to the applicable compliance dates be in compliance with such requirements and regulations.

3. Work cooperatively with EOHHS on all activities related to implementation of and ongoing compliance with HIPAA requirements, as directed by EOHHS; and

4. Execute, at EOHHS' direction, a Trading Partner Agreement and any other agreements EOHHS determines are necessary to comply with HIPAA requirements.

Section 3.5 Enrollee Grievances

The PCC shall assist in Grievance resolution procedures as follows:

A. If an Enrollee has a Grievance related to the PCC, the PCC shall work cooperatively with the Enrollee and EOHHS to resolve the Grievance.

B. If the Enrollee wishes to file a Grievance, the PCC shall instruct the Enrollee to contact the MassHealth Customer Service Center.

Section 3.6 Enrollee Rights

A. The PCC must comply with all applicable Federal and State laws that pertain to Enrollee rights, including but not limited to, the Americans with Disabilities Act and the Civil Rights Act of 1964.

B. The PCC must ensure that its staff and any affiliated providers take those rights into account when furnishing services to Enrollees.

C. Enrollee rights shall include:

1. The right to receive the information required pursuant to this Contract;

2. The right to be treated with respect and with due consideration of his or her dignity and privacy;

3. The right to receive information on available treatment options and alternatives, presented in a manner appropriate to the Enrollee's condition and ability to understand;

4. The right to participate in decisions regarding his or her health care, including the right to refuse treatment;

5. The right to be free from any form of restraint or seclusion used as a means of coercion, discipline, convenience, or retaliation;

6. The right to request and receive a copy of his or her medical records, and request that they be amended or corrected, as specified in 45 CFR 164.524 and 164.526 (HIPAA);

7. The right to freely exercise his or her rights without adversely affecting the way the PCC treats the Enrollee; and

8. The right to choose his or her health professional to the extent possible and appropriate.

Section 3.7 Performance Improvement Management Services (PIMS)

The PCC shall participate in PIMS and other quality improvement activities specified by EOHHS. Participation by PCCs for whom a PCC Profile Report is produced shall include, without limitation:

A. Site visits by a Regional Network Manager with a PCC clinician, or a PCC clinician and an administrative staff member to review PCC Profile Report and any other reports and materials; and

B. The development and implementation of written action plans around specific quality improvement activities.

SECTION 4. EOHHS RESPONSIBILITIES

Section 4.1 Provider Application

EOHHS will act upon each received PCC Plan Provider Application, and either approve the application, withhold a decision pending the receipt of additional information, or deny the application and provide the reason or reasons for the denial within 30 days of the receipt of the application.

Section 4.2 Administration and Contract Management

EOHHS shall:

A. Provide the PCC with information on how to contact relevant EOHHS units and vendors for assistance with issues such as billing, prior authorization, covered services and other PCC responsibilities;

B. Conduct ongoing data and record reviews to help ensure the delivery of services in the most appropriate setting in accordance with medical standards and protocols;

C. Conduct quality management activities such as HEDIS measurement and Member satisfaction surveys to assess the effectiveness of the PCC Plan performance and make the results available to PCCs;

D. Pay the PCC an enhanced rate for certain Primary Care services provided to the PCC's Enrollees (see **Sections 5.1 and 5.2**);

E. Notify the PCC of all programmatic and policy changes that may affect the PCC's participation in MassHealth; and

F. Reserve the right to change the current MassHealth program, including but not limited to covered services, Member eligibility, cost-sharing, or PCC Plan programmatic features upon written notice to the PCC of any such changes.

Section 4.3 Member Enrollment and Disenrollment Activities

EOHHS shall:

A. Ensure an equitable Member enrollment process, which considers PCC Panel size and restrictions and existing Member and Provider relationships as guidelines;

B. Provide the PCC with a monthly report of Member enrollment;

C. Include on the Recipient Eligibility Verification System (REVS) the name and telephone number of the PCC with whom the Member is enrolled;

D. Provide Members with enrollment materials that describe the PCC Plan;

E. Transfer Members, through the MassHealth Customer Service Center, when a PCC leaves the PCC Plan;

F. Respond within three business days of receipt to a written non-urgent request made by a PCC to disenroll an Enrollee from the PCC's Panel, and within one business day of receipt to a written, urgent request made by a PCC to disenroll an Enrollee from the PCC's Panel;

G. Assist in the outreach to PCC Enrollees that the PCC is unable to locate; and

H. Inform the PCC of any new EOHHS-sponsored contract that affects PCC Plan Enrollees.

SECTION 5. PAYMENT

Section 5.1 PCC Enhanced Rate

A. EOHHS shall pay the PCC for services delivered to PCC Plan Enrollees in accordance with the terms and conditions contained in the EOHHS regulations that govern the PCC's MassHealth provider type. (See 130 CMR 433.000 and 410.000.)

B. EOHHS shall pay the PCC an enhanced rate for providing certain Primary Care services designated by EOHHS to PCC Plan Enrollees. See **Attachment A** for codes eligible for an enhanced rate.

C. EOHHS reserves the right to add or delete service codes to which such enhanced rate applies without a Contract amendment. EOHHS will provide PCCs with written advance notice of any changes to the codes to which the enhanced rate applies. EOHHS will provide such notice through written notification to PCCs.

D. The enhanced rate will only be paid for services provided by the PCC to Enrollees enrolled in the PCC's Panel on the date that the service was delivered.

E. EOHHS shall not pay PCCs for any claims submitted for an appointment missed by an Enrollee. PCCs are prohibited from charging EOHHS or Enrollees for a missed appointment.

Section 5.2 EPSDT Enhanced Rate

A. PCCs will receive an EPSDT enhanced rate for providing well-child care screens to Enrollees under age 21, when delivered in accordance with the EPSDT Periodicity Schedule and 130 CMR 450.140 through 150, and billed in accordance with all applicable billing instructions.

B. PCCs will receive a separate rate for providing the following services when delivered in accordance with the EPSDT Periodicity Schedule and 130 CMR 450.140 through 150, and billed in accordance with all applicable billing instructions:

1. The laboratory services that are listed in **Appendix Z** of all MassHealth provider manuals and included in the EPSDT Periodicity Schedule are payable (see 130 CMR 450.146(A));

2. The audiometric hearing test and the bilateral quantitative screening of visual acuity that are listed in **Appendix Z** of all MassHealth provider manuals and included in the EPSDT Periodicity Schedule (see 130 CMR 450.146(B)); and

3. The standardized behavioral health screening tools that is listed in **Appendix Z** of all MassHealth provider manuals and set forth in the EPSDT Periodicity Schedule (see 130 CMR 450.146(C)).

Section 5.3 Prospective Interim Payment (PIP)

A. Upon written request to EOHHS, EOHHS will make a monthly advance in the form of a prospective interim payment (PIP) to physician, independent nurse practitioner, group practice, and community health center PCCs. Outpatient department (OPD) and hospital-licensed health center (HLHC) PCCs are not eligible for a PIP.

B. The PIP is a monthly amount equal to 25% of the average monthly payments, including enhancements, made the previous quarter for all services provided to Enrollees.

C. EOHHS will conduct an ongoing reconciliation between the PIP and actual paid claims, and will adjust the PIP accordingly.

D. Upon notice of termination or planned termination of this Contract by either party, EOHHS will, at its discretion, close the PIP account.

Section 5.4 Claims Submission

A. PCC Claims

All statutes, regulations, rules, billing instructions, bulletins, and other written policy statements governing claims submissions for physicians, independent nurse practitioners, group practices, community health centers, and outpatient departments apply to the PCC Plan.

B. Other Provider Claims

The PCC shall provide the PCC referral number to all referred Providers. If a Provider submits a claim for a service that requires a referral and the PCC's referral number is not on the claim, the claim will be denied.

SECTION 6. ADDITIONAL TERMS AND CONDITIONS

Section 6.1 Compliance with Law

The PCC shall comply with all state and federal statutes, rules, regulations, billing instructions, provider bulletins, and other written policy guidance applicable to the PCC Plan. All statutory and regulatory citations contained in this Contract refer to those statutes and regulations, as they may be amended. Without limiting the generality of the foregoing, the PCC shall comply with Title VI of the Civil Rights Act of 1964, as implemented by regulations at 45 CFR Part 80; Title IX of the Education Amendments of 1972; the Age Discrimination Act of 1975, as implemented by regulations at 45 CFR Part 91; the Rehabilitation Act of 1973; the Americans with Disabilities Act; Titles XIX and XXI of the Social Security Act and waivers thereof; and 42 CFR Part 438, to the extent such provisions apply.

Section 6.2 Subcontracts

The PCC shall:

A. Maintain all subcontracts relating to this Contract in writing. All such subcontracts shall fulfill all applicable requirements of 42 CFR Part 438, and shall contain all relevant provisions of this Contract appropriate to the subcontracted service or activity.

B. Remain fully responsible for meeting all of the terms and requirements of this Contract regardless of whether the PCC subcontracts for performance of any Contract responsibility. No subcontract will operate to relieve the PCC of its legal responsibilities under this Contract.

C. Prior to any delegation, evaluate the prospective subcontractor's ability to perform the activities to be delegated.

D. Monitor the subcontractor's performance on an ongoing basis.

Section 6.3 Prohibited Affiliations

In accordance with 42 U.S.C. § 1936u-2(d)(1) and 42 CFR 438.610, the PCC shall not knowingly have an employment, consulting, or other agreement for the provision of items and services that are significant and material to the PCC's obligations under this Contract with any person, or affiliate of such person who is debarred, suspended, or otherwise excluded, under federal law, regulation, executive order, or guidelines, from certain procurement and non-procurement activities. Further, no such person may have beneficial ownership of more than five percent of the PCC's equity nor be permitted to serve as a director, officer, or partner of the PCC.

Section 6.4 Intermediate Sanctions

A. EOHHS shall provide the PCC with timely written notice prior to imposing any intermediate sanctions, which explain the basis and nature of the sanction, including any other due process protections that EOHHS elects to provide.

B. At any point during the Contract term, if EOHHS identifies any deficiency in the PCC's performance of this Contract, EOHHS may impose sanctions that it deems necessary, including termination in accordance with **Section 6.5**, notifying Enrollees of the violation, intermediate sanction, and their right to disenroll, restricting Member enrollment, reassigning Enrollees within the PCC's Panel, and disenrolling Enrollees from the PCC's Panel and such other measures as EOHHS determines appropriate to address the deficiency.

C. The intermediate sanction provisions in this Contract are pursuant to state authority.

Section 6.5 Contract Termination

A. Either party may terminate this Contract without cause by giving written notice to the other at least 30 calendar days prior to the effective date of termination as stated in the notice, or such other period as is mutually agreed upon by the parties.

B. Either party may terminate this Contract if the other party fails to fulfill the obligations of this Contract or laws governing this Contract by giving written notice to the other at least 14 days before the effective date of termination stated in the notice. The notice shall state the circumstances of the alleged breach and may state a reasonable period, not less than seven calendar days, during which the alleged breach may be cured. EOHHS may terminate this Contract immediately and without prior notice in the event of fraud or program abuse or if the health or safety of Enrollees is in jeopardy.

C. EOHHS will provide the PCC with a hearing before termination when required by law. Any such hearing will be held in substantial conformity with the procedures set forth in EOHHS' Provider sanction regulations

D. The termination provisions in this Contract are pursuant to state authority.

Section 6.6 Amendment

A. By mutual agreement, the parties may amend this Contract where such amendment does not violate state or federal statutory, regulatory, or waiver provisions, provided that such amendment is in writing. Further, the PCC agrees to take such actions as is necessary to amend this Contract in order for EOHHS to comply with all applicable state and federal laws and waivers, including, but not limited to HIPAA and the Balanced Budget Amendments of 1997 (BBA) and any regulations promulgated thereunder.

B. The PCC shall submit to EOHHS an executed original of any amendment to this Contract within 60 days of receipt. If the PCC does not execute the amendment, the PCC's participation in the PCC Plan shall continue under the terms and conditions of this Contract as amended by EOHHS, unless EOHHS opts to terminate this Contract in accordance with **Section 6.5** above.

Appendix D-1

Data Warehouse
Paid Encounter Data Set Request

COMMONWEALTH OF MASSACHUSETTS

EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

MassHealth Data Warehouse

Paid Encounter Data Set Request (Expanded Format)

Version 4.11

May 2, 2019

Table of Contents

Acronyms - 6 -
1.0 Introduction - 6 -
1.1 Data Requirements - 7 -
1.2 How to Use this Document - 8 -
Data Element Clarifications - 8 -
Data Elements - 8 -
Encounter Record Layout - 8 -
Media Requirements and Data Formats - 8 -
Standard Data Values - 8 -
Data Quality Checks - 8 -
2.0 Data Element Clarifications - 9 -
Member Ids - 9 -
Provider Ids - 9 -
NPI - 9 -
DRG - 10 -
Diagnosis Codes - 10 -
Procedure Code - 10 -
Capitation Payments - 10 -
Dollar Amounts - 10 -
Claim Number & Suffix - 13 -
Former Claim Number & Suffix - 13 -
Record Creation Date - 13 -
Inpatient Claim - 13 -
Old, pre-November 2016, DW Logic - 13 -
LTC Claims - 13 -
Physician-Administered Drug Claim Definition - 13 -
Administrative Fees - 14 -
Bundle Indicator, Claim Number & Suffix - 14 -
Provider ID submission in Encounter and Provider Files - 16 -
3.0 Encounter Data Set Elements with Record Layout - 17 -
Data Elements - 17 -
Programs with withhold amount - 17 -
Demographic Data - 17 -
Service Data - 20 -
Provider Data - 24 -
Financial Data - 25 -
Medicaid Program-Specific Data - 26 -
Other Fields - 27 -
3.1 Provider Data Set with Record Layout - 41 -
3.2 MCE Internal Provider Type Data Set Elements with Record Layout - 47 -
3.3 Provider Specialty Data Set Elements - 48 -
3.4 Additional Reference Data Set Elements - 49 -
4.0 Encounter Record Layout Amendment Process and Layout - 51 -
5.0 Error Handling - 52 -
Error Codes - 52 -
6.0 Media Requirements - 54 -
Format - 54 -
Filename - 54 -
Project Related Filename - 54 -
The Manual Override File - 55 -
The Zip File should contain: - 55 -
Metadata file - 55 -
Monthly Financial Report - CURRENTLY DECOMISSIONED! - 57 -
Secure FTP Server - 59 -
Sending Encounter data - 59 -

Receiving Error reports ..... - 59 -
CMS Internet Security Policy ..... - 60 -
7.0 Standard Data Values ..... - 66 -
TABLE A ..... - 67 -
Type of Admission (UB) ..... - 67 -
TABLE B ..... - 68 -
Source of Admission (UB) ..... - 68 -
TABLE C ..... - 69 -
Place of Service (HCFA 1500) ..... - 69 -
Place of Service Codes for Professional Claims ..... - 69 -
CMS Database (updated November 2016) ..... - 69 -
TABLE D ..... - 74 -
Place of Service (from UB Bill Type – 1st & 2nd digits) ..... - 74 -
Discharge Status (UB Patient Status) ..... - 75 -
TABLE G ..... - 76 -
Servicing Provider Type ..... - 76 -
TABLE H ..... - 79 -
Servicing Provider Specialty (from CMS 1500) ..... - 79 -
TABLE I – A ..... - 82 -
Service Category (Using the 4B reporting groups) ..... - 82 -
TABLE I – B1 ..... - 83 -
Service Category (Using the SCO reporting groups) ..... - 83 -
Note: For the Claims with Date of Service on or after October 1, 2016 ..... - 83 -
TABLE I – B2 ..... - 83 -
Service Category (Using the SCO reporting groups) ..... - 83 -
Note: For the Claims with Date of Service before October 1, 2016 ..... - 83 -
TABLE I – C ..... - 84 -
Service Category (Using the One Care - ICO reporting groups) ..... - 84 -
201 - 84 -
Acute Inpatient ..... - 84 -
202 - 84 -
Inpatient – MH/SA ..... - 84 -
203 - 84 -
Hospital Outpatient ..... - 84 -
204 - 84 -
Outpatient – MH/SA ..... - 84 -
205 - 84 -
Professional ..... - 84 -
210 - 84 -
Pharmacy ..... - 84 -
212 - 84 -
Long-Term Care (LTC) Facility ..... - 84 -
213 - 84 -
Home and Community Based Services (HCBS)/Home Health ..... - 84 -
215 - 84 -
Transportation ..... - 84 -
216 - 84 -
Durable Medical Equipment (DME) and Supplies ..... - 84 -
217 - 84 -
*All Other ..... - 84 -
TABLE K ..... - 85 -
Bill Classifications - Frequency (3rd digit) ..... - 85 -
TABLE M ..... - 86 -
Present on Admission (UB) ..... - 86 -
CMS POA Indicator Options and Definitions ..... - 86 -
CMS Updated on June 2008 ..... - 86 -
TABLE O ..... - 87 -

UNIT OF MEASURE ..... - 87 -
8.0 Quantity and Quality Edits, Reasonability and Validity Checks ..... - 88 -
Raw Data ..... - 88 -
Data Quality ..... - 88 -
9.0 Appendices ..... - 95 -
Appendix C – *Member Enrollment File Specifications* ..... - 95 -

Acronyms

ACO	Accountable Care Organization
DW	Data Warehouse
EOHHS	Executive Office of Health and Human Services
MCE	Managed Care Entity (MCO, SCO, One Care, and BH Vendor collectively)
MCO	Managed Care Organization
MH	MassHealth
PCC	Primary Care Center
PIDSL	Provider ID Service Location
SCO	Senior Care Organization

1.0 Introduction

MassHealth Data Warehouse was required to build and maintain a database of health care services provided to Massachusetts Medicaid recipients enrolled in managed care programs. EHS is using the database for a number of different projects including Centers for Medicare and Medicaid Services (CMS, formerly HCFA) reporting, program evaluation, and rate development. It is critical that each Managed Care Entity (ACO/MCO, BH Vendor, SCO, and One Care) provides EHS DW with records accurately reflecting all encounters provided to Medicaid recipients enrolled in MCEs' managed care program. Only with complete and accurate encounter data MassHealth is able to assess the effectiveness of the managed care program.

With the implementation of the ACO project, all MCEs are required to submit extended encounter information on paid claims and related data. Encounters for both, MCO and ACO, should be submitted in the same file.

For denied claims submissions, please see denied claims specifications document.

All the plans, including SCO and One Care plans should follow the new file format in their submissions.

MassHealth expects the MCEs to provide new, replacement, and void claims in each submission. MassHealth processes the data and returns rejected claims to the MCEs with the appropriate error codes. MCEs are expected to correct the offending claims and send them in a correction file within a week. **The submission-rejection-resubmission cycle has to be completed within a month of submission**. The number of rejected claims must be below a MassHealth defined threshold.
If you cannot submit data in this fashion, or if you have any questions about any of these documents, please contact Alla Kamenetsky at *Alla.Kamenetsky@state.ma.us*

1.1 Data Requirements

- The data referred to in this document are encounter data - records of health care services performed for Massachusetts Medicaid managed care beneficiaries. An encounter is defined as a unique service or procedure performed for a recipient. Multiple encounters can occur during a single visit to a provider, and each encounter should have a separate encounter record.

  - Send all fully adjudicated paid claims. All claims should reflect the final status of the claim on the date it is pulled.

  - Submit one encounter record for each service performed (i.e., if a claim consisted of five services, each service should have a separate encounter record).

  - Data should conform to the Record Layout specified later in this document. Any deviations from this format must be approved by EHS.

  - **Each row in a submitted file should have a unique Claim Number + Suffix combination.**

  - Only Paid claim lines should be submitted.

  - A feed should consist of new (original) claims, amendments, replacements and voids.
    The replacements and voids should have a former claim number and former suffix to associate them with the claim+suffix they are voiding or replacing.

- The association of the adjustments and voids to the ACO claims will be based on the date of service, so there will not be a situation where the original claim is associated with an ACO and the adjustment - with an MCO and vice versa.
-
- MCO claims where "From Service Date" is prior to 03/01/2018, the value of MCO PIDSL should be entered in "Entity PIDSL" field (#3)

- While processing the submission, MassHealth scans the files for the errors and returns error reports in the format of the input file with extra two columns to indicate an error code and the field with the error. MCEs should correct the errors and resubmit the records within a week from the date the file was loaded.

1.2 How to Use this Document

This *Encounter Data Set Request* is intended as a reference document. Its purpose is to identify the data elements that MassHealth needs to load into encounter database. The goal of this document is to clarify the standard record layout, format, and values that MassHealth will accept.

Data Element Clarifications

In 2.0 "Data Set Clarification" section provides clarifications and expectations on data elements like DRG, Diagnosis Codes, Procedure Codes, and Provider IDs.

Data Elements

The information contained in the Data Elements sections defines each of the fields included in the record layout. When appropriate, a list of valid values is included there. Nationally recognized coding schemes have been used whenever they exist.

Encounter Record Layout

Section 4.0 "Encounter Record Layout" specifies encounter file layout. All the MCEs must use that format when compiling the Encounter Data file that might contain all or any Claim Category (facility, professional, dental, etc.). MassHealth requests that the encounter data file is provided in a pipe-delimited text file with each service on a separate line.
Contact MassHealth if you need further clarification.

Media Requirements and Data Formats

Section 6.0 "Media Requirements and Data Formats" contains complete information about all the files that should be submitted to EHS DW. MCEs submit their data to MassHealth through a secure FTP server. Each MCE has a home directory on this server and is given an ID with public key/private key-based login. Please also note the security requirements for Internet transmissions noted in the Media Requirements section.

Standard Data Values

Section 7.0 "Standard Data Values" contains tables referenced in the specific fields of the Data Elements section (Tables A through H).

Data Quality Checks

This section within 8.0 "Quantity and Quality Edits, Reasonability and Validity Checks" provides the validity and quality criteria that encounter data are expected to meet.

2.0 Data Element Clarifications

MassHealth has identified several data elements that require further clarification with respect to the expectations for those elements. The information in this section details MassHealth's expectations for Recipient Identifiers, Provider IDs, DRG, Diagnosis Codes (primary through fifth), and Procedure Codes.

Member Ids
Encounter data records must include MassHealth member IDs that are "active" as of the time of data submission.

Provider Ids
MassHealth is asking plans to provide an identifier that is unique to the plan. The acceptable ID types are:

ID Type	ID Description	Comments
1	NPI	Accepted for any provider including Referring and Prescribing Provider IDs. Note: MassHealth expects MCEs to submit MCE Internal ID in Provider IDs and use NPI as a Provider ID only when necessary and when an internal ID is not available. When NPI is used in Provider ID fields, provider file must have it entered in Field #2 (Provider ID) and in field #26 (NPI). Field #26 (NPI) must also be populated for all other Provider ID types except when it's not available, like in the case of atypical providers.
6	MCE Internal ID	Accepted for any provider
8	DEA Number	Should be used with pharmacy claims only
9	NABP Number	Should be used with pharmacy claims only

- All the provider attributes should be filled out in the provider file as much as possible.
- The Provider ID, Provider ID Type, and Provider ID Location Code should be 100 % present on all provider records.
- 100% of Pharmacy and Physician-Administered Drugs claims must have Billing Provider NPI numbers in provider file
- At least 80% of all the records in submission should have NPI numbers included
- At least 80% of all the records in submission should have Provider Type entered.
- All the provider records in provider file, which are part of the PCC enrollment with MCE, need to have PCC details on the same line.

NPI
The Centers for Medicare & Medicaid Services (CMS) require all Medicare and Medicaid providers and suppliers of medical services that qualify for a National Provider Identifier (NPI) to include NPI on all claims. Type 1 NPI is for Health care providers who are individuals, including physicians, psychiatrists and all sole proprietors. Type 2 NPI is for Health care providers that are organizations, including physician groups, hospitals, nursing homes, and the corporations formed when an individual incorporates him/herself.

MCEs should submit the individual NPI (Type1) for Servicing/Rendering, Referring, Prescribing, and Primary Care Providers in Provider file. MCEs should submit individual (Type 1) or group (Type 2) NPI for billing providers and PCCs.

MH DW will closely monitor submission of servicing/rendering, billing, and referring provider NPI numbers in Provider File. With a change of the business rules, claims with missing NPI numbers in Provider File might be rejected. Plans will be notified about the change ahead of time.
The above does not apply to "atypical" providers.

DRG
The DRG field (field #72) is a field requested by CMS. Not all plans collect DRGs so MassHealth has developed a preferred course of action:

1. A plan that collects DRGs- should provide DRG values in data submissions.
2. A plan that does not collect DRGs, should ensure that primary, secondary, and tertiary diagnosis values are as complete and accurate as possible, so that MassHealth may use a DRG grouper if necessary. Accurate procedure codes are also required for DRG assignment.
3. In the future, MassHealth may request that all plans provide DRGs.
4. MassHealth requests from MCEs that report DRGs to also report in DRG related fields: DRG Type, DRG Version, Severity of Illness level, and Risk of Mortality.

Diagnosis Codes
Requirements for validity and completeness are detailed in the ICD clinical guide that is published by the American Medical Association. Current validating process at MH DW requires that diagnosis codes contain the required number of digits outlined in the ICD code books.

At least one diagnosis code (in Primary Diagnosis field #19) is required for all provider type encounters as specified in section 8.0.
The values in all other Diagnosis fields listed in Data Elements section should be submitted when available.

Procedure Code
Many plans accept and use non-standard codes such as State specific and MCE specific codes. Current validating process at EHS DW looks for <u>standard codes only</u> - CPT, HCPCS, and ADA.

HIPPAA regulations require that only standard HCPCS Level I (CPT) and II be used for reporting and data exchange.
The only field containing procedure codes is the Procedure Code field (field #26).

Capitation Payments
Capitation payment arrangement refers to a periodic payment per member, paid in advance to health care providers for the delivery of covered services to each enrolled member assigned to them. The same amount is paid for each period regardless of whether the member receives the services during that period or not.
Note: Capitation payment is <u>not</u> "Bundled" payment, which is usually paid for Episodes of care or other bundled services.

Dollar Amounts
MassHealth wants to ensure that the dollar amounts on the individual lines of the claim represent the actual or computed amounts associated with each encounter. Therefore, whenever dollar amounts are not included at the detail level, and the summary-level line is not available, the MCE should add an extra detail line with a Record Indicator of 0 and report all summary-level amounts/quantities on that line. If the summary-level line is already available in the MCE's source system and is not artificially created, then it should have a Record Indicator 6 (Bundled Summary-Level line) **unless** other Record Indicator values apply (like, for example, 5 for DRG).
All detail lines with 0 dollar amounts (that are **not** artificially created and are **not** summary-level lines) should have any value **other than 0 or 6** placed in Record Indicator field. In such case, MCE decides on the value based on the definition of the Record Indicator in the table below.

For the claims covered by the capitation payments, MCEs must report either FFS equivalent amounts or amounts reported by the provider/vendor on their claims and use Record Indicator values 2 or 3 to indicate the type of payment arrangement.

Record Indicator Table:

Record Indicator	Dollar Amount Split
0: Artificial Line	Dollar amounts / quantities represent numbers that are available only at a summary level.
1: Fee-For-Service	Dollar amounts should be available at the detail line level in the source system.
2: Encounter Record with FFS equivalent	Dollar amounts should be available at the detail line level in the source system for a service provided under a capitation arrangement
3: Encounter Record w/out FFS equivalent	Dollar amount, if any, as reported by the provider or vendor to the MCE for a service provided under a capitation arrangement
4: Per Diem Payment	Total dollar amount for the entire stay. This is not the per-diem rate but the per-diem rate multiplied by the Quantity [numbers of days of inpatient admission. See Quantity]. If the amount applies to all lines on the claim, the claim must bring in a record with indicator = 0.
5: DRG Payment	Total dollar amount for the entire stay. If the amount applies to all lines on the claim, the claim must bring in a record with indicator = 0.
6: Bundled Summary-Level Line	Total dollar amount for a bundled summary-level claim line where the dollar amounts represent numbers that are available only at a summary line level in the source system and is not artificially created. A record with indicator = 6 for a **summary-level line of a bundled claim is used when none of the above payment arrangements apply**
7: Bundled detail line with 0 dollar amount	A bundled detail claim line where the dollar amounts are 0 or not available at the detail level. A record with indicator = 7 is used for a **detail-level line of a bundled claim when none of the above payment arrangements apply**

Below are few examples of possible scenarios for Record Indictor values:

Example 1 - Artificial Line 0 and Detail Lines with Record Indicator 4:

Claim Number	Claim Suffix	Record Indicator	Payment Amount
44444444444	1	4 - Per Diem Payment	0
44444444444	2	4 - Per Diem Payment	0
44444444444	3	4 - Per Diem Payment	0
44444444444	4	4 - Per Diem Payment	0
44444444444	5	0 - Artificial Line: dollar amounts available at summary level only	260

Example 2 - Artificial Line 0 and Detail Lines with Record Indicator 7:

Claim Number	Claim Suffix	Record Indicator	Payment Amount
55555555555	1	7 - Bundled detail line with 0 dollar amount	0
55555555555	2	7 - Bundled detail line with 0 dollar amount	0
55555555555	3	0 - Artificial Line: dollar amounts available at summary level only	100

Example 3 – Bundled Summary Line 6 and Detail Lines with Record Indicator 7:

Claim Number	Claim Suffix	Record Indicator	Payment Amount
66666666666	1	7 - Bundled detail line with 0 dollar amount	0
66666666666	2	7 - Bundled detail line with 0 dollar amount	0
66666666666	3	6 - Bundled Summary-Level Line	500

Example 4 – Bundled Summary Line 6 and Detail Lines with Record Indicator 1:

Claim Number	Claim Suffix	Record Indicator	Payment Amount
22222222222	1	1 - Fee-For-Service	0
22222222222	2	1 - Fee-For-Service	0
22222222222	3	6 - Bundled Summary-Level Line	500

Claim Number & Suffix
Every Original / Void or Replacement claim submitted to MassHealth should have a new claim number + suffix combination. There can be no duplicate claim number + claim suffix in one feed

Former Claim Number & Suffix
In order to void or replace old transactions, MassHealth requires for all the MCEs to add former claim number and former claim suffix to the claim lines of record type 'R', 'V'. The objective is to get a snapshot of the claims at the end of each period after all debit or credit transactions have been applied to them.

Examples:

Adjustments:

Claim Payer	Claim Number	Claim Suffix	Claim Category	Record Type	Former Claim Number	Former Claim Suffix	Payment Amount
XXX	11111111111	4	1	O			10
XXX	33333333333	4	1	R	11111111111	4	20
XXX	88888888888	4	1	R	33333333333	4	25

Voids:

Claim Payer	Claim Number	Claim Suffix	Claim Category	Record Type	Former Claim Number	Former Claim Suffix	Payment Amount
XXX	66666666666	1	1	O			15
XXX	77777777777	2	1	V	66666666666	1	10
XXX	99999999999	1	1	O			30

Record Creation Date
This is the date on which the claim was created in the MCE's database. If a replacement record represents the final result of multiple adjustments to a claim between submissions, Record Creation Date is the date of the last adjustment to that claim. For encounter records where Record Indicator value is 2 or 3, Record Creation Date should be the same as the Paid Date.

Inpatient Claim

Old, pre-November 2016, DW Logic
MassHealth applies a modified logic on encounter data to identify "Inpatient" claims. This new logic is an internal change that does not affect the encounter data submission process and only applies to the claims with "**From Service Date**" (field# 17) on or after October 1, 2016.

New DW Logic
Claims with Claim Category = 1 (Facility except LTC) and **Type of Bill** values **11x and 41x** are defined as "Inpatient". All other claims with Claim category = 1 are defined as "Outpatient".

LTC Claims
Claims with Claim Category = 6 (Long Term Care - Nursing Home, Chronic Care & Rehab) are defined as "**LTC**". MCEs should ***continue*** sending all "Long Term Care" claims with Claim Category='6'.

Physician-Administered Drug Claim Definition
Claims with Claim Category 1 (Facility except LTC) or 2 (Professional) and value in "NDC Number" field (#37).

Administrative Fees

Administrative Fees such as PBM fees should not be reported in the encounter data as part of the "Net Payment Amount". MCEs should inform EOHHS of any arrangement where these fees are included in their claims processing, and should work with their PBM or other agencies to separate out the administrative fees from the encounter cost component in their claim processing**.**

Bundle Indicator, Claim Number & Suffix

The Bundle indicator is a Y/N field to indicate that the claim line is part of a bundle. This indicator should always be 'Y' for **all** bundled claims (see example 1 and 2). The Bundle Claim Number and Suffix refer to the claim number and the claim suffix of the claim line with the bundled payment. The examples below illustrate how these two fields should be populated. Example 1 illustrates a scenario with one bundle within a claim, Example 2 illustrates a scenario with multiple bundles within a claim, and Example 3 illustrates a scenario with one bundle across multiple claims.

The assumption is that when a bundled claim line gets adjusted, all bundled claim lines for that claim would be adjusted as well. Please see Examples 4 and 5 below for scenarios where there is an adjustment of a bundled claim. MCE should leave the Bundle claim number and suffix blank when this assumption is inaccurate and when they do not have this information. However, these two fields are expected when MCE have this information in their system. Bundle Indicator should be provided on all bundled claims with no exception.

Example 1 – One Bundle per Claim Number:

Claim Payer	Claim Number	Claim Suffix	Bundle Ind	Bundle Claim Number	Bundle Claim Suffix	Payment Amount
XXX	AAAAAAAA	1	Y	AAAAAAAA	6	0
XXX	AAAAAAAA	2	Y	AAAAAAAA	6	0
XXX	AAAAAAAA	3	Y	AAAAAAAA	6	0
XXX	AAAAAAAA	4	Y	AAAAAAAA	6	0
XXX	AAAAAAAA	5	Y	AAAAAAAA	6	0
XXX	AAAAAAAA	6	Y	AAAAAAAA	6	120

Example 2 – Two Bundles per Claim Number:

Claim Payer	Claim Number	Claim Suffix	Bundle Ind	Bundle Claim Number	Bundle Claim Suffix	Payment Amount
XXX	CCCCCCCC	1	Y	CCCCCCCC	3	0
XXX	CCCCCCCC	2	Y	CCCCCCCC	3	0
XXX	CCCCCCCC	3	Y	CCCCCCCC	3	60
XXX	CCCCCCCC	4	Y	CCCCCCCC	6	0
XXX	CCCCCCCC	5	Y	CCCCCCCC	6	0
XXX	CCCCCCCC	6	Y	CCCCCCCC	6	80

Example 3 One Bundle for Two Claim Numbers:

Claim Payer	Claim Number	Claim Suffix	Bundle Claim Number	Bundle Claim Suffix	Payment Amount
XXX	DDDDDDDD	1	NNNNNNNN	1	0
XXX	DDDDDDDD	2	NNNNNNNN	1	0
XXX	DDDDDDDD	3	NNNNNNNN	1	0
XXX	NNNNNNNN	1	NNNNNNNN	1	50

Example 4 – Adjustment/Void of Bundled Claims with Record Indicator 0:

Claim Payer	Claim Number	Claim Suffix	Record Type	Former Claim Number	Former Claim Suffix	Bundle Claim Number	Bundle Claim Suffix	Payment Amount	Record Indicator	Procedure Code
XXX	44444444444	1	O			44444444444	4	0	4	96360
XXX	44444444444	2	O			44444444444	4	0	4	96375
XXX	44444444444	3	O			44444444444	4	0	4	96376
XXX	44444444444	4	O			44444444444	4	260	0	96366
XXX	55555555555	1	R	44444444444	1	55555555555	4	0	4	96360
XXX	55555555555	2	V	44444444444	2	55555555555	4	0	4	96375
XXX	55555555555	3	R	44444444444	3	55555555555	4	0	4	96376
XXX	55555555555	4	R	44444444444	4	55555555555	4	200	0	96366

Example 5 – Adjustment/Void of Bundled Claims with Record Indicator 6:

Claim Payer	Claim Number	Claim Suffix	Record Type	Former Claim Number	Former Claim Suffix	Bundle Claim Number	Bundle Claim Suffix	Payment Amount	Record Indicator	Procedure Code
XXX	66666666666	1	O			66666666666	3	0	7	96375
XXX	66666666666	2	O			66666666666	3	0	7	96376
XXX	66666666666	3	O			66666666666	3	500	6	96366
XXX	77777777777	1	R	66666666666	1	77777777777	3	0	7	96375

XXX	77777777777	2	V	66666666666	2	77777777777	3	0	7	96376
XXX	77777777777	3	R	66666666666	3	77777777777	3	400	6	96366

Submission Clarification Code

420-DK-Code indicating that the pharmacist is clarifying the submission.
MassHealth recognizes that submission clarification code value 20 indicates that prior to providing service, the pharmacy has determined the product being billed is purchased pursuant to right available under Section 340B of the Public Health Act of 1992 including sub-celling purchases authorized by section 340B(a)(10) and those made though the Prime Vendor Program 340B(a)(8).

For additional information about submission clarification code values, please refer to the NCPDP standards.

Provider ID submission in Encounter and Provider Files
Among several new elements introduced in Version 4.6 of the current document were Provider ID Address Location Code fields.
The values in the Provider ID, Provider ID Type, and Provider ID Address Location fields entered in claims file should match the values in corresponding fields of the provider file.

Example:

Claims File

Entity PIDSL	Claim Number	Claim Suffix	Servicing Provider ID	Servicing Provider ID Type	Servicing Provider ID Address Location Code
999999999R	98765432WS	1	1234569	6	A
999999999R	23568974RV	1	1234568	6	B
999999999R	741852969K	1	1234567	6	C
999999999R	369874123L	1	1234566	6	D

Provider File

Entity PIDSL	Provider ID	Provider ID Type	Address Location Code	Provider Bundle ID	Provider Last Name
999999999R	1234569	6	A	65656	Smith
999999999R	1234568	6	B	65656	Smith
999999999R	1234567	6	C	65656	Smith
999999999R	1234566	6	D	65656	Smith

3.0 Encounter Data Set Elements with Record Layout

Data Elements

This section contains field names and definitions for the encounter record. It is divided into five sections:

- Demographic Data
- Service Data
- Provider Data
- Financial Data
- Medicaid Program-Specific Data

For the fields that contain codified values (e.g. Patient Status), we use national standard (e.g. UB92 coding standards) values whenever possible.
In the table below 'X' indicates a Claim Category the data element is applicable in. The columns are labeled as:

- H – Facility (*except Long Term Care*)
- P – Professional
- L – Long Term Care
- R – Prescription Drug
- D – Dental

Programs with withhold amount
Some Managed Care programs include withhold risk-sharing arrangements with their providers when a portion of the approved payment amount is withheld from the provider payment amount and placed in a risk-sharing pool for later distribution. In such case, the withheld amount should be recorded in a separate field "Withhold Amount" (#69) and included in the amounts in the Eligible Charges and "Net Payment" (#68) fields.

Demographic Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization. **Code that identifies your Organization :** **ACO/MCO** 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England **SCO** 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan **One Care** 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	X	X	X	X	X	3	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
2	Claim Category	A code indicating the category of this claim. Valid values are: 1 = Facility (*except Long Term Care*) 2 = Professional (includes transportation claims) 3 = Dental 4 = Vision 5 = Prescription Drug 6 = Long Term Care *(Nursing Home, Chronic Care & Rehab)*	X	X	X	X	X	1	C
3	Entity PIDSL	ACO PIDSL on the ACO claims (an ACO with which a PCC is contracted with) or MCO PIDSL on the MCO claims or One Care Plan PIDSL on One Care claims or SCO PIDSL for SCO claims *Example*: 999999999A	X	X	X	X	X	10	C
4	Record Indicator	This information refers to the payment arrangement under which the rendering provider was paid. Value identifies whether the record was a fee-for-service claim, or a service provided under a capitation arrangement (encounter records). For encounter records, indicate whether or not there are Fee-For-Service (FFS) equivalents and payment amounts on the record. 0 Artificial record – Refers to a line item inserted to hold amounts / quantities available only at a summary (claim) level. 1 Claim Record – Refers to a claim paid on a Fee-For-Service (FFS) basis 2 Encounter Record with FFS equivalent - Refers to services provided under a capitation arrangement and for which an FFS equivalent is given 3 Encounter Record w/out FFS equivalent - Refers to services provided under a capitation arrangement but for which no FFS equivalent is available 4 Per Diem Payment - Refers to a record for an inpatient stay paid on a per diem basis. 5 DRG Payment - Refers to a record for an inpatient stay paid on a DRG basis 6 Bundled Summary-Level Line – Refers to a record with a bundled summary-level amounts/quantities as available in the MCE source system. Use this value when none of the above values apply. 7 Bundled detail line with 0 dollar amount – Refers to a bundled detail claim line where the dollar amounts are 0 or not available at the detail level. Use this value when none of the above values apply ***See discussion under Dollar Amounts in the Data Elements Clarification Section.***	X	X	X	X	X	1	C
5	Claim Number	A unique number assigned by the administrator to this claim (e.g., ICN, TCN, DCN). It is very important to include a Claim Number on each record since this will be	X	X	X	X	X	15	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		the key to summarizing from the service detail to the claim level. ***See discussion under <u>Claim Number/Suffix</u> in the Data Elements Clarification Section***							
6	Claim Suffix	This field identifies the line or sequence number in a claim with multiple service lines. ***See discussion under <u>Claim Number/Suffix</u> in the Data Elements Clarification Section***	X	X	X	X	X	4	C
7	Pricing Indicator	Pricing Indicator; currently it is a subject of internal discussion. MCEs will be notified when decision is made.						20	C
8	Recipient DOB	The birth date of the patient expressed as YYYYMMDD. For example, August 31, 1954, would be coded "19540831".	X	X	X	X	X	8	D/YYYYMMDD
9	Recipient Gender	The gender of the patient: 1 = Male 2 = Female 3 = Other	X	X	X	X	X	1	C
10	Recipient ZIP Code	The ZIP Code of the patient's residence as of the date of service.	X	X	X	X	X	5	N
11	Medicare Code	A code indicating if Medicare coverage applies and, if so, the type of Medicare coverage. Medicare code should indicate what part of Medicare is being used to cover the <u>services</u> billed within the claim, NOT all of the parts of Medicare that the member is enrolled in. 0= No Medicare 1 = Part A Only 2 = Part B Only 3 = Part A and B **4 = Part D Only** **5 = Part A and D** **6 = Part B and D** **7 = Part A, B, and D**	X	X	X	X	X	1	N

Service Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
12	Other Insurance Code	A Yes/No flag that indicates whether or not third party liability exists. 1 = Yes; 2 = No	X	X	X	X	X	1	C
13	Submission Clarification Code	420-DK- Code indicating that the pharmacist is clarifying the submission. Please refer to *Segment "2.0 Data Element Clarifications"* for the details.				X		7	N
14	Claim Type	BH Vendor Specific field	X	X	X	X	X	18	C
15	Admission Date	For facility services, the date the recipient was admitted to the facility. The format is YYYYMMDD.	X		X				
16	Discharge Date	For facility services, the date the recipient was discharged from the facility. The format is YYYYMMDD. Cannot be prior to Admission Date.	X		X			8	D/YYYYMMDD
17	From Service Date	The actual date the service was rendered; if services were rendered over a period of time, this is the date of the first service for this record. The format is YYYYMMDD.	X	X	X	X	X	8	D/YYYYMMDD
18	To Service Date	The last date on which a service was rendered for this record. The format is YYYYMMDD.	X	X	X		X	8	D/YYYYMMDD
19	Primary Diagnosis	The ICD diagnosis code chiefly responsible for the hospital confinement or service provided. The code should be left justified, coded to the fifth digit when applicable (blank filled when less than five digits are applicable). *DO NOT include decimal points in the code.* ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X		X	7	C/ No decimal points (780.31 must be entered as 78031)
20	Secondary Diagnosis	The ICD diagnosis code explaining a secondary or complicating condition for the service. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
21	Tertiary Diagnosis	The tertiary ICD diagnosis code. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
22	Diagnosis 4	The fourth ICD diagnosis code. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
23	Diagnosis 5	The fifth ICD diagnosis code. See above for format. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
24	Type of Admission	Should be valid and present on all Hospital and Long Term Care claims with hospital admission. For the UB standard values see Table A.	X		X			1	C
25	Source of Admission	Should be valid and present on all Hospital and Long Term Care claims with hospital admission. For the UB standard values see Table B	X		X			1	C
26	Procedure Code	A code explaining the procedure performed. This code may be any valid code included in the coding systems identified in the Procedure Type field below. *Any internal coding systems used must be translated to one of the coding systems identified in field #**30** below.* Should not contain ICD procedure codes. All ICD procedure codes should be submitted in the surgical procedure code fields (#101 – #113) ***including the ICD-treatment procedure codes***	X	X	X		X	6	C

		See discussion in Data Element Clarifications section.							
27	Procedure Modifier 1	A current procedure code modifier (CPT or HCPCS) corresponding to the procedure coding system used, when applicable.	X	X	X		X	2	C
28	Procedure Modifier 2	Second procedure code modifier, required, if used.	X	X	X		X	2	C
29	Procedure Modifier 3	Third procedure code modifier, required, if used.	X	X	X		X	2	C
30	Procedure Code Indicator	A code identifying the type of procedure code used in field#26: 2= CPT or HCPCS Level 1 Code 3= HCPCS Level II Code 4= HCPCS Level III Code (State Medicare code). 5= American Dental Association (ADA) Procedure Code (Also referred to as CDT code.) 6= State defined Procedure Code 7= Plan specific Procedure Code ICD procedure codes should go in Surgical Procedure code fields (Field # 103 – 111) *State defined procedure codes should be used, when coded, for services such as EPSDT procedures.* ***See discussion in the Data Element Clarifications section.***	X	X	X		X	1	N
31	Revenue Code	For facility services, the UB Revenue Code associated with the service. *Only standard UB92 Revenue Codes values are allowed; plans may* ***not*** *use "in house" codes. Values should be sent in 4 digit format. Revenue codes less than 4 digits long should be submitted with leading zeros. For Example:* *a. Revenue code -1 - as '0001';* *b. Revenue Code 23 - as '0023;* *c. Revenue code 100 - as '0100';* *Revenue Code 2100 – as '2100'.*	X		X			4	C
32	Place of Service	This field hosts Place of Service (POS) that comes on the Professional claim). See Table C for CMS 1500 standard		X			X	2	C
33	Type Of Bill	For encounter data supporting UB claims submission the Type of Bill is submitted as a 3-digit bill type in accordance with national billing guideline. The first two digits denote the place of services and the third digits denotes the frequency. See Table D for UB Type of Bill values indicating place. ***Note*****:** for UB Type of Bill, use the 1st and 2nd positions only.) Frequency values can be found in Table K and are documented in field # ***91 as well.***	X		X			3	C
34	Patient Discharge Status	This is 2-digit Discharge Status Code (UB Patient Status) for hospital admissions. Values from 1 to 9 should always be entered with leading '0'. Examples: a. Patient Discharge Status '1' should be submitted as '01'; b. Patient Discharge Status '19' should be submitted as '19'.	X		X			2	C
35	Filler							2	C

36	Quantity	This value represents the actual quantity and should be submitted with decimal point when applicable. For inpatient admissions, the number of days of confinement. Count the day of admission but not the day of discharge (for admission and discharge on the same day, Quantity is counted as 1). For all other procedures, the number of units performed for this procedure. For most procedures, this number should be "1". In some cases, a procedure may be repeated, in which case this number should reflect the number of times the procedure was performed. For anesthesia services, this should be the total number of minutes that make up the beginning and ending clock time of anesthesia service administered. Please make sure that the Quantity corresponds to the procedure code. For example, if the psychiatric code 90844 is used (Individual psychotherapy, 45-50 minutes), the Quantity should be "1" NOT "45" or "50". For Inpatient records, it should represent number of days of care. Values of 30, 60 or 1 00 are most common on drug records. *Note*: Length of this field has been increased to accommodate the actual quantity. Quantity=10 should be submitted as 10; Quantity=10.5 should be submitted as 10.5; Quantity=10.55 should be submitted as 10.55	X	X	X		X	9	SN
37	NDC Number	For prescription drugs, the valid National Drug Code number assigned by the Food and Drug Administration (FDA). For Compound drugs claims submit NDC Number for the primary drug, If primary drug is unknown, submit NDC Number for most expensive drug. NDC codes having less than 11 digits should be submitted with leading 0's. For Example NDC "603373932" should be submitted as "00603373932".	X	X		X		11	N
38	Metric Quantity	For prescription drugs, the total number of units or volume (e.g., tablets, milligrams) dispensed. Should be submitted with decimal point when applicable. Note: Length of this field has been increased to accommodate the actual Metric Quantity. Metric Quantity=10 should be submitted as 10; Metric Quantity=10.5 should be submitted as 10.5; Metric Quantity=10.55 should be submitted as 10.55	X	X		X		9	N
39	Days Supply	The number of days of drug therapy covered by this prescription.				X		3	N
40	Refill Indicator	A number indicating whether this is an original prescription (0) or a refill number (e.g., 1, 2, 3, etc.) on Pharmacy claims.				X		2	N
41	Dispense As Written Indicator	An indicator specifying why the product dispensed was selected by the pharmacist and should be entered in a 2 digit format with leading zero: 00 = No DAW 01 = Physician DAW 02 = Patient DAW 03 = Pharmacist DAW 04 = Generic Not In Stock				X		2	N

		05 = Brand Dispensed as Generic 06 = Override 07 = Brand Mandated by Law 08 = No Generic Available 09 = Other							
42	Dental Quadrant	One of the four equal sections into which the dental arches can be divided; begins at the midline of the arch and extends distally to the last tooth. 1 = Upper Right 2 = Upper Left 3 = Lower Left 4 = Lower Right					X	1	N
43	Tooth Number	The number or letter assigned to a tooth for identifications purposes as specified by the American Dental Association. A - T (for primary teeth) 1 - 32 (for secondary teeth)					X	2	C
44	Tooth Surface	The tooth surface on which the service was performed: M = Mesial D = Distal O = Occlusal L = Lingual I = Incisal F = Facial B = Buccal A = All 7 surfaces This field can list up to six values. When multiple surfaces are involved, please list the value for each surface without punctuation between values. For example, work on the mesial, occlusal, and lingual surfaces should be listed as "MOL "(three spaces following the third value).					X	6	C
45	Paid Date	For encounter records, the date on which the record was processed. For services performed on a fee-for-service basis, the date on which the claim was paid. The format is YYYYMMDD.	X	X	X	X	X	8	D/YYYYMMDD
46	Service Class	BH Vendor Specific field	X	X	X	X	X	23	C

Provider Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
47	PCP Provider ID	A unique identifier for the Primary Care Physician selected by the patient as of the date of service. ***See discussion in the Data Element Clarifications section.***	X	X	X		X	15	C
48	PCP Provider ID Type	A code identifying the type of ID provided in PCP Provider ID above. For example, 6 = Internal ID (Plan Specific)	X	X	X		X	1	N
49	PCC Internal Provider ID	PCC Internal ID	X	X	X	X	X	15	C
50	Servicing Provider ID	A unique identifier for the provider performing the service. ***See discussion in the Data Element Clarifications section.***	X	X	X	X	X	15	C
51	Servicing Provider ID Type	A code identifying the type of ID provided in Servicing Provider ID above. For example, 6 = Internal ID (Plan Specific) 9 = NAPB Number (for pharmacy claims only)	X	X	X	X	X	1	N
52	Referring Provider ID	A unique identifier for the provider. ***See discussion in the Data Element Clarifications section.***	X	X	X	X	X	15	C
53	Referring Provider ID Type	A code identifying the type of ID provided in Referring Provider ID above. For example, 1 = NPI 6 = Internal ID (Plan Specific) 8 = DEA Number (for pharmacy claims only)	X	X	X	X	X	1	N
54	Servicing Provider Class	A code indicating the class for this provider: 1 = Primary Care Provider 2 = In plan provider, non PCP 3 = Out of plan provider Note: This code relates to the class of the provider and a PCP does not necessarily indicate the recipient's selected or assigned PCP. PCP class should be assigned only to those physicians whom the plan considers to be a participating PCP.	X	X	X	X	X	1	C
55	Servicing Provider Type	A code indicating the type of provider rendering the service represented by this encounter or claim. (Use Servicing Provider Type values, see Table G)	X	X	X	X	X	3	N
56	Servicing Provider Specialty	The specialty code of the servicing provider. (Use CMS 1500 standard, see Table H)	X	X	X		X	3	C
57	Servicing Provider ZIP Code	The servicing provider's ZIP code. The ZIP code where the service occurred is preferred.	X	X	X	X	X	5	N
58	Billing Provider ID	A unique identifier for the provider billing for the service.	X	X	X	X	X	15	C
59	Authorization Type	BH Vendor Specific field	X	X	X	X	X	25	C

Financial Data

Most of the fields below apply to services for which reimbursement is made on a fee-for-service basis. For capitated services, the record should include fee-for-service equivalent information when available. Line item amounts are required for these fields.

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
60	Billed Charge	The amount the provider billed for the service.	X	X	X	X	X	9	SN
61	Gross Payment Amount	The amount that the provider was paid in total by all sources for this service. *NOTE: This field should include any withhold amount, if applicable.*	X	X	X	X	X	9	SN
62	TPL Amount	Any amount of third party liability paid by another medical coverage carrier for this service. If the TPL amount is available only at the summary level, it must be recorded on a special line on the claim which will have a record indicator value of 0. See Dollar Amounts.	X	X	X	X	X	9	SN
63	Medicare Amount	Any amount paid by Medicare for this service.	X	X	X	X	X	9	SN
64	Copay/ Coinsurance	Any co-payment amount the member paid for this service.	X	X	X	X	X	9	SN
65	Deductible	Any deductible amount the member paid for this service.	X	X	X	X	X	9	SN
66	Ingredient Cost	The cost of the ingredients included in the prescription.				X		9	SN
67	Dispensing Fee	The dispensing fee charged for filling the prescription.				X		9	SN
68	Net Payment	The amount the Medicaid MCE paid for this service. (Should equal Eligible Charges less COB, Medicare, Copay/Coinsurance, and Deductible.)	X	X	X	X	X	9	SN
69	Withhold Amount	Any amount withheld from fee-for-service payments to the provider to cover performance guarantees or as incentives.	X	X	X		X	9	SN
70	Record Type	A code indicating the type of record: O = Original V = Void or Back Out R = Replacement A = Amendment ***See discussion under 'Former Claim Number / Suffix' in the Data Elements Clarification Section***	X	X	X	X	X	1	C
71	Group Number	For non-MHSA MCEs 1 = MCO MassHealth 2 = MCO Commonwealth Care 3 = SCO 5 = CarePlus 6 = One Care (ICO) 7 = ACO-A 8 = ACO-B 9 = ACO-C	X	X	X	X	X	25	C

Medicaid Program-Specific Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
72	DRG	The DRG code used to pay for an inpatient confinement and should always be submitted in 3- digit format. One and two digit codes should be completed with leading zeros to comply. For example: a. DRG code '1' should be submitted as '001'; b. DRG code '25' should be submitted as '025'; c. DRG code '301' should be submitted as '301'. ***See discussion in the Data Element Clarifications section***.	X		X			3	C
73	EPSDT Indicator	A flag that indicates those services which are related to EPSDT: 1 = EPSDT Screen 2 = EPSDT Treatment 3 = EPSDT Referral		X			X	1	N
74	Family Planning Indicator	A flag that indicates whether or not this service involved family planning services, which may be matched by CMS at a higher rate: 1 = Family planning services provided 2 = Abortion services provided 3 = Sterilization services provided 4 = No family planning services provided (see Table I)	X	X		X		1	C
75	MSS/IS	*Please leave this field blank, it will be further defined at a later date.* A flag that indicates services related to MSS/IS: 1 = Maternal Support Services 2 = Infant Support Services		X				1	N
76	New Member ID	The ***"Active" Medicaid*** identification number assigned to the individual. This number is assigned by MassHealth and may change.	X	X	X	X	X	25	C

Other Fields

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
77	Former Claim Number	If this is not an Original claim [Record Type = 'O'], then the previous claim number that this claim is replacing/voiding. ***See discussion under Former Claim Number / Suffix in the Data Elements Clarification Section***	X	X	X	X	X	15	C
78	Former Claim Suffix	If this is not an Original claim [Record Type = 'O'], then the previous claim suffix that this claim is replacing/voiding. ***See discussion under Former Claim Number / Suffix in the Data Elements Clarification Section***	X	X	X	X	X	4	C
79	Record Creation Date	The date on which the record was created. ***See discussion under Record Creation Date in the Data Elements Clarification Section.***	X	X	X	X	X	8	D
80	Service Category	Service groupings from financial reports like 4B (see Table I)	X	X	X	X	X	3	C
81	Prescribing Prov. ID	Federal Tax ID or UPIN or other State assigned provider ID for the prescribing provider on the Pharmacy claim.				X		15	C
82	Date Script Written	Date prescribing provider issued the prescription.				X		8	D/YYYYMMDD
83	Compound Indicator	Indicates that the prescription was a compounded drug. 1 = Yes 2 = No				X		1	C
84	Rebate Indicator	PBM received rebate for drug dispensed. 1 = Yes 2 = No				X		1	C
85	Admitting Diagnosis	Diagnosis upon admission. May be different from principal diagnosis. Should not be External Injury codes. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
86	Allowable Amount	Amount allowed under the Health Plan formulary.	X	X	X	X	X	9	N
87	Attending Prov. ID	Provider ID of the provider who attended at facility. Federal Tax ID or UPIN or other State assigned provider ID.	X					15	C
88	Non-covered Days	Days not covered by Health Plan.	X		X			3	N
89	External Injury Diagnosis 1	If there is an External Injury Diagnosis code 1 (ICD E-Code) present on the claim, it should be submitted in this field. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C
90	Claim Received Date	Date claim received by Health Plan, if processed by a PBM.				X		8	D/YYYYMMDD
91	Frequency	The third digit of the UB92 Bill Classification field. Submitted as a third digit in Type of Bill (#33)	X		X			1	C
92	PCC Internal Provider ID_Type	One code identifying the type of ID provided in the PCC Internal Provider ID in Field # 49 above For example,	X	X	X	X	X	1	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		6 = Internal ID (Plan Specific) 8 = DEA Number 9 = NABP Number 1 = NPI							
93	Billing Provider ID _Type	A code identifying the type of ID provided in Billing Provider ID above. For example, 6 = Internal ID (Plan Specific) *9 = NABP Number* (for pharmacy claims only)	X	X	X	X	X	1	N
94	Prescribing Prov. ID _Type	A code identifying the type of ID provided in Prescribing Provider ID above. For example, 1 = NPI 6 = Internal ID (Plan Specific) 8 = DEA Number				X		1	N
95	Attending Prov. ID _Type	A code identifying the type of ID provided in Attending Prov. ID above. For example, *6 = Internal ID (Plan Specific)*	X					1	N
96	Admission Time	For inpatient facility services, the time the recipient was admitted to the facility. If not an inpatient facility, the value should be missing. This field ***must*** be in HH24MI format. For example, 10:30AM would be 1030 and 10:30PM would be 2230.	X		X			4	
97	Discharge Time	For inpatient facility services, the time the recipient was discharged from the facility. If not an inpatient facility, the value should be missing. This field ***must*** be in HH24MI format. For example, 10:30AM would be 1030 and 10:30PM would be 2230.	X		X			4	N/HH24MI
98	Diagnosis 6	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
99	Diagnosis 7	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
100	Diagnosis 8	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
101	Diagnosis 9	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
102	Diagnosis 10	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
103	Surgical Procedure code 1	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
104	Surgical Procedure code 2	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
105	Surgical Procedure code 3	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
106	Surgical Procedure code 4	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank.	X					7	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							
107	Surgical Procedure code 5	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
108	Surgical Procedure code 6	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
109	Surgical Procedure code 7	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
110	Surgical Procedure code 8	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
111	Surgical Procedure code 9	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
112	Employment	Is the patient's condition related to Employment Y N	X	X	X	X	X	1	C
113	Auto Accident	Is the patient's condition related to an Auto Accident Y N	X	X	X	X	X	1	C
114	Other Accident	Is the patient's condition related to Other Accident Y N	X	X	X	X	X	1	C
115	Total Charges	This field represents the total charges, covered and uncovered related to the current billing period.	X	X	X	X	X	9	N
116	Non Covered charges	This field represents the uncovered charges by the payer related to the revenue code. This is the amount, if any, that is not covered by the primary payer for this service.	X	X	X	X	X	9	N
117	Coinsurance	Any coinsurance amount the member paid for this service.	X	X	X	X	X	9	N
118	Void Reason Code	The reason the claim line was voided 1 TPL 2 accident recovery 3 provider audit recoveries 4 Other	X	X	X	X	X	1	C
119	DRG Description	Description of DRG Code	X		X			132	C
120	DRG Type	*Values:* 1=Medicare CMS-DRG 2=Medicare MS-DRG 3=Refined DRGs (R-DRG)	X		X			1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		4=All Patient DRGs (AP-DRG) 5=Severity DRGs (S-DRG) 6=All Patient, Severity-Adjusted DRGs (APS-DRG) 7=All Patient Refined DRGs (APR-DRG) 8=International-Refined DRGs (IR-DRG) 9=Other ***Please use the accurate and specific DRG type and avoid using the value "Other". Please communicate to MassHealth any DRG types you are using that are missing from the above list***							
121	DRG Version	DRG Version number associated with DRG type	X		X			3	C/ No decimal points (26.1 must be entered as 261)
122	DRG Severity of Illness Level	A code that describes the Severity of the claim with the assigned DRG: Valid values are: 1 = minor 2 = moderate 3 = major 4 = extreme ***Associated with DRG Type=APR-DRG (DRT Type =7) or any other DRG that has these fields***	X		X			1	C
123	DRG Risk of Mortality Level	A code that describes the Mortality of the patient with the assigned DRG code. Valid values are: 1 = minor 2 = moderate 3 = major 4 = extreme ***Associated with DRG Type=APR-DRG (DRT Type =7) or any other DRG that has these fields.***	X		X			1	C
124	Patient Pay Amount	Patient paid amount for nursing facility stays and hospitals	X		X			9	SN
125	Patient Reason for Visit Diagnosis 1	ICD diagnosis code describing the patient's (or patient representative's) stated reason for seeking care at the time of outpatient (ER) visit ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
126	Patient Reason for Visit Diagnosis 2	ICD diagnosis code describing the patient's (or patient representative's) stated reason for seeking care at the time of outpatient (ER) visit ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
127	Patient Reason for Visit Diagnosis 3	ICD diagnosis code describing the patient's (or patient representative's) stated reason for seeking care at the time of outpatient (ER) visit ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
128	Present on Admission (POA) 1	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
129	Present on Admission (POA) 2	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
130	Present on Admission (POA) 3	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
131	Present on Admission (POA) 4	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
132	Present on Admission (POA) 5	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
133	Present on Admission (POA) 6	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
134	Present on Admission (POA) 7	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
135	Present on Admission (POA) 8	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
136	Present on Admission (POA) 9	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
137	Present on Admission (POA) 10	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
138	Diagnosis 11	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points (26.1 must be entered as 261)
139	Present on Admission (POA) 11	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
140	Diagnosis 12	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points (26.1 must be entered as 261)
141	Present on Admission (POA) 12	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
142	Diagnosis 13	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
143	Present on Admission (POA) 13	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
144	Diagnosis 14	The ICD diagnosis code.	X		X			7	C/ No decimal points

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							(26.1 must be entered as 261)
145	Present on Admission (POA) 14	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
146	Diagnosis 15	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
147	Present on Admission (POA) 15	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
148	Diagnosis 16	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
149	Present on Admission (POA) 16	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
150	Diagnosis 17	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
151	Present on Admission (POA) 17	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
152	Diagnosis 18	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
153	Present on Admission (POA) 18	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
154	Diagnosis 19	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
155	Present on Admission (POA) 19	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
156	Diagnosis 20	The ICD diagnosis code.	X		X			7	C/ No decimal

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							points (26.1 must be entered as 261)
157	Present on Admission (POA) 20	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
158	Diagnosis 21	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
159	Present on Admission (POA) 21	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
160	Diagnosis 22	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
161	Present on Admission (POA) 22	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
162	Diagnosis 23	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
163	Present on Admission (POA) 23	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
164	Diagnosis 24	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
165	Present on Admission (POA) 24	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
166	Diagnosis 25	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
167	Present on Admission (POA) 25	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
168	Diagnosis 26	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
169	Present on Admission (POA) 26	This is an indicator that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
170	Present on Admission (POA) EI 1	This is an indicator associated with External Injury Diagnosis 1 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
171	External Injury Diagnosis 2	If there is an External Injury Diagnosis code 2 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
172	Present on Admission (POA) EI 2	This is an indicator associated with External Injury Diagnosis 2 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
173	External Injury Diagnosis 3	If there is an External Injury Diagnosis code 3 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
174	Present on Admission (POA) EI 3	This is an indicator associated with External Injury Diagnosis 3 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
175	External Injury Diagnosis 4	If there is an External Injury Diagnosis code 4 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
176	Present on Admission (POA) EI 4	This is an indicator associated with External Injury Diagnosis 4 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
177	External Injury Diagnosis 5	If there is an External Injury Diagnosis code 5 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
178	Present on Admission (POA) EI 5	This is an indicator associated with External Injury Diagnosis 5 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
179	External Injury Diagnosis 6	If there is an External Injury Diagnosis code 6 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
180	Present on Admission (POA) EI 6	This is an indicator associated with External Injury Diagnosis 6 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
181	External Injury Diagnosis 7	If there is an External Injury Diagnosis code 7 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
182	Present on Admission (POA) EI 7	This is an indicator associated with External Injury Diagnosis 7 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
183	External Injury Diagnosis 8	If there is an External Injury Diagnosis code 8 (ICD-E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
184	Present on Admission (POA) EI 8	This is an indicator associated with External Injury Diagnosis 8 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
185	External Injury Diagnosis 9	If there is an External Injury Diagnosis code 9 (ICD E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
186	Present on Admission (POA) EI 9	This is an indicator associated with External Injury Diagnosis 9 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
187	External Injury Diagnosis 10	If there is an External Injury Diagnosis code 10 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
188	Present on Admission (POA) EI 10	This is an indicator associated with External Injury Diagnosis 10 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
189	External Injury Diagnosis 11	If there is an External Injury Diagnosis code 11 (ICD- E-Code) present on the claim, it should be submitted in this field.	X		X			7	C/ No decimal points (26.1

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							must be entered as 261)
190	Present on Admission (POA) EI 11	This is an indicator associated with External Injury Diagnosis 11 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
191	External Injury Diagnosis 12	If there is an External Injury Diagnosis code 12 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/ No decimal points (26.1 must be entered as 261)
192	Present on Admission (POA) EI 12	This is an indicator associated with External Injury Diagnosis 12 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
193	ICD Version Qualifier	ICD9 or ICD10. The value "ICD9" must be populated on claim records with either ICD-9-CM diagnosis codes or ICD-9-CM procedure codes. The value "ICD10" must be populated on claim records with either ICD-10-CM diagnosis codes or ICD-10-CM procedure codes. One claim record must ***never*** have a combination of ICD9 and ICD10 codes. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X		X	5	C
194	Procedure Modifier 4	4th procedure code modifier, required, if used.	X	X	X		X	2	C
195	Service Category Type	This field describes the Type of Financial reports the service category is based on. The values are: '4B' for MCO Service Categories 'ACO' for ACO Categories 'SCO' for SCO Service Categories 'ICO' for Care One (ICO) Service Categories	X	X	X	X	X	3	C
196	Ambulance Patient Count	AMBULANCE PATIENT COUNT. REQUIRED WHEN MORE THAN ONE PATIENT IS TRANSPORTED IN THE SAME VEHICLE FOR AMBULANCE OR NON-EMERGENCY TRANSPORTATION SERVICES.		X				3	N
197	Obstetric Unit Anesthesia Count	The number of additional units reported by an anesthesia provider to reflect additional complexity of services.		X				5	N
198	Prescription Number	Rx Number.				X		15	C
199	Taxonomy Code	This is the Taxonomy code for Servicing Provider identified on the claim. Taxonomy codes are National specialty codes used by providers to indicate their	X	X	X		X	10	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		specialty. These codes can be found on the Website of Centers for Medicare & Medicaid Service (CMS)							
200	Rate Increase Indicator	Indicates if the provider is eligible to receive the enhanced primary care rate ***for this service***, as specified in the Affordable Care Act – Section 1202 final regulations. 1=Yes 2=No 3=Unknown 4=Not Applicable **Note: If a service is considered eligible based on the ACA regulations, then the value should be equal to "1" even if the MCE is already paying the provider at the higher rate.**	X	X	X			1	C
201	Bundle Indicator	Indicates if the claim line is part of a bundle. Values: Y=Yes, the claim line is part of a bundle. All bundled lines including the line with the bundled payment should have a value of 'Y' N=No, the claim line is not part of a bundle.	X	X	X	X	X	1	C
202	Bundle Claim Number	This is the claim number of the claim line with the bundled payment. ***See discussion in Data Element Clarifications section,***	X	X	X	X	X	15	C
203	Bundle Claim Suffix	This the claim suffix of the claim line with the bundled payment. ***See discussion in Data Element Clarifications section,***	X	X	X	X	X	4	C
204	Value Code	Code used to relate values to identify data elements necessary to process a UB92 claim. Submit only when the value=54 for Newborn claims	X					2	AN
205	Value Amount	Weight of a newborn in grams. Must be present on all newborn claims when the value code "54"is submitted in Field #204	X					9	N
206	Surgical Procedure Code 10	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
207	Surgical Procedure Code 11	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
208	Surgical Procedure Code 12	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
209	Surgical Procedure Code 13	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
210	Surgical Procedure Code 14	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
211	Surgical Procedure Code 15	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
212	Surgical Procedure Code 16	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
213	Surgical Procedure Code 17	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
214	Surgical Procedure Code 18	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
215	Surgical Procedure Code 19	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
216	Surgical Procedure Code 20	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
217	Surgical Procedure Code 21	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
218	Surgical Procedure Code 22	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
219	Surgical Procedure Code 23	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
220	Surgical Procedure Code 24	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
221	Surgical Procedure Code 25	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank.	X					7	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							
222	Attending Prov. ID Address Location Code	Code to identify address location of Attending Provider ID in field #87	X					15	C
223	Billing Provider ID Address Location Code	Code to identify address location of Billing Provider ID in field # 58	X	X	X	X	X	15	C
224	Prescribing Prov. ID Address Location Code	Code to identify address location of Prescribing Provider ID in field # 81				X		15	C
225	PCP Provider ID Address Location Code	Code to identify address location of PCP Provider ID in field # 47	X	X	X	X	X	15	C
226	Referring Provider ID Address Location Code	Code to identify address location of Referring Provider ID in filed # 52	X	X	X			15	C
227	Servicing Provider ID Address Location Code	Code to identify address location of Servicing Provider ID in field # 50	X	X	X	X	X	15	C
228	PCC Provider ID Address Location Code	Code to identify address location of PCC Internal Provider ID In field **# 49**	X	X	X	X	X	15	C
229	Submission Clarification Code 2	420-DK- Code indicating that the pharmacist is clarifying the submission. Please refer to *Segment "2.0 Data Element Clarifications"* for the details.				X		7	N
230	Submission Clarification Code 3	420-DK- Code indicating that the pharmacist is clarifying the submission. Please refer to *Segment "2.0 Data Element Clarifications"* for the details.				X		7	N
231	Unit of Measure	To be provided on all Pharmacy and Physician-Administered Drugs claims. A unit of the value entered in "Metric Quantity" field (# 38). Please refer to Table O for the allowed values, standard references and available links	X	X		X		2	C
232	Provider Payment	The Gross Amount that the Plan/PBM paid to the pharmacy for the claim						9	SN
233	Filler							9	SN

Please see Key to Data Types on the next page

*** Key to Data Types**

C *Character*
Includes space, A-Z (upper or lower case), 0-9
Left justified with trailing blanks.
Unrecorded or missing values are blank

N *Numeric*
Include 0-9.
Right justified, lead-zero filled.
Unrecorded or missing values are blank

D *Date Fields*
Dates should be in a numeric format. The format for all dates is eight digits in YYYYMMDD format, where YYYY represents a four digit year, MM = numeric month indicator (01 - 12); DD = numeric day indicator (01 - 31).
Example: November 22, 1963 = 19631122

Financial Fields

MassHealth prefers to receive both dollars and cents, with an **implied decimal point** before the last two digits in the data.
Example: the data string "1234567" would represent $12,345.67
Please do not include the actual decimal point in the data.

3.1 Provider Data Set with Record Layout

Data Elements

This section contains field names and definitions for the provider record. To be able to link providers across the MCEs, it is essential to accurately report as many data elements as possible.

Provider file has to contain a snapshot of complete provider data at the time the provider file is created for encounter data submission.

All locations for Provider ID and Provider ID Type are expected to be sent in the provider file, and service location - in the encounter file. For Billing Providers the primary address location should be included in the encounter file.

To reflect the changes in provider contract status, an MCE should provide one record per provider/location with the effective and term dates populated accurately. In this case, the effective and term dates per Provider ID/Provider ID Type/location will not overlap.

Effective and Term dates should ***not*** be blank. Providers, who are enrolled with the MCE at the time of the data submission, are expected to have "End of Time" as a Term date in that submission. The preferred value for the "End of Time" field is '99991231'.

Providers with multiple servicing sites or addresses ***must*** have different IDs for each location.

File Processing

I. The values should be submitted in all fields when available including:
   1. Tax Id Number when available (filed#30)
   2. APCD ORG ID when available in APCD data (filed#34)

II. 100% of providers on Pharmacy and Physician-Administered Drugs claims must have:
   1. NPI (Field #2) value

III. Reject the file if:
   1. NPI is missing on more than 20% of the records. At least 80% of the records should have NPI
   2 Provider Type is missing on more than 20% of the records.
   At least 80% of the records should have Provider Type entered
   3 Provider ID, or Provider ID Type, or Provider ID Location Code are missing

The following fields are 100% required on all records:

1. Org. Code (Field #1)
2. Provider ID (Field #2)
3. Provider ID Type (Field #3)
4. Provider last Name (Field #4)
5. Provider First Name (Field #5)
6. Provider Office Address Street (Field #8)
7. Provider Office Address City (Field #9)
8. Provider Office Address State (Field #10)
9. Provider Office Address Zip (Field #11)
10. Provider Mailing Address Street (Field #12)
11. Provider Mailing Address City (Field #13)
12. Provider Mailing Address State (Field #14)
13. Provider Mailing Address zip (Field #15)
14. Provider Effective Date (Field #18)
15. Provider Term Date (Field #19)
16. Provider DEA Number when applicable (Field #24)
17. Provider ID Address Location Code (Field#36)
18. Provider Bundle ID (Field #40)
19. Entity PIDSL (Field# 35)

#	Field Name	Definition/Description	Length	Data Type
1	Org.Code	Unique ID assigned by MH DW to each submitting organization. **This code identifies your Organization :** 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	3	N
2	Provider ID	Multiple formats for the same Provider ID must be avoided. For example, ID '00001111' and '001111' should be submitted with one consistent format if it indicates the same ID for the same provider.	15	C
3	Provider ID Type	A code identifying the type of ID provided in the Provider ID above. For example, 1 = NPI 6 = Internal Plan ID 8 = DEA Number (For Pharmacy claims ONLY) 9 = NABP Number (For Pharmacy claims ONLY)	1	C
4	License Number	State license number.	9	C
5	Medicaid Number	State Medicaid number (MassHealth/MMIS Provider ID).	10	C
6	Provider Last Name	Last name of provider. In case of an organization or entity or hospital, name should be entered in this field only. Please avoid using abbreviations and enter names consistently. For example, enter "Massachusetts General Hospital" instead of "MGH". Length increased to 200 characters	200	C
7	Provider First Name	First name of the provider Please submit First Name consistently. In case of an organization or entity or hospital, name should be entered in "Provider Last Name" field above and **not** in this field. Length increased to 100 characters	100	C
8	Provider Office Address Street	Street address where services were rendered. This field has to be a street address. It cannot be a post office or lock box if the provider is the billing provider	45	C
9	Provider Office Address City	City where services were rendered.	20	C
10	Provider Office Address State	State where services were rendered.	2	C
11	Provider Office Address ZIP	Zip where services were rendered. ZIP+4	9	C

#	Field Name	Definition/Description	Length	Data Type
12	Provider Mailing Address Street	Street address where correspondence is received. This field has to be a street address. It cannot be a post office or lock box if the provider is the billing provider	45	C
13	Provider Mailing Address City	City where correspondence is received.	20	C
14	Provider Mailing Address State	State where correspondence is received.	2	C
15	Provider Mailing Address ZIP	Zip where correspondence is received. ZIP+4	9	C
16	Provider Type	Please use the values from Table G. **Note** that value "-4" for "Incomplete/No Information" option has been removed.	3	N
17	Filler		3	C
18	Provider Effective Date	Date provider becomes eligible to perform services.	8	D
19	Provider Term Date	Date provider is no longer eligible to perform services.	8	D
20	Provider Non-par Indicator	Non-participating provider indicator. 2 non-participating provider 3 participating provider	1	C
21	Provider Network ID	The network the provider is affiliated to by the Health Plan (internal plan ID).	15	C
22	PCC Provider ID	Required for PCCs enrolled with the MCE.	15	C
23	Panel Open Indicator	Is the provider accepting new patients? 1 Accepting new patients 2 Not accepting new patients	1	C
24	Provider DEA Number	Provider DEA Number	11	C
25	Provider Type Description	Description of the provider type	50	C
26	National Provider Identifier (NPI)	National Provider Identifier issued by the National Plan and Provider Enumeration System (NPPES). It is required on all claims.	10	C
27	Medicare ID Number		15	C
28	Social Security Number	Provider's SSN is 9 digits field and should be entered with no dashes (e.g.04-3333333 should be entered as 043333333 and 099-99-9999 should be entered as 099999999). Values less that 9-character long are invalid.	9	C
29	NABP Number	National Association of Boards of Pharmacy number	9	C
30	Tax ID Number	Tax ID Number is primarily the Federal Employee Identification Number (FEIN); however, when Providers don't have Tax ID Number for the reasons like being sole proprietors or small business owners without employees, provider's SSN should be entered in both fields, # 28 and #30, in same 9 digits format with no dashes (e.g.04-3333333 should be entered as 043333333 and 099-99-9999 should be entered as 099999999). Values less that 9-character long are invalid.	9	C
31	PCC Provider ID Type	Required for PCCs enrolled with the MCE.	1	C

#	Field Name	Definition/Description	Length	Data Type
32	Gender Code	”M” for Male, “F” for Female, and “O” for Other	1	C
33	Primary Care Eligibility Indicator	Provider is eligible to receive enhanced Medicare rate for their primary care services. This indicator should follow the CMS and MassHealth regulations on provider eligibility for Affordable Care Act – Section 1202. 0=Yes, Eligible based on 60% Attestation 1=Yes, Eligible based on Board Certification 2=No, Not Eligible 3=Unknown 4=Not Applicable **Note:** The values ‘0’ and ‘1’ indicating provider eligibility for the “ACA Section 1202” Rate Increase should be only applicable when providers have active contracts with MCEs. If a provider contract gets terminated then the provider would no longer be eligible for the rate increase, and the value for this flag would be ‘2’ (Not Eligible). The assumption is that eligible providers are either eligible based on Board Certification or 60% attestation. In the case where the MCE receives a 60% attestation from a provider that has already been determined to be eligible based on Board Certification then MCE should use value “1”.	1	C
34	APCD ORG ID	This is a new field added to get the APCD Provider Organization ID (OrgID) for the provider. Length is 6 characters. It should be submitted for all providers whose Org ID had been submitted to APCD.	6	C
35	Entity PIDSL	MCO/ACO providers - if the provider is enrolled with MCO only (not with ACO) - MCO PIDSL - if the provider is enrolled with ACO only - ACO PIDSL - if the provider is enrolled with both, ACO and MCO, then ACO PIDSL - if provider is enrolled with multiple ACOs (e.g. a specialist), and a plan is an active MCO - MCO PIDSL - if provider is enrolled with multiple ACOs (e.g. a specialist) and a plan is not an active MCO - old MCO PIDSL SCO PIDSL for SCO providers One Care PIDSL for One Care providers Example: 999999999A	10	C
36	Provider ID Address Location Code	Code to identify address location of Provider ID in Field # 2.	15	C
37	PCC Provider ID Address Location Code	Code to identify address location of PCC Provider ID in Field # 22.	15	C
38	Provider Network ID Type	Type of Provider Network ID in Field # 21.	1	N
39	Provider Network ID Address Location Code	Code to identify address location of Provider Network ID in Field # 21.	15	C
40	Provider Bundle ID	ID to tie together all the IDs for a particular provider	15	C
41	Provider ID Primary Address	Y/N value to indicate primary address location	1	C

#	Field Name	Definition/Description	Length	Data Type
	Location Indicator			

Example of Provider Bundle ID

This example shows the case when Provider ID is different for every location.
In most cases Provider ID is unique per each provider within the organization and will be the same on every line

Org. Code	Provider ID	Provider ID Type	Address Location Code	Provider Bundle ID	Provider ID Primary Address Location Indicator	Provider Last Name	Provider First Name
888	1234569	6	A	65656	N	Smith	John
888	1234568	6	B	65656	N	Smith	John
888	1234567	6	C	65656	Y	Smith	John
888	1234566	6	D	65656	N	Smith	John

Provider Error Process:

1. Provider records with null ID and/or null ID Type do not get loaded into MH DW. Such records get rejected and returned in the provider error response file.

2. If duplicate records per provider ID, Provider ID Type, Provider Address Location, and Provider Term Date are ***erroneously*** submitted, one record will be accepted based on "best fit" logic and all other records will be rejected and returned in the provider error file.

3. "Best" fit logic picks one record per provider ID, provider ID Type and provider Term Date in a provider file, based on the record that has the most populated information (NPI, provider name, address, tax ID, license number, and Medicaid Number, respectively).

4. Records sent with "null" or missing effective/term dates, will also be returned to the MCEs in the provider error response file. The MCE is expected to correct and resubmit these records in the Correction file data submissions.

5. A Correction file for provider records rejected for any of the reasons above should be submitted with a zipped Correction file for the ***same*** submission.

3.2 MCE Internal Provider Type Data Set Elements with Record Layout

Data Elements

This section contains field names and definitions for the provider type record that is based on the Provider Types that are **internally** used by the MCE. This is different from MassHealth Provider Types submitted in the Provider Data Set defined above***. This table should only have providers who have an internal provider type code. In other words, this table should not have providers with missing internal provider type code.***

#	Field Name	Definition/Description	Length	Data Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization. **This code identifies your Organization :** 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	3	N
2	Provider ID	Provider ID.	15	C
3	Provider ID Type	A code identifying the type of ID provided in Provider ID above: One code identifying the type of ID provided in the Provider ID above. For example, 6 = Internal ID (Plan Specific)) 8 = DEA Number 9 = NABP Number 1 = NPI	1	N
4	Internal Provider Type Code	Provider Type code as defined internally by the MCE	6	C
5	Internal Provider Type Description	Description of Provider Type code as defined internally by the MCE	120	C
6	Provider ID Address Location Code	Code to identify address location of Provider ID in Field # 2	15	C

3.3 Provider Specialty Data Set Elements

Data Elements

This section contains field names and definitions for the provider specialty record. If a provider has multiple specialties, please provide one record for each specialty per provider.

#	Field Name	Definition/Description	Length	Data Type
1	Org.Code	Unique ID assigned by MH DW to each submitting organization. **This code identifies your Organization :** 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	3	N
2	Provider ID	Provider ID, Federal Tax ID, UPIN or Health Plan ID.	15	C
3	Provider Specialty	Please use the values contained in Table H. If there are provider specialties not contained in table H, assign them a new three digit number. List the description of the new values in the Provider Specialty Description field.	3	C
4	Provider Specialty Date	Date provider becomes eligible to perform specialty services.	8	D
5	Provider ID Type	A code identifying the type of ID provided in Provider ID above: One code identifying the type of ID provided in the Provider ID above. For example: 6 = Internal ID (Plan Specific)) 8 = DEA Number 9 = NABP Number 1 = NPI	1	C
6	Provider Specialty Description	Description of the Provider Specialty	50	C
7	Provider ID Address Location Code	Code to identify address location of Provider ID in Field # 2.	15	C

3.4 Additional Reference Data Set Elements

These files currently apply only to the BH Vendor.

Authorization Type Data Set Elements

#	Field Name	Description	Length	Data Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization.	3	N
2	ATHTYP	Two digit code identifying the type of service.	6	C
3	ATHTYP DESCRIPTION	Description for the ATHYTYP codes.	100	C

Claim Type Data Set Elements

#	Field Name	Description	Length	Data Type
1	Org. Code	Unique ID assigned in MassHealth DW to each submitting organization	3	N
2	CLATYP	Code identifying a service.	6	C
3	CLATYP DESCRIPTION	Description for the CLATYP codes.	100	C

Group Number Data Set Elements

#	Field Name	Description	Length	Data Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization.	3	N
2	Member Rating Category	Description for the Member Rating Category.	50	C
3	DMA/DMH Indicator	Description for the DMA/DMH Indicator.	50	C
4	Eligibility Group Name	Description for the Eligibility Group Name.	100	C
5	Eligibility Group Number	Six digit number identifying the Eligibility Group.	10	N
6	MMIS Plan Type	Two digit code identifying the MMIS Eligibility Plan Type.	2	C

Service Class Data Set Elements

#	Field Name	Description	Length	Data Type
1	Org. Code	Unique ID assigned in MassHealth DW to each submitting organization	3	N
2	Service Class	Code identifying a service class.	10	C
3	Description	Description of service class codes	100	C

Services Data Set Elements

#	Field Name	Description	Length	Data Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization.	3	N
2	SVCLVLE	Description of Service Level I.	60	C
3	SVCLVLMHSA	Description of Service Level II.	90	C
4	SVCGRP	Description of Service Level III.	100	C
5	SVCDESC	Description of Service Level IV.	120	C
6	UNITTYP	Description of Unit Type.	4	C
7	UNITCONVE	Unit Conversion Value. This must be a positive number greater than zero.	12	N
8	ATHTYP	Authorization Type Code.	1	C
9	SVCCOD_REFSERVICES	Service Code.	6	C
10	CLATYP_REFSERVICES	Claim Type Code.	2	C
11	MOD1_REFSERVICES	Modifier Code.	2	C
12	ID_SERVICES	ID Services Value.	10	N
13	CBHI_FLAG	An indicator to distinguish CBHI Services	10	C
14	SERVICE_24_HOUR	Specifies if it was 24-Hour or Non-24-Hour Service (or other descriptions such as P4P)	11	C
15	INTERMEDIATE_SVCLVLE	Specifies what kind of Intermediate Service Level was provided	50	C
16	SVCLVLI	Specifies service level provided	60	C
17	MHSAEM	Service provided: whether it was EM, or MH, or NA, or SA	2	C
18	SVCDIRECTORY	Service Directory	82	C

4.0 Encounter Record Layout Amendment Process and Layout

1. Amendment processing has been created to allow MCEs to make retroactive changes to the existing claims. "Existing" are the claims that have been accepted and loaded in MH DW.

2. MH DW expects that amendments are used to reflect retroactive dimension changes, such as Member ID, Servicing Category, etc.

3. There are no constraints on timing for submissions of the amendments.

4. Amendments can be sent as a part of a regular submission or as one-off submission. The one-off submission should contain claims file in the format outlined in segment 3.0 "Encounter Data Set Elements" and a metadata file in the format outlined in segment 6.0 "Media Requirements" of this document.

5. Amendments should be submitted with the Type of Feed 'ENC'

6. In submission amendment record is identified by Record Type 'A'. When inserted in MH DW, it inherits the record type of the record it is amending.

7. If the Claim Number + Claim Suffix combination of the 'A' record is not found in MH DW, the record will be rejected with error code 11"Active Original Claim No-Claim Suffix Not Found"

8. If the claim that has to be amended already has Former Claim Number information on a line, that Former Claim Number information should be repeated precisely on the amendment claim

9. All columns should be populated according to the standards like any other submitted claim and should contain post-change values

10. All provider data on the claim must point to a provider reference data.

11. A claim submitted prior to the introduction of Commonwealth Care must have valid data in the Group Number field.

12. Multiple amendments to the same record in the same feed are not allowed and will be rejected with error code "10 - Duplicate Claim No-Claim Suffix -- in same feed".

13. The amendment file loads with the same iterative error process as the regular submission.

14. Dollar amount changes on the claims that happen in the source system, like adjustments and voids, should be handled via existing process set up to handle those kinds of transactions.

5.0 Error Handling

MassHealth will validate the feeds received from the MCEs and the BH Vendor and return files containing erroneous records back to the MCEs and the BH Vendor for correction and resubmission. The error rate in the initial submission should be no more than 3% for the data to be considered complete and accurate. The format of the error files will be the same as the input record layout described above with 2 fields appended as the last 2 fields on the record layout. These will be the erroneous field number and the error code for that field. Section 8.0 Quantity & Quality Edits lays out the expectation for each field in the record format for the feed. In addition to these edits, MassHealth will also subject the records to some intra-record validation tests. These may include validation checks like "net amount <= gross amount", "non-unique claim number + claim suffix combination", etc. Error checking is likely to evolve with time therefore a complete list of all pseudo-columns and error codes will accompany the rejected records returned to the MCEs and BH Vendor. A list is published below.

Error Codes

Error Code	Description
1	Incorrect Data Type
2	Invalid Format
3	Missing value
4	Code missing from reference data
5	Invalid Date
6	Admissions Date is greater than Discharge Date
7	Discharge Date is less than Admissions Date
8	Paid Date is less than Admission or Discharge or Service Dates
9	Date is prior to Birth Date
10	Duplicate Claim No-Claim Suffix -- in same feed
11	Active Original Claim No-Claim Suffix Not Found
12	Bad Zip Code
13	Replacement received for a voided record
14	Date is in the future
15	From Service Date is greater than To Service Date
16	To Service Date is less than From Service Date
17	Cannot be Negative
18	Non HIPAA/Standard code.
19	Bad Metadata File.
20	Local Code Not present in MassHealth DW.
21	Cannot be Zero.
22	Former Claim No-Claim Suffix fields should not contain data for Original Claim
23	Only Original claims allowed in the Initial feed
24	Duplicate Claim No-Claim Suffix -- from prior submission
25	Filler
26	Original Claim No-Claim Suffix, Former Claim No-Claim Suffix -- in same feed
27	Metadata - No metadata file found or file is empty.
28	Metadata - MCE_Id incorrect for the plan.
29	Metadata - MCE_ID not found in metadata file.
30	Metadata - Date_Created not found in metadata file.
31	Metadata - Date_Created is not a valid date.
32	Metadata - Data_File_Name not found in metadata file.
33	Metadata - Data_File_Name does not exist or is not a regular file.
34	Metadata - Pro_file_Name not found in metadata file.

Error Code	Description
35	Metadata - Pro_file_Name does not exist or is not a regular file.
36	Metadata - Pro_Spec_Name not found in metadata file.
37	Metadata - Pro_Spec_Name does not exist or is not a regular file.
38	Metadata - Total_Records not found in metadata file.
39	Metadata - Total_Records does not match actual record count.
40	Metadata - Total_Net_Payments not found in metadata file.
41	Metadata - Total_Net_Payments does not match actual sum of dollar amount.
42	Metadata - Time_Period_From not found in metadata file.
43	Metadata - Time_Period_From is not a valid date.
44	Metadata - Time_Period_To not found in metadata file.
45	Metadata - Time_Period_To is not a valid date.
46	Metadata - Return_To not found in metadata file.
47	Metadata - Type_Of_Feed not found in metadata file.
48	Metadata - Type_Of_Feed contains invalid value. Refer to the spec for valid values.
49	Metadata - Metadata - Ref_Services_File_Name not found in metadata file.
50	Metadata - Ref_Services_File_Name does not exist or is not a regular file.
51	Metadata - ATHTYP_File_Name not found in metadata file.
52	Metadata - ATHTYP_File_Name does not exist or is not a regular file.
53	Metadata - GRPNUM_File_Name not found in metadata file.
54	Metadata - GRPNUM_File_Name does not exist or is not a regular file.
55	Metadata - SVCCLS_File_Name not found in metadata file.
56	Metadata - SVCCLS_File_Name does not exist or is not a regular file.
57	Metadata - CLATYP_File_Name not found in metadata file.
58	Metadata - CLATYP_File_Name does not exist or is not a regular file.
59	RefService not found.
60	If former claim number filled in, so must former_claim_suffix.
70	ICD Version Qualifier ICD9 used on a claim post ICD10 implementation (To Service Date >=10/01/2015)
71	ICD Version Qualifier ICD9 used on a claim post ICD10 implementation (Discharge Date>=10/01/2015)
72*	(Denial Code not in Denied_Claims file) Claim Number/Suffix in Denied_Claims_Reason_Code file not in Denied_Claims file
*73**	*Claim Number/Suffix in Denied_Claims file not in Denied_Claims_Reason_Code file*
74	Correction to a claim that is not in MH DW
61	*Missing Provider NPI – Not used at present*
62	Metadata - Pro_MCEType_Name not found in metadata file.
63	Metadata - Pro_MCEType_Name does not exist or is not a regular file.

*Applies to the Denied Claims submissions only

All the MCEs including the BH Vendor should resubmit corrected records within a week of receiving the error files from MassHealth. This process will be repeated until the number of validation errors falls below a MassHealth defined threshold. Refer to the "**Encounter Data" section** of the **MassHealth Contract** for more details on the action required when data submission is not in compliance with Encounter Data requirements.

6.0 Media Requirements

Format

File Type:	**PKZIP/WINZIP compressed plain text file**
Character Set:	ASCII

All submitted files should be ***pipe-delimited.*** Please compress the data file using PKZIP/WINZIP or compatible program. All records in the data file should follow the record layout specified in section 4.0 where the length represents the maximum length of each field. Padding fields with 0s or spaces is ***not*** required.

Each record should end with the standard MS Windows text file end-of-line marker ("\r\n" - a carriage control followed by a new line).

Filename

The Zip file name should conform to the following naming convention
MCE_Claims_YYYYMMDD.zip

Example:

"BMC_Claims_20010701.zip", where
YYYYMMDD -the date of file creation (4 digit year, 2 digit month, 2 digit day) and
MCE identifies the Plan according to the following:

MCOs:
BMC - Boston Medical Center HealthNet Plan
CHA - Cambridge Network Health
FLN- Fallon Community Health Plan
MBH - Massachusetts Behavioral Health Partnership
NHP - Neighborhood Health Plan
HNE - Health New England
CAR - CeltiCare

SCOs:
CCA - Commonwealth Care Alliance
UHC – United HealthCare
NAV - Navicare
SWH - Senior Whole Health
TFT – Tufts Health Plan
BHP – BMC HealthNet Plan

One Care (ICO):
CCI - Commonwealth Care Alliance
NWI – Cambridge Network Health
FTC – Fallon Total Care

Project Related Filename

1. Names of the files submitted for the special projects should have an extension up to 6 characters after the date part of the name. For example, the files submitted for the J-Code project might have an extension "JCODE" in the name of the file.

Example:

"MCE_Claims_YYYYMMDD_JCODE.zip"

2. MH DW will give the MCEs specific instructions on the file naming standards related to specific projects

The Manual Override File
The manual override file should be named MCE_Claims_YYYYMMDD_**MO**. The "_MO" files should be sent only after the error file has been returned to the MCEs, and the MCEs have re-submitted a corrected file. The manual override file should have a file type of EMO in the metadata file.

The Zip File should contain:
The Encounter Data file
The Provider data file
The Provider specialty file
The MCE Internal Provider Type file
The Manual Override file (if applicable)
The Service Reference file (BH Vendor Only)
The Service Class Codes file (BH Vendor Only)
The Authorization Type Codes file (BH Vendor Only)
The Claim Type Codes file (BH Vendor Only)
The Group Number Codes file (BH Vendor Only)
Additional Documentation File or Metadata file

Metadata file
Please submit an additional file called **metadata.txt** which contains the following Key Value Pairs. A regular submission or error submission file should have a file type of ENC. The manual override file should have a file type of EMO in the metadata file.

	ENC/EMO
MCE_Id="Value" (MCO: FLN, NHP, BMC, CHA, MBH, HNE, CAR) (SCO: CCA, UHC, NAV, SWH, TFT, BHP) (One Care-ICO: CCI, NWI, FTC)	Mandatory
Date_Created=" YYYYMMDD"	Mandatory
Data_File_Name="Value"	Mandatory
Pro_File_Name="Value"	Mandatory
Pro_Spec_Name="Value"	Mandatory
Pro_MCEType_Name="Value"	Mandatory
Total_Records="Value"	Mandatory
Total_Net_Payments="Value"	Mandatory
Time_Period_From="Value" (YYYYMMDD)	Mandatory
Time_Period_To="Value" (YYYYMMDD)	Mandatory
Return_To="email address"	Mandatory
Type_Of_Feed="Value" (ENC/EMO)	Mandatory
Ref_Services_File_Name ="Value"	Optional
SVCCLS_File_Name ="Value"	Optional
ATHTYP_File_Name ="Value"	Optional
CLATYP_File_Name ="Value"	Optional
GRPNUM_File_Name ="Value"	Optional

a) Names of the files in the metadata file must match the names of the actual files in submission
b) Send a zero byte None.txt for missing files - provider or specialty and set corresponding field value to "None.txt"
c) A file posted on SFTP server must have a unique name
d) Discrepancy between the actual feed and the values in Metadata file fields Total_Net_Payments and/or Total_Records results in rejection of the entire feed.
e) The names of the fields in Metadata file should match the spelling suggested in the spec (Example: Total_Net_Payments)
f) From a processing perspective there is no difference between the original submission file, a correction file, and an Amendment file. All these types of submissions should have Type_ Of_ Feed = ”ENC” in metadata file

Monthly Financial Report - CURRENTLY DECOMISSIONED!

some additional updates might be introduced later

This is a stand-alone text file submitted monthly separate from encounter data submission; however, it must be always submitted ***after*** the manual override file. Please follow instructions in Section 1.1 "Data Requirements".

Monthly Financial Report is submitted as a pipe-delimited text file based on the following specifications:

1. File name should conform to the following naming convention:
   MCE_FinReport_YYYYMMDD.txt where the date reflects the date of a file submission.

   Example:
   A report submitted by Boston Medical Center HealthNet Plan in May of 2015 for the month of March of 2015 would be named: **BMC_FinReport_20150531.txt**

2. Along with the report file, a confirmation file named **"mce_fin_done.txt"** should be submitted. This file should contain one field only indicating the name of the financial report submitted.

   Example:
   mce_fin_done.txt submitted along with **BMC_FinReport_20150531.txt** file will have the following content:
   "MCE_FINREP_FILE="BMC_FinReport_20150531.txt"

   First report record is a mandatory header record with the following details:
   MCE_ID|Reporting_YearMonth|Date_Created|Total_Records|Return_To

   Example:

   BMC|201503|20150531|25|abc.xyz@bmchp.org

3. Definition of header record by data element:

#	Field Name	Definition
1	MCE_ID	One of the following values: MCO: FLN,NHP,BMC,CHA,MBH,HNE,CAR; SCO: CCA, UHC, NAV, SWH, TFT, BHP; One Care-ICO: CCI, NWI, FTC.
2	Reporting_YearMonth	Must be the year and the month of the reporting month in "YYYYMM" format. (Same as "YearMonth" in the report).
3	Date_Created	Must be the date of submission with format "YYYYMMDD"
4	Total_Records	Number of records in the report excluding the header record.
5	Return_To	Must have the email address of the MCE contact person(s).

4. Data records should follow the header record with the layout described below:

#	Field Name	Definition	Length	Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization.	3	Number
2	Service Category	Service Category as defined in Tables I-A, I-B, I-C	3	Text
3	Description	Description of Service Category	120	Text
4	Total_Number_Of_Claim_Lines	Total number of claim lines per Service Category	10	Number
5	Total Net Payment	Total expenses per Service Category	15	*Number/No Decimal Point
6	YearMonth	The Year and Month of the report based on the dates of service on the claims. There is only one value per monthly report. See example below for August 2014 report.	6	Text

*MassHealth prefers to receive dollars and cents with an **implied decimal point** before the last two digits in the data. Actual decimal point must not be included in dollar amounts.

For example, a data string "1234567" would represent $12,345.67.

Report Example:

BMC|201503|20150531|25|abc.xyz@bmchp.org
997|5|Behavioral Health - Emergency Services|148|12365400|201408
997|9|Facility - Medical/Surgical|321|987456|201408
997|13|Laboratory|654|321456|201408
……

Note: No Pipes are allowed in the values of any above mentioned elements

Secure FTP Server

MassHealth has set up a Secure FTP server for exchanging data with the MCEs. Details of the server are below:

Sever: virtualgateway**dw**.ehs.state.ma.us ID currently set up for MCOs: fln, nhp, bmc, cha, BH Vendor, gu02 (CAR), gu04 (HNE).
ID currently set up for SCOs: swh, uhc, nav, cca, tft, bhp.
ID currently set up for One Care (ICOs): cci, nwi, ftc.
Home directory :/<mce>: example /nhp.

- Each home directory currently contains following sub directories *ehs_dw* : production folder for exchanging encounter data and error reports.
- *test_masshealth*: used by MassHealth for testing purpose.
- *test_mco*: available for mce to send any test files or adhoc data to MassHealth.

Sending Encounter data

Transfer encounter data file in a format and content as described in sections above to the production folder on the server. After the data transfer is complete, include a zero byte file called *mce_done.txt.*

- Please refrain from sending several files with the same name.
- Please make sure to post only one encounter or member file at the same time.
- If a second file is a project specific, please work with MH DW to follow the instructions on file submission related to the project

Receiving Error reports

After the data has been processed, an error zip file (beginning with err) will be posted to the production folder. A notification email will be sent to the email address provided in the Metadata feed. Please note that the error file will be available on the server for a period of 30 days. MassHealth may need to revise the retention period in the future, based on available disk space on the server. If you post a file and do not receive email message about the error file back in 7 business days, please contact MassHealth.

CMS Internet Security Policy

DATE OF ISSUANCE: November 24, 1998

SUBJECT:
Internet Communications Security and Appropriate Use Policy and Guidelines for CMS Privacy Act-protected and other Sensitive CMS Information.

1. Purpose.

This bulletin formalizes the policy and guidelines for the security and appropriate use of the Internet to transmit CMS Privacy Act-protected and other sensitive CMS information.

2. Effective Date.

This bulletin is effective as of the date of issuance.

3. Expiration Date.

This bulletin remains in effect until superseded or canceled.

4. Introduction.

The Internet is the fastest growing telecommunications medium in our history. This growth and the easy access it affords has significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among health care providers, CMS contractors, CMS components, State agencies acting as CMS agents, Medicare and Medicaid beneficiaries, and researchers.
However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The very nature of the Internet communication mechanisms means that security risks cannot be totally eliminated. Up to now, because of these security risks and the need to research security requirements vis-a-vis the Internet, CMS has prohibited the use of the Internet for the transmission of all CMS Privacy Act-protected and other sensitive CMS information by its components and Medicare/Medicaid partners, as well as other entities authorized to use this data.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually-identifiable data. Section 5 U.S.C. 552a (e) (10) of the Act is very clear; federal systems must: "...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." One of CMS's primary responsibilities is to assure the security of the Privacy Act-protected and other sensitive information it collects, produces, and disseminates in the course of conducting its operations. CMS views this responsibility as a covenant with its beneficiaries, personnel, and health care providers. This responsibility is also assumed by CMS's contractors, State agencies acting as CMS agents, other government organizations, as well as any entity that has been authorized access to CMS information resources as a party to a Data Release Agreement with CMS.

However, CMS is also aware that there is a growing demand for use of the Internet for inexpensive transmission of Privacy Act-protected and other sensitive information. CMS has a responsibility to accommodate this desire

as long as it can be assured that proper steps are being taken to maintain an acceptable level of security for the information involved.

This issuance is intended to establish the basic security requirements that must be addressed for use of the Internet to transmit CMS Privacy Act-protected and/or other sensitive CMS information.

The term "CMS Privacy Act-protected Data and other sensitive CMS information" is used throughout this document. This phrase refers to data which, if disclosed, could result in harm to the agency or individual persons. Examples include:

> All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act; i.e., for which unauthorized disclosure would constitute a "clearly unwarranted invasion of personal privacy" likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.
>
> Payment information that is used to authorize or make cash payments to individuals or organizations. These data are usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter. As modification of such records could cause an improper payment, these records must be adequately protected.
>
> Proprietary information that has value in and of itself and which must be protected from unauthorized disclosure.
>
> Computerized correspondence and documents that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.

5. Policy

This Guide establishes the fundamental rules and systems security requirements for the use of the Internet to transmit CMS Privacy Act-protected and other sensitive CMS information collected, maintained, and disseminated by CMS, its contractors, and agents.

It is permissible to use the Internet for transmission of CMS Privacy Act-protected and/or other sensitive CMS information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information. Detailed guidance is provided below in item 7.

6. Scope.

This policy covers all systems or processes which use the Internet, or interface with the Internet, to transmit CMS Privacy Act-protected and/or other sensitive CMS information, including Virtual Private Network (VPN) and tunneling implementations over the Internet. Non-Internet Medicare/Medicaid data communications processes (e.g., use of private or value added networks) are not changed or affected by the Internet Policy.

This policy covers Internet data transmission only. It does not cover local data-at-rest or local host or network protections. Sensitive data-at-rest must still be protected by all necessary measures, in conformity with the guidelines/rules which govern the entity's possession of the data. Entities must use due diligence in exercising this responsibility.

Local site networks must also be protected against attack and penetration from the Internet with the use of firewalls and other protections. Such protective measures are outside the scope of this document, but are essential to providing adequate local security for data and the local networks and ADP systems which support it.

7. Acceptable Methods

CMS Privacy Act-protected and/or other sensitive CMS information sent over the Internet must be accessed only by authorized parties. Technologies that allow users to prove they are who they say they are (authentication or identification) and the organized scrambling of data (encryption) to avoid inappropriate disclosure or modification must be used to insure that data travels safely over the Internet and is only disclosed to authorized parties. Encryption must be at a sufficient level of security to protect against the cipher being readily broken and the data compromised. The length of the key and the quality of the encryption framework and algorithm must be increased over time as new weaknesses are discovered and processing power increases.

User authentication or identification must be coupled with the encryption and data transmission processes to be certain that confidential data is delivered only to authorized parties. There are a number of effective means for authentication or identification which are sufficiently trustworthy to be used, including both in-band authentication and out-of-band identification methods. Passwords may be sent over the Internet only when encrypted.

(footnote)1 We note that the Health Insurance Portability and Accountability Act of 1966 (HIPAA) calls for stringent security protection for electronic health information both while maintained and while in transmission. The proposed Security Standard called for by HIPAA was published in the Federal Register on August 12, 1998. The public had until October 13, 1998, to comment on the proposed regulation. Based on public comments, a final regulation is planned for late 1999. Policy guidance contained in this bulletin is consistent with the proposed HIPAA security requirements.

ENCRYPTION MODELS AND APPROACHES

Figure 1 depicts three generalized configurations of connectivity to the Internet. The generic model is not intended to be a literal mirror of the actual Internet interface configuration, but is intended to show that the encryption process takes place prior to information being presented to the Internet for transmission, and the decryption process after reception from the Internet. A large organization would be very likely to have the Internet Server/Gateway on their premises while a small organization would likely have only the Internet Client, e.g., a browser, on premises with the Internet Server at an Internet Service Provider (ISP). The Small User and Large User examples offer a more detailed depiction of the functional relationships involved.

The Encryption/Decryption process depicted graphically represents a number of different approaches. This process could involve encryption of files prior to transmittal, or it could be implemented through hardware or software functionality. The diagram does not intend to dictate how the process is to be accomplished, only that it must take place prior to introduction to the
Internet. The "Boundary" on the diagrams represents the point at which security control passes from the local user. It lies on the user side of the Internet Server and may be at a local site or at an Internet Service Provider depending upon the configuration.

FIGURE 1: INTERNET COMMUNICATIONS EXAMPLES in PDF.

Acceptable Approaches to Internet Usage

The method(s) employed by all users of CMS Privacy Act-protected and/or other sensitive
CMS information must come under one of the approaches to encryption and at least one of the authentication or identification approaches. The use of multiple authentication or identification approaches is also permissible. These approaches are as generic as possible and as open to specific implementations as possible, to provide maximum user flexibility within the allowable limits of security and manageability.

Note the distinction that is made between the processes of "authentication" and "identification". In this Internet Policy, the terms "Authentication" and "Identification" are used in the following sense. They should not be interpreted as terms of art from any other source. Authentication refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet communications data channel itself, generally called an
"in-band process." Identification refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path such as the telephone or US mail.

The listed approaches provide encryption and authentication/identification techniques which are acceptable for use in safeguarding CMS Privacy Act-protected and/or other sensitive CMS information when it is transmitted over the Internet.

In summary, a complete Internet communications implementation must include adequate encryption, employment of authentication or identification of communications partners, and a management scheme to incorporate effective password/key management systems.

ACCEPTABLE ENCRYPTION APPROACHES

Note: As of November 1998, a level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems is recognized by CMS as minimally acceptable. CMS reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brute-force exhaustive search).

HARDWARE-BASED ENCRYPTION:

1. Hardware encryptors - While likely to be reserved for the largest traffic volumes to a very limited number of Internet sites, such symmetric password "private" key devices (such as link encryptors) are acceptable.

SOFTWARE-BASED ENCRYPTION:

2. Secure Sockets Layer (SSL) (Sometimes referred to as Transport Layer Security - TLS) implementations - At a minimum SSL level of Version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets Layer are acceptable.

3. S-MIME - Standard commercial implementations of encryption in the e-mail layer are acceptable.

4. In-stream - Encryption implementations in the transport layer, such as pre-agreed passwords, are acceptable.

5. Offline - Encryption/decryption of files at the user sites before entering the data communications process is acceptable. These encrypted files would then be attached to or enveloped (tunneled) within an unencrypted header and/or transmission.

ACCEPTABLE AUTHENTICATION APPROACHES

AUTHENTICATION (This function is accomplished over the Internet, and is referred to as an "in-band" process.)

1. Formal Certificate Authority-based use of digital certificates is acceptable.

2. Locally-managed digital certificates are acceptable, providing all parties to the communication are covered by the certificates.

3. Self-authentication, as in internal control of symmetric "private" keys, is acceptable.

4. Tokens or "smart cards" are acceptable for authentication. In-band tokens involve overall network control of the token database for all parties.

ACCEPTABLE IDENTIFICATION APPROACHES

IDENTIFICATION (The process of identification takes place outside of the Internet connection and is referred to as an "out-of-band" process.)

1. Telephonic identification of users and/or password exchange is acceptable.

2. Exchange of passwords and identities by U.S. Certified Mail is acceptable.

3. Exchange of passwords and identities by bonded messenger is acceptable.

4. Direct personal contact exchange of passwords and identities between users is acceptable.

5. Tokens or "smart cards" are acceptable for identification. Out-of-band tokens involve local control of the token databases with the local authenticated server vouching for specific local users.

8. REQUIREMENTS AND AUDITS

Each organization that uses the Internet to transmit CMS Privacy Act-protected and/or other sensitive CMS information will be expected to meet the stated requirements set forth in this document.

All organizations subject to OMB Circular A-130 are required to have a Security Plan. All such organizations must modify their Security Plan to detail the methodologies and protective measures if they decide to use the Internet for transmittal of CMS Privacy Act-protected and/or other sensitive CMS information, and to adequately test implemented measures.

CMS reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this policy. This includes the right to require that any organization utilizing the Internet for transmission of CMS Privacy Act-protected and/or other sensitive information submit documentation to demonstrate that they meet these requirements.

9. ACKNOWLEDGMENT OF INTENT

Organizations desiring to use the Internet for transmittal of CMS Privacy Act-protected and/or other sensitive CMS information must notify CMS of this intent. An e-mail address is provided below to be used for this acknowledgment. An acknowledgment must include the following information:
Name of Organization
Address of Organization
Type/Nature of Information being transmitted
Name of Contact (e.g., CIO or an accountable official)
Contact's telephone number and e-mail address
For submission of acknowledgment of intent, send an e-mail to: internetsecurity@CMS.gov. Internal CMS elements must proceed through the usual CMS system and project development process.

10. POINT OF CONTACT
For questions or comment, write to:

Office of Information Services, CMS
Security and Standards Group
Division of CMS Enterprise Standards -Internet
7500 Security Boulevard
Baltimore, MD 21244

Also, check out the Security Policy FAQs
Return to Information Clearinghouse Listing

Last Updated January 31, 2001

7.0 Standard Data Values

Contents

This section contains tables that identify the standard coding structures for several of the encounter data fields.

Use of Standard Data Values

The tables list all of the standard data values for the fields, with descriptions.

Standard data values are given for the following tables:

Table A	Admit Type (UB)
Table B	Admit Source (UB)
Table C	Place of Service (CMS 1500)
Table D	Place of Service (from UB Type of Bill)
Table E	Discharge Status (UB Patient Status)
Table G	Servicing Provider Type
Table H	Servicing Provider Specialty (CMS 1500)
Table I	Service Category I-A: MCO I-B: SCO I-C: One Care (ICO)
Table K	Bill Classifications – (UB Bill Classification, 3rd digit)
Table M	Present on Admission (UB)
Table O	UB-4 UNIT OF MEASURE

Note: The abbreviation **NEC** after a description stands for **Not Elsewhere Classified**.

TABLE A
Type of Admission (UB)

Value	Definition
1	Emergency
2	Urgent
3	Elective
4	Newborn
5	Trauma Center
6-8	Reserved for National Assignment
9	Information not available

TABLE B
Source of Admission (UB)

Value	Description
1	Physician Referral
2	Clinic/Outpatient Referral
3	HMO Referral
4	Transfer from Hospital
5	Transfer from SNF
6	Transfer from another Facility
7	Emergency Room
8	Court/Law Enforcement
9	Information not available
A	RESERVED FOR ASSIGNMENT BY THE NUBC (END 10/1/07)
B	TRANSFER FROM ANOTHER HOME HEALTH AGENCY
C	RESERVED FOR ASSIGNMENT BY THE NUBC (END 7/1/10)
D	TRANSFER FROM ONE UNIT TO ANOTHER - SAME HOSP
E	TRANSFER FROM AMBULATORY SURGICAL CENTER
F	TRANSFER FROM HOSPICE/ENROLLED IN HOSPICE PROGRAM

For Newborns

Value	Description
1	Normal Delivery
2	Premature Delivery
3	Sick Baby
4	Extramural Birth

TABLE C
Place of Service (HCFA 1500)

Place of Service Codes for Professional Claims

CMS Database (updated November 2016)

Value	Place of Service Name	Place of Service Description
01	Pharmacy**	A facility or location where drugs and other medically related items and services are sold, dispensed, or otherwise provided directly to patients (effective 10/1/05)
02	Telehealth	The location where health services and health related services are provided or received, through a telecommunication system. (Effective January 1, 2017)
03	School	A facility whose primary purpose is education.
04	Homeless Shelter	A facility or location whose primary purpose is to provide temporary housing to homeless individuals (e.g., emergency shelters, individual or family shelters).
05	Indian Health Service Free-standing Facility	A facility or location, owned and operated by the Indian Health Service, which provides diagnostic, therapeutic (surgical and non-surgical), and rehabilitation services to American Indians and Alaska Natives who do not require hospitalization.
06	Indian Health Service Provider-based Facility	A facility or location, owned and operated by the Indian Health Service, which provides diagnostic, therapeutic (surgical and non-surgical), and rehabilitation services rendered by, or under the supervision of, physicians to American Indians and Alaska Natives admitted as inpatients or outpatients.
07	Tribal 638 Free-standing Facility	A facility or location owned and operated by a federally recognized American Indian or Alaska Native tribe or tribal organization under a 638 agreement, which provides diagnostic, therapeutic (surgical and non-surgical), and rehabilitation services to tribal members who do not require hospitalization.
08	Tribal 638 Provider-based Facility	A facility or location owned and operated by a federally recognized American Indian or Alaska Native tribe or tribal organization under a 638 agreement, which provides diagnostic, therapeutic (surgical and non-surgical), and rehabilitation services to tribal members admitted as inpatients or outpatients.
09	Prison-Correctional Facility	A prison, jail, reformatory, work farm, detention center, or any other similar facility maintained by either Federal, State or local authorities for the purpose of confinement or rehabilitation of adult or juvenile criminal offenders. (effective 7/1/06)
10	Unassigned	N/A
11	Office	Location, other than a hospital, skilled nursing facility (SNF), military treatment facility, community health center, State or local public health clinic, or intermediate care facility (ICF), where the health professional routinely provides health examinations, diagnosis, and treatment of illness or injury on an ambulatory basis.
12	Home	Location, other than a hospital or other facility, where the patient receives care in a private residence.

Value	Place of Service Name	Place of Service Description
13	Assisted Living Facility	Congregate residential facility with self-contained living units providing assessment of each resident's needs and on-site support 24 hours a day, 7 days a week, with the capacity to deliver or arrange for services including some health care and other services. (effective 10/1/03)
14	Group Home*	A residence, with shared living areas, where clients receive supervision and other services such as social and/or behavioral services, custodial service, and minimal services (e.g., medication administration).
15	Mobile Unit	A facility/unit that moves from place-to-place equipped to provide preventive, screening, diagnostic, and/or treatment services.
16	Temporary Lodging	A short term accommodation such as a hotel, camp ground, hostel, cruise ship or resort where the patient receives care, and which is not identified by any other POS code.
17	Walk-in Retail Health Clinic	A walk-in health clinic, other than an office, urgent care facility, pharmacy or independent clinic and not described by any other Place of Service code, that is located within a retail operation and provides, on an ambulatory basis, preventive and primary care services. (This code is available for use immediately with a final effective date of May 1, 2010)
18	Place of Employment-Worksite	A location, not described by any other POS code, owned or operated by a public or private entity where the patient is employed, and where a health professional provides on-going or episodic occupational medical, therapeutic or rehabilitative services to the individual. (This code is available for use effective January 1, 2013, but no later than May 1, 2013)
19	Off Campus-Outpatient Hospital	A portion of an off-campus hospital provider based department which provides diagnostic, therapeutic (both surgical and nonsurgical), and rehabilitation services to sick or injured persons who do not require hospitalization or institutionalization. (Effective January 1, 2016)
20	Urgent Care Facility	Location, distinct from a hospital emergency room, an office, or a clinic, whose purpose is to diagnose and treat illness or injury for unscheduled, ambulatory patients seeking immediate medical attention.
21	Inpatient Hospital	A facility, other than psychiatric, which primarily provides diagnostic, therapeutic (both surgical and nonsurgical), and rehabilitation services by, or under, the supervision of physicians to patients admitted for a variety of medical conditions.
22	On Campus-Outpatient Hospital	A portion of a hospital's main campus which provides diagnostic, therapeutic (both surgical and nonsurgical), and rehabilitation services to sick or injured persons who do not require hospitalization or institutionalization. (Description change effective January 1, 2016)
23	Emergency Room – Hospital	A portion of a hospital where emergency diagnosis and treatment of illness or injury is provided.
24	Ambulatory Surgical Center	A freestanding facility, other than a physician's office, where surgical and diagnostic services are provided on an ambulatory basis.
25	Birthing Center	A facility, other than a hospital's maternity facilities or a physician's office, which provides a setting for labor, delivery, and immediate post-partum care as well as immediate care of new born infants.

Value	Place of Service Name	Place of Service Description
26	Military Treatment Facility	A medical facility operated by one or more of the Uniformed Services. Military Treatment Facility (MTF) also refers to certain former U.S. Public Health Service (USPHS) facilities now designated as Uniformed Service Treatment Facilities (USTF).
27-30	Unassigned	N/A
31	Skilled Nursing Facility	A facility which primarily provides inpatient skilled nursing care and related services to patients who require medical, nursing, or rehabilitative services but does not provide the level of care or treatment available in a hospital.
32	Nursing Facility	A facility which primarily provides to residents skilled nursing care and related services for the rehabilitation of injured, disabled, or sick persons, or, on a regular basis, health-related care services above the level of custodial care to other than individuals with intellectual disabilities.
33	Custodial Care Facility	A facility which provides room, board and other personal assistance services, generally on a long-term basis, and which does not include a medical component.
34	Hospice	A facility, other than a patient's home, in which palliative and supportive care for terminally ill patients and their families are provided.
35-40	Unassigned	N/A
41	Ambulance – Land	A land vehicle specifically designed, equipped and staffed for lifesaving and transporting the sick or injured.
42	Ambulance – Air or Water	An air or water vehicle specifically designed, equipped and staffed for lifesaving and transporting the sick or injured.
43-48	Unassigned	N/A
49	Independent Clinic	A location, not part of a hospital and not described by any other Place of Service code, that is organized and operated to provide preventive, diagnostic, therapeutic, rehabilitative, or palliative services to outpatients only. (effective 10/1/03)
50	Federally Qualified Health Center	A facility located in a medically underserved area that provides Medicare beneficiaries preventive primary medical care under the general direction of a physician.
51	Inpatient Psychiatric Facility	A facility that provides inpatient psychiatric services for the diagnosis and treatment of mental illness on a 24-hour basis, by or under the supervision of a physician.
52	Psychiatric Facility-Partial Hospitalization	A facility for the diagnosis and treatment of mental illness that provides a planned therapeutic program for patients who do not require full time hospitalization, but who need broader programs than are possible from outpatient visits to a hospital-based or hospital-affiliated facility.

Value	Place of Service Name	Place of Service Description
53	Community Mental Health Center	A facility that provides the following services: outpatient services, including specialized outpatient services for children, the elderly, individuals who are chronically ill, and residents of the CMHC's mental health services area who have been discharged from inpatient treatment at a mental health facility; 24 hour a day emergency care services; day treatment, other partial hospitalization services, or psychosocial rehabilitation services; screening for patients being considered for admission to State mental health facilities to determine the appropriateness of such admission; and consultation and education services.
54	Intermediate Care Facility/ Individuals with Intellectual Disabilities	A facility which primarily provides health-related care and services above the level of custodial care to individuals but does not provide the level of care or treatment available in a hospital or SNF.
55	Residential Substance Abuse Treatment Facility	A facility which provides treatment for substance (alcohol and drug) abuse to live-in residents who do not require acute medical care. Services include individual and group therapy and counseling, family counseling, laboratory tests, drugs and supplies, psychological testing, and room and board.
56	Psychiatric Residential Treatment Center	A facility or distinct part of a facility for psychiatric care which provides a total 24-hour therapeutically planned and professionally staffed group living and learning environment.
57	Non-residential Substance Abuse Treatment Facility	A location which provides treatment for substance (alcohol and drug) abuse on an ambulatory basis. Services include individual and group therapy and counseling, family counseling, laboratory tests, drugs and supplies, and psychological testing. (effective 10/1/03)
58-59	Unassigned	N/A
60	Mass Immunization Center	A location where providers administer pneumococcal pneumonia and influenza virus vaccinations and submit these services as electronic media claims, paper claims, or using the roster billing method. This generally takes place in a mass immunization setting, such as, a public health center, pharmacy, or mall but may include a physician office setting.
61	Comprehensive Inpatient Rehabilitation Facility	A facility that provides comprehensive rehabilitation services under the supervision of a physician to inpatients with physical disabilities. Services include physical therapy, occupational therapy, speech pathology, social or psychological services, and orthotics and prosthetics services.
62	Comprehensive Outpatient Rehabilitation Facility	A facility that provides comprehensive rehabilitation services under the supervision of a physician to outpatients with physical disabilities. Services include physical therapy, occupational therapy, and speech pathology services.
63-64	Unassigned	N/A
65	End-Stage Renal Disease Treatment Facility	A facility other than a hospital, which provides dialysis treatment, maintenance, and/or training to patients or caregivers on an ambulatory or home-care basis.
66-70	Unassigned	N/A
71	Public Health Clinic	A facility maintained by either State or local health departments that provide ambulatory primary medical care under the general direction of a physician. (effective 10/1/03)
72	Rural Health Clinic	A certified facility which is located in a rural medically underserved area that provides ambulatory primary medical care under the general direction of a physician.
73-80	Unassigned	N/A

Value	Place of Service Name	Place of Service Description
81	Independent Laboratory	A laboratory certified to perform diagnostic and/or clinical tests independent of an institution or a physician's office.
82-98	Unassigned	N/A
99	Other Place of Service	Other place of service not identified above.

TABLE D
Place of Service (from UB Bill Type – 1st & 2nd digits)

Type of Facility (1st digit)

Value	Description
1	Hospital
2	Skilled Nursing Facility (SNF)
3	Home Health Agency (HHA)
4	Christian Science (Hospital)
5	Christian Science (Extended Care)
6	Intermediate Care
7	Clinic (refer to *Clinics Only* for 2nd digit)
8	Substance Abuse or Specialty Facility
9	Halfway House

Bill Classifications – Facilities (2nd digit)

Value	Description
1	Inpatient (including Medicare Part A)
2	Inpatient (Medicare Part B only)
3	Outpatient
4	Other
5	Basic Care
6	Complementary Inpatient
7	Complementary Outpatient
8	Swing Beds
9	Halfway House

Bill Classifications – Clinics only (2nd digit)

Value	Description
1	Rural Health Clinic
2	Hospital-based or Freestanding End State Renal Dialysis Facility
3	Freestanding Clinic
4	Other Rehab Facility (ORF) or Community Mental Health Center
5	Comprehensive Outpatient Rehab Facility (CORF)
6-8	Reserved for national assignment
9	Other

Bill Classifications – Specialty Facility (2nd digit)

Value	Description
1	Hospice (non-hospital based)
2	Hospice (hospital based)
3	Ambulatory Surgery Center
4	Free Standing Birthing Center
5	Critical Access Hospital
6	Residential Facility
7-8	Reserved for national assignment
9	Other

TABLE E
Discharge Status (UB Patient Status)

Value	Description
01	Discharged alive to home / self-care (routine discharge)
02	Discharged/Transferred to short term general hospital
03	Discharged/Transferred to skilled nursing facility (SNF)
04	Discharged/Transferred to intermediate care facility (ICF)
05	Discharged/Transferred to other facility
06	Discharged/Transferred to home care
07	Left against medical advice
08	Discharged/Transferred to home under care of a home IV drug therapy provider
09	Admitted as an inpatient to this hospital
10 – 19	Discharged to be defined at State level if necessary
20	Expired (Did not recover – Christian Science Patient)
21 – 29	Expired to be defined at State level if necessary
30	Still a patient
31 – 39	Still a patient to be defined at State level if necessary
40	Expired at home (Hospice claims only)
41	Died in a medical facility (Hospice claims only)
42	Place of death unknown (Hospice claims only)
43 – 99	Reserved for National Assignment

TABLE G
Servicing Provider Type

Value	Description
00	Placeholder PCP
01	Acute Care Hospital-Inpatient
02	Acute Care Hospital-Outpatient
03	Chronic Hospital-Inpatient
04	Chronic Hospital-Outpatient
05	Ambulatory Surgery Centers
06	Trauma Center
10	Birthing Center
15	Treatment Center
20	Mental Health/Chemical Dep. (NEC)
21	Mental Health Facilities
22	Chemical Dependency Treatment Ctr.
23	Mental Health/Chem Dep Day Care
25	Rehabilitation Facilities
30	Long-Term Care (NEC)
31	Extended Care Facility
32	Geriatric Hospital
33	Convalescent Care Facility
34	Intermediate Care Facility
35	Residential Treatment Center
36	Cont. Care Retirement Community
37	Day/Night Care Center
38	Hospice
40	Facility (NEC)
41	Infirmary
42	Special Care Facility (NEC)
50	Physician
51	Medical Doctor MD
52	Osteopath DO
53	Allergy & Immunology
54	Anesthesiology
55	Colon & Rectal Surgery
56	Dermatology
57	Emergency Medicine
58	Family Practice
59	Geriatric Medicine
60	Internist (NEC)
61	Cardiovascular Diseases
62	Critical Care Medicine
63	Endocrinology/Metabolism
64	Gastroenterology
65	Hematology
66	Infectious Disease
67	Medical Oncology
68	Nephrology
69	Pulmonary Disease
70	Rheumatology
71	Neurological Surgery
72	Nuclear Medicine

Value	Description
73	Obstetrics/Gynecology
74	Ophthalmology
75	Orthopedic Surgery
76	Otolaryngology
77	Pathology
78	Pediatrician (NEC)
79	Pediatric Specialist
80	Physical Medicine and Rehabilitation
81	Plastic Surgery/Maxillofacial Surgery
82	Preventative Medicine
83	Psychiatry/Neurology
84	Radiology
85	Surgeon
86	Surgical Specialist
87	Thoracic Surgery
88	Urology
95	Dentist
96	Dental Specialist
99	Podiatry
100	Unknown Clinic
120	Chiropractor
125	Dental Health Specialists
130	Dietitian
135	Medical Technologists
140	Midwife
145	Nurse Practitioner
146	Nursing Services
150	Optometrist
155	Pharmacist
160	Physician's Assistant
165	Therapy (physical)
170	Therapists (supportive)
171	Psychologist
175	Therapists (alternative)
180	Acupuncturist
185	Spiritual Healers
190	Health Educator
200	Transportation
205	Health Resort
210	Hearing Labs
215	Home Health Organization
220	Imaging Center
225	Laboratory
230	Pharmacy
235	Supply Center
240	Vision Center
245	Public Health Agency
246	Rehab Hospital-Inpatient
247	Rehab Hospital-Outpatient
248	Psychiatric Hospital-Inpatient
249	Psychiatric Hospital-Outpatient

Value	Description
250	Community Health Center
301	General Hospital
302	Certified Clinical Nurse Specialist
303	Infusion Therapy
304	Palliative Care Medicine
305	Adult Day Health
306	Adult Foster Care / Group Adult Foster Care
307	Fiscal Intermediary Services (FIS)
308	Personal Care Management Agency
309	Independent Living Centers
310	Day Habilitation
311	Durable Medical Equipment
312	Oxygen And Respiratory Therapy Equip
313	Prosthetics
314	Orthotics
315	Renal Dialysis Clinics
316	Respite Care
317	Intensive Residential Treatment Program (IRTP)
318	Complex Care Management
319	Special Programs
320	Recovery Learning Community (RLCs)
321	Certified Peer Specialist
322	Emergency Services Program (ESP)
323	Community Health Worker
324	Hospital Licensed Health Center
325	Aging Services Access Point (ASAP)
326	Geriatric Mental Health
327	Child Mental Health
328	Deaf and Hard of Hearing Independent Living Services Programs
329	Home Modification Service Providers
330	Transitional Assistance (across settings) Providers
331	Medication Management Providers
332	Substance Abuse Treatment Center
333	Magnetic Resonance Centers
334	Psych Day Treatment
335	QMB (Qualified Medicare Beneficiaries) Only Provider
336	Group Practice Physicians
337	School-Based Clinic or Health Center
338	Billing Agent

TABLE H
Servicing Provider Specialty (from CMS 1500)

Value	Description
01	General Practice
02	General Surgery
03	Allergy / Immunology
04	Otolaryngology
05	Anesthesiology
06	Cardiology
07	Dermatology
08	Family Practice
10	Gastroenterology
11	Internal Medicine
12	Osteopathic Manipulative therapy
13	Neurology
14	Neurosurgery
15	Speech Language Pathologists
16	Obstetrics / Gynecology
17	Hospice and Palliative Care
18	Ophthalmology
19	Oral Surgery (Dentists Only)
20	Orthopedic Surgery
22	Pathology
23	Sports Medicine
24	Plastic & Reconstructive Surgery
25	Physical Medicine and Rehabilitation
26	Psychiatry
27	Geriatric Psychiatry
28	Colorectal Surgery
29	Pulmonary Disease
30	Diagnostic Radiology
31	Intensive Cardiac Rehabilitation
32	Anesthesiologist Assistant
33	Thoracic Surgery
34	Urology
35	Chiropractic
36	Nuclear Medicine
37	Pediatric Medicine
38	Geriatric Medicine
39	Nephrology
40	Hand Surgery
41	Optometrist
42	Certified Nurse Midwife
43	CRNA, Anesthesia Assistant
44	Infectious Diseases
45	Mammography Screening Center
46	Endocrinology
48	Podiatrist
49	Ambulatory Surgery Center
50	Nurse Practitioner
51	Med Supply Co w/Certified Orthotist
52	Med Supply Co w/Certified Prosthetist
53	Med Supply Co w/Certified Prosthetist/Orthotist
54	Med Supply Co not included in 51, 52 or 53
55	Individual Certified Orthotist

Value	Description
56	Individual Certified Prosthetist
57	Individual Certified Prosthetist/Orthotist
58	Individuals not included in 55, 56 or 57
59	Ambulance Service Supplier
60	Public Health or Welfare Agency (Federal, State & Local Govt)
61	Voluntary Health Agency (ex: Planned Parenthood)
62	Psychologist
63	Portable X-Ray Supplier
64	Audiologist
65	Physical Therapist
66	Rheumatology
67	Occupational Therapist
68	Clinical Psychologist
69	Clinical Laboratory
70	Multispecialty Clinic or Group Practice
71	Registered Dietician/Nutrition Professional
72	Pain Management
73	Mass Immunization Roster Biller
74	Radiation Therapy Centers
75	Slide Preparation Facilities
76	Peripheral Vascular Disease
77	Vascular Surgery
78	Cardiac Surgery
79	Addiction Medicine
80	Licensed Clinical Social Worker
81	Critical Care (Intensivists)
82	Hematology
83	Hematology/Oncology
84	Preventive Medicine
85	Maxillofacial Surgery
86	Neuropsychiatry
87	All Other Suppliers (i.e. Drug, & Department Stores)
88	Unknown Supplier/Provider Specialty
89	Certified Clinical Nurse Specialist
90	Medical Oncology
91	Surgical Oncology
92	Radiation Oncology
93	Emergency Medicine
94	Interventional Radiology
95	Independent Physiological Lab
96	Optician
97	Physician Assistant
98	Gynecologist/Oncologist
99	Unknown Physician Specialty
A0	Hospital
A1	SNF
A2	Intermediate Care Facility
A3	Nursing Facility, Other
A4	HHA
A5	Pharmacy
A6	Medical Supply Co w/Respiratory Therapist
A7	Department Store
A8	Grocery Store
A9	Dentist

Value	Description
B2	Pedorthic Personnel
B3	Medical Supply Company with Pedorthic Personnel
B4	Rehabilitation Agency
B5	Ocularist

TABLE I – A
Service Category (Using the 4B reporting groups)

Value	Description
1	Capitated Physician Services
2	Fee For Service Physician Services
3	Behavioral Health –Inpatient Services
4	Behavioral Health –Diversionary Services *
5	Behavioral Health –Emergency Services Program (ESP) Services
6	Behavioral Health –Mental Health Outpatient Services *
7	Behavioral Health –Substance Abuse Outpatient Services *
8	Behavioral Health –Other Outpatient Services *
9	Facility- Medical/Surgical
10	Facility- Pediatric/Sick Newborns
11	Facility- Obstetrics
12	Facility- Skilled Nursing Facility/Rehab
13	Facility- Other Inpatient
14	Facility- Emergency Room
15	Facility –Ambulatory Care
16	Prescription Drug
17	Laboratory
18	Radiology
19	Home Health
20	Durable Medical Equipment
21	Emergency Transportation
22	Therapies
23	Other (Please use this for Vision and Dental claims)
24	Other Alternative Care
25	Mental Health and Substance Abuse Outpatient Services(BH Vendor Only)*
26	Outpatient Day Services (BH Vendor Only) *
27	Non-ESP Emergency Services (BH Vendor Only) *
28	Behavioral Health –Diversionary Services – 24-Hour
29	Behavioral Health – Diversionary Services – Non-24-Hour
30	Behavioral Health –Standard Outpatient Services
31	Behavioral Health –Other Services
32	Behavioral Health – Intensive Home or Community Based Outpatient Services for Youth (Please note this new category is where all CBHI services, except youth mobile crisis intervention would be listed. Youth mobile crisis intervention would be considered part of the Emergency Services Program Services.)

*** Use these categories *only* for the claims with Dates of Service before 07/01/2010.**

TABLE I – B1

Service Category (Using the SCO reporting groups)

Note: For the Claims with Date of Service **on or after October 1, 2016**

Value	Description
301	Hospital Inpatient
302	Behavioral Health (BH) Hospital Inpatient
303	Hospital Outpatient
304	Behavioral Health (BH) Hospital Outpatient
305	Professional
306	Vision
307	Dental
308	Therapy
309	Pharmacy/Drugs
309B	Pharmacy/Drugs (non-Part D)
310	Laboratory, Radiology, Testing
311	Institutional Long Term Care
312	Community Long Term Care
313	Home and Community Based Waiver
314	Transportation
315	Medical Equipment
316	Hospice
317	Case Management
318	Other Miscellaneous

TABLE I – B2

Service Category (Using the SCO reporting groups)

Note: For the Claims with Date of Service **before October 1, 2016**

Value	Description
101	Acute Inpatient
102	Chronic Inpatient
103	Outpatient Clinic
104	Mental Health/Substance Abuse
105	Physicians
106	Nonphysician Practitioners
107	Vision Care
108	Dental Care
109	Therapies
110	Pharmacy
111	Laboratory, radiology, testing
112	Institutional Long Term Care
113	Community Long Term Care
114	Waiver Services
115	Transportation
116	Supplies/ Durable Medical Equipment
117	Hospice
118	Care Management
119	Miscellaneous

TABLE I – C
Service Category (Using the One Care - ICO reporting groups)

Value	Description
201	Acute Inpatient
202	Inpatient – MH/SA
203	Hospital Outpatient
204	Outpatient – MH/SA
205	Professional
210	Pharmacy
212	Long-Term Care (LTC) Facility
213	Home and Community Based Services (HCBS)/Home Health
215	Transportation
216	Durable Medical Equipment (DME) and Supplies
217	*All Other

*Should follow the definition in the "Quarterly Financial Report" submitted to EOHHS Budget Unit

TABLE K
Bill Classifications - Frequency (3rd digit)

Value	Description
0	Nonpayment/Zero Claims
1	Admit thru discharge claim
2	Interim-first claim
3	Interim –continuing claim
4	Interim-last claim
5	Late charges only claim
6	Adjustment of prior claim
7	Replacement of prior claim
8	Void/back out of prior claim
9	Final claim for Home Health PPS episode
A	Admission/Election Notice
B	Hospice termination revocation notice
C	Hospice change of provider notice
D	Hospice Void/back out
E	Hospice change of ownership
F	Beneficiary Initiated adjustment claim-other
G	CWF Initiated adjustment claim-other
H	CMS Initiated adjustment claim-other
I	Intermediary adjustment claim (other than PRO or Provider)
J	Initiated adjustment claim-other
K	OIG initiated adjustment claim
L	Reserved for national assignment
M	MSP initiated adjustment claim
N	PRO adjustment Claim
O	Nonpayment/Zero Claims
P-W	Reserved for national assignment
X	Void/back out a prior abbreviated encounter submission
Y	Replacement of a prior abbreviated encounter submission
Z	New abbreviated encounter submission

TABLE M
Present on Admission (UB)
CMS POA Indicator Options and Definitions

Code	Reason for Code
Y	Diagnosis was present at time of inpatient admission
N	Diagnosis was not present at time of inpatient admission.
U	Documentation was insufficient to determine if the condition was present at the time of inpatient admission.
W	Clinically undetermined, Provider was unable to clinically determine whether the condition was present at the time of inpatient admission.
1	Unreported/Not used. Exempt from POA reporting. This code is equivalent to a blank on the UB-04, however; it was determined that blanks are undesirable when submitting this data via the 4010A.

CMS Updated on June 2008

TABLE O
UNIT OF MEASURE

#	Unit	Description	POPS Suggested Rules
1	F2	International Unit (for example, anti-hemophilia factor)	Physician Administered Drug claims only
2	GR	Gram (for creams, ointments, and bulk powder)	Physician Administered Drug claims only
3	ME	Milligrams (for creams, ointments, and bulk powder)	Physician Administered Drug claims only
4	UN	Unit (for tablets, capsules, suppositories, and powder filled vials)	Physician Administered Drug claims
5	ML	Milliliters (for liquids, suspensions, and lotions)	Physician Administered Drug claims **and** Pharmacy
6	EA	Each	Pharmacy claims only
7	GM	Gram	Pharmacy claims only

Unit of Measure Reference

#	Unit	Standard Referenced	Available Link
1	F2	ANSI 5010 837P and ANSI 5010 837I	
2	GR	ANSI 5010 837P and ANSI 5010 837I	
3	ME	ANSI 5010 837P and ANSI 5010 837I	
4	UN	ANSI 5010 837P and ANSI 5010 837I	
5	ML	ANSI 5010 837P, ANSI 5010 837I, and NCPDP	NCPDP: http://www.ncpdp.org/NCPDP/media/pdf/BUS_fact_sheet.pdf
6	EA	NCPDP	NCPDP: http://www.ncpdp.org/NCPDP/media/pdf/BUS_fact_sheet.pdf
7	GM	NCPDP	NCPDP: http://www.ncpdp.org/NCPDP/media/pdf/BUS_fact_sheet.pdf

8.0 Quantity and Quality Edits, Reasonability and Validity Checks

Raw Data

- File layout format
- Length and data type of the fields
- Reasonability of data
- ***ICD Version Qualifier*** (field # 193) is populated on every encounter claim record that has either ICD diagnosis codes or ICD procedure codes.
- All ICD diagnosis and ICD procedure codes on a claim record are consistent with ICD Version Qualifier.

Data Quality

- Each field is checked for quantity and quality
- Distribution reports
- Percentage reports
- Valid value reports
- Reasonability reports

Claims File

#	Field Name	MassHealth Standard
1	Org. Code	100% present
2	Claim Category	100% present and valid, as found in Data Elements table.
3	Entity PIDSL	100% present on all encounters
4	Record Indicator	100% present
5	Claim Number	100% present
6	Claim Suffix	100% present
7	Pricing Indicator	Directions will be provided later, validation standards TBD
8	Recipient DOB	100% present and valid, as compared to encounter service dates
9	Recipient Gender	100% present and valid, as found in Data Elements table
10	Recipient ZIP Code	100% present
11	Medicare Code	Provide if applicable
12	Other Insurance Code	100% present and valid, as found in Data Elements table
13	Submission Clarification Code	Provide on Pharmacy and Provider-Administered Drug claims
14	Claim Type	100% present and valid for BH Vendor only
15	Admission Date	100% present and valid value on all Inpatient claims, Long Term Care claims and all hospital (institutional) claims with admission.
16	Discharge Date	100% present and valid value on all Hospital discharges and Long Term Care discharges.
17	From Service Date	100% present and valid date on all claims; dates should be evenly distributed across time
18	To Service Date	100% present and valid date on all claims.
19	Primary Diagnosis	100% present and valid ICD codes on

#	Field Name	MassHealth Standard
		all Professional, Institutional (including Long Term Care) , Vision, and Transportation claims. • On Transportation claims for the services like "a ride to the grocery store", MCEs should use generic diagnosis codes such as: V46.3 – Wheelchair dependence; V49.9 – Unspecified problem with limbs and other problems; V58.9 – Unspecified aftercare. • Should be submitted on Dental claims when available. • Not required on Pharmacy claims. • E-codes not valid as primary diagnosis. • Consistent with ICD Version Qualifier.
20	Secondary Diagnosis	60% present and valid ICD codes on inpatient facility and 20% present and valid on other records, excluding drug and vision. Not routinely coded on Dental records and LTC. Consistent with ICD Version Qualifier.
21	Tertiary Diagnosis	Provide if available. Consistent with ICD Version Qualifier.
22	Diagnosis 4	Provide if available. Consistent with ICD Version Qualifier.
23	Diagnosis 5	Provide if available. Consistent with ICD Version Qualifier.
24	Type of Admission	100% present and valid value *(Admit Type, Table A) on all inpatient claims,* Long Term Care claims, and all hospital (institutional) claims with admission.
25	Source of Admission	100% present and valid value (*Admit Source, Table B*) *on all inpatient claims,* Long Term Care claims, and all hospital (institutional) claims with admission.
26	Procedure Code	98% present and valid in general but should be 100% present on all professional claims .Procedure Code Indicator match (i.e., if the code is a "CPT or HCPCS Level 1 Code" then the Procedure code indicator should be "2").
27	Procedure Modifier 1	Provide if available
28	Procedure Modifier 2	Provide if available
29	Procedure Modifier 3	Provide if available
30	Procedure Code Indicator	100% present and valid if Procedure Code field is filled
31	Revenue Code	98% present and valid on Hospital and Long Term Care claims only and should be 100% present on all Inpatient claim detail lines
32	Place of Service	100% present and valid value *on all professional claims.*
33	Type Of Bill	100% present and valid on all Inpatient and Long Term Care claims
34	Patient Discharge Status	100% present and valid value on all Inpatient claims, LTC claims, all hospital (institutional) claims with admission.
35	FILLER	
36	Quantity	100% present on all claim categories.
37	NDC Number	98% present and valid values, on Pharmacy claims; and on Hospital and Professional claims when applicable
38	Metric Quantity	100% present and valid values, only on Pharmacy claims, reasonability of values (total number of units or volume) and on Hospital and Professional claims when applicable.
39	Days Supply	100% present and valid values, only on all prescription drug Pharmacy claims.
40	Refill Indicator	100% present and valid values, only on all prescription drug Pharmacy claims.
41	Dispense As Written Indicator	100% present and valid values, only on all prescription drug Pharmacy claims.
42	Dental Quadrant	100% present and valid values (1-4), only on dental claims , where applicable
43	Tooth Number	100% present, only on dental claims, where applicable
44	Tooth Surface	100% present, only on dental claims, where applicable

#	Field Name	MassHealth Standard
45	Paid Date	100% present and valid date, falls within submitted date range, falls after "Admit, Discharge, To, and From Dates"
46	Service Class	100% present and valid for BH Vendor only
47	PCP Provider ID	100% present should be an enrolled provider listed in provider enrollment file. Not applicable to BH Vendor.
48	PCP Provider ID Type	100% present and valid based on PCP Provider ID field. Not applicable to BH Vendor.
49	PCC Internal Provider ID	If applicable, should be an enrolled provider listed in provider enrollment file.
50	Servicing Provider ID	100% present and valid on all claims except Pharmacy. Should be an enrolled provider listed in provider enrollment file.
51	Servicing Provider ID Type	100% present and valid on all claims except Pharmacy, Based on Servicing Provider ID field
52	Referring Provider ID	If applicable, should be an enrolled provider listed in provider enrollment file.
53	Referring Provider ID Type	100% present and valid, only when Referring Provider ID is present
54	Servicing Provider Class	100% present and valid on all records, as found in the Data Elements table.
55	Servicing Provider Type	100% present and valid value (*Servicing Provider Type, Table G*)
56	Servicing Provider Specialty	100% present and valid value (*Servicing Provider Specialty, Table H*)
57	Servicing Provider ZIP Code	100% present and valid
58	Billing Provider ID	100% present and valid on all claims; should be an enrolled provider listed in provider enrollment file.
59	Authorization Type	100% present and valid for BH Vendor only
60	Billed Charge	100% present financial field with implied 2 decimals, mathematical check with other dollar amounts
61	Gross Payment Amount	100% present financial field with implied 2 decimals, mathematical check with other dollar amounts
62	TPL Amount	If applicable, financial field with implied 2 decimals, mathematical check with other dollar amounts
63	Medicare Amount	If applicable, financial field with implied 2 decimals, mathematical check with other dollar amounts
64	Copay/Coinsurance	If applicable, financial field with implied 2 decimals, mathematical check with other dollar amounts
65	Deductible	If applicable, financial field with implied 2 decimals, mathematical check with other dollar amounts
66	Ingredient Cost	100% present and valid on prescription drug records, financial field with implied 2 decimals, mathematical check with other dollar amounts only on Pharmacy claims
67	Dispensing Fee	100% present and valid on prescription drug records, financial field with implied 2 decimals, mathematical check with other dollar amounts only on Pharmacy claims
68	Net Payment	100% present financial field with implied 2 decimals, mathematical check with other dollar amounts
69	Withhold Amount	If applicable, financial field with implied 2 decimals, mathematical check with other dollar amounts
70	Record Type	100% present and valid on all records, as found in the Data Elements table, dollar amount checks
71	Group Number	100% present and valid
72	DRG	100% present and valid value (001 - 495), on Acute Inpatient Hospital claims, when collected by plan.
73	EPSDT Indicator	Not coded at the present time
74	Family Planning Indicator	Not coded at the present time
75	MSS/IS	Not coded at the present time
76	New Member ID (consistent with above data)	100% Present and valid on all claims; not allowed to be missed or invalid.

#	Field Name	MassHealth Standard
77	Former Claim Number	100% present and valid, only when Record Type is not O
78	Former Claim Suffix	100% present and valid, only when Record Type is not O
79	Record Creation Date	100% present and valid date
80	Service Category	100% present and valid (*Service Category, Table I*)
81	Prescribing Prov. ID	100% present and valid on Pharmacy claims. Should be an enrolled provider listed in provider enrollment file.
82	Date Script Written	100% present and valid on Pharmacy claims.
83	Compound Indicator	100% present and valid on prescription drug records
84	Rebate Indicator	100% present and valid on prescription drug records
85	Admitting Diagnosis	100% present and valid value on all Inpatient claims, Long Term Care claims, and all hospital (institutional) claim with admission.
86	Allowable Amount	100% present and valid, financial field with implied 2 decimals, mathematical check with other dollar amounts
87	Attending Prov. ID	100% present should be an enrolled provider listed in provider enrollment file. Inpatient Claims only.
88	Non-covered Days	Provide if applicable
89	External Injury Diagnosis 1	Provide if available. Consistent with ICD Version Qualifier.
90	Claim Received Date	100% present and valid date
91	Frequency	100% present and valid on Inpatient claims.
92	PCC Internal Provider ID Type	100% present and valid, when PCC Provider ID is present
93	Billing Provider ID _Type	100% present, and valid on all claims.
94	Prescribing Prov. ID _ Type	100% present and valid on Pharmacy claims.
95	Attending Prov. ID _ Type	100% present, and valid
96	Admission Time	100% present and valid value on Hospital and Long Term Care claims
97	Discharge Time	100% present and valid value on Hospital and Long Term Care claims
98	Diagnosis 6	Provide if available. Consistent with ICD Version Qualifier.
99	Diagnosis 7	Provide if available. Consistent with ICD Version Qualifier.
100	Diagnosis 8	Provide if available. Consistent with ICD Version Qualifier.
101	Diagnosis 9	Provide if available. Consistent with ICD Version Qualifier.
102	Diagnosis 10	Provide if available. Consistent with ICD Version Qualifier.
103	Surgical Procedure code 1	Provide if available. Consistent with ICD Version Qualifier.
104	Surgical Procedure code 2	Provide if available. Consistent with ICD Version Qualifier.
105	Surgical Procedure code 3	Provide if available. Consistent with ICD Version Qualifier.
106	Surgical Procedure code 4	Provide if available. Consistent with ICD Version Qualifier.
107	Surgical Procedure code 5	Provide if available. Consistent with ICD Version Qualifier.
108	Surgical Procedure code 6	Provide if available. Consistent with ICD Version Qualifier.
109	Surgical Procedure code 7	Provide if available. Consistent with ICD Version Qualifier.
110	Surgical Procedure code 8	Provide if available. Consistent with ICD Version Qualifier.
111	Surgical Procedure code 9	Provide if available. Consistent with ICD Version Qualifier.
112	Employment	Provide if available
113	Auto Accident	Provide if available
114	Other Accident	Provide if available
115	Total Charges	Provide if available
116	Non Covered charges	Provide if available
117	Coinsurance	Provide if available
118	Void Reason Code	Provide if available
119	DRG Description	Provide if applicable
120	DRG Type	Provide if applicable
121	DRG Version	Provide if applicable
122	DRG Severity of Illness Level	Provide if applicable
123	DRG Risk of Mortality Level	Provide if applicable
124	Patient Pay Amount	Provide if applicable
125	Patient Reason for Visit Diagnosis 1	Provide if applicable. Consistent with ICD Version Qualifier.

#	Field Name	MassHealth Standard
126	Patient Reason for Visit Diagnosis 2	Provide if applicable. Consistent with ICD Version Qualifier.
127	Patient Reason for Visit Diagnosis 3	Provide if applicable. Consistent with ICD Version Qualifier.
128	Present on Admission (POA) 1	100% present on Hospital and Long Term Care claims
129	Present on Admission (POA) 2	Provide if Diagnosis 2 is available on Hospital and Long Term Care claims
130	Present on Admission (POA) 3	Provide if Diagnosis 3 is available on Hospital and Long Term Care claims
131	Present on Admission (POA) 4	Provide if Diagnosis 4 is available on Hospital and Long Term Care claims
132	Present on Admission (POA) 5	Provide if Diagnosis 5 is available on Hospital and Long Term Care claims
133	Present on Admission (POA) 6	Provide if Diagnosis 6 is available on Hospital and Long Term Care claims
134	Present on Admission (POA) 7	Provide if Diagnosis 7 is available on Hospital and Long Term Care claims
135	Present on Admission (POA) 8	Provide if Diagnosis 8 is available on Hospital and Long Term Care claims
136	Present on Admission (POA) 9	Provide if Diagnosis 9 is available on Hospital and Long Term Care claims
137	Present on Admission (POA) 10	Provide if Diagnosis 10 is available on Hospital and Long Term Care claims
138	Diagnosis 11	Provide if available. Consistent with ICD Version Qualifier.
139	Present on Admission (POA) 11	Provide if Diagnosis 11 is available on Hospital and Long Term Care claims
140	Diagnosis 12	Provide if available. Consistent with ICD Version Qualifier.
141	Present on Admission (POA) 12	Provide if Diagnosis 12 is available on Hospital and Long Term Care claims
142	Diagnosis 13	Provide if available. Consistent with ICD Version Qualifier.
143	Present on Admission (POA) 13	Provide if Diagnosis 13 is available on Hospital and Long Term Care claims
144	Diagnosis 14	Provide if available. Consistent with ICD Version Qualifier.
145	Present on Admission (POA) 14	Provide if Diagnosis 14 is available on Hospital and Long Term Care claims
146	Diagnosis 15	Provide if available. Consistent with ICD Version Qualifier.
147	Present on Admission (POA) 15	Provide if Diagnosis 15 is available on Hospital and Long Term Care claims
148	Diagnosis 16	Provide if available. Consistent with ICD Version Qualifier.
149	Present on Admission (POA) 16	Provide if Diagnosis 16 is available on Hospital and Long Term Care claims
150	Diagnosis 17	Provide if available. Consistent with ICD Version Qualifier.
151	Present on Admission (POA) 17	Provide if Diagnosis 17 is available on Hospital and Long Term Care claims
152	Diagnosis 18	Provide if available. Consistent with ICD Version Qualifier.
153	Present on Admission (POA) 18	Provide if Diagnosis 18 is available on Hospital and Long Term Care claims
154	Diagnosis 19	Provide if available. Consistent with ICD Version Qualifier.
155	Present on Admission (POA) 19	Provide if Diagnosis 19 is available on Hospital and Long Term Care claims
156	Diagnosis 20	Provide if available. Consistent with ICD Version Qualifier.
157	Present on Admission (POA) 20	Provide if Diagnosis 20 is available on Hospital and Long Term Care claims
158	Diagnosis 21	Provide if available. Consistent with ICD Version Qualifier.
159	Present on Admission (POA) 21	Provide if Diagnosis 21 is available on Hospital and LTC claims
160	Diagnosis 22	Provide if available. Consistent with ICD Version Qualifier.

#	Field Name	MassHealth Standard
161	Present on Admission (POA) 22	Provide if Diagnosis 22 is available on Hospital and Long Term Care claims
162	Diagnosis 23	Provide if available. Consistent with ICD Version Qualifier.
163	Present on Admission (POA) 23	Provide if Diagnosis 23 is available on Hospital and Long Term Care claims
164	Diagnosis 24	Provide if available. Consistent with ICD Version Qualifier.
165	Present on Admission (POA) 24	Provide if Diagnosis 24 is available on Hospital and Long Term Care claims
166	Diagnosis 25	Provide if available. Consistent with ICD Version Qualifier.
167	Present on Admission (POA) 25	Provide if Diagnosis 25 is available on Hospital and Long Term Care claims
168	Diagnosis 26	Provide if available. Consistent with ICD Version Qualifier.
169	Present on Admission (POA) 26	Provide if Diagnosis 26 is available on Hospital and Long Term Care claims
170	Present on Admission (POA) EI 1	Provide if External Injury Diagnosis 1 is available on Hospital and Long Term Care claims
171	External Injury Diagnosis 2	Provide if available. Consistent with ICD Version Qualifier.
172	Present on Admission (POA) EI 2	Provide if External Injury Diagnosis 2 is available on Hospital and Long Term Care claims
173	External Injury Diagnosis 3	Provide if available. Consistent with ICD Version Qualifier.
174	Present on Admission (POA) EI 3	Provide if External Injury Diagnosis 3 is available on Hospital and Long Term Care claims
175	External Injury Diagnosis 4	Provide if available. Consistent with ICD Version Qualifier.
176	Present on Admission (POA) EI 4	Provide if External Injury Diagnosis 4 is available on Hospital and Long Term Care claims
177	External Injury Diagnosis 5	Provide if available. Consistent with ICD Version Qualifier.
178	Present on Admission (POA) EI 5	Provide if External Injury Diagnosis 5 is available on Hospital and Long Term Care claims
179	External Injury Diagnosis 6	Provide if available. Consistent with ICD Version Qualifier.
180	Present on Admission (POA) EI 6	Provide if External Injury Diagnosis 6 is available on Hospital and Long Term Care claims
181	External Injury Diagnosis 7	Provide if available. Consistent with ICD Version Qualifier.
182	Present on Admission (POA) EI 7	Provide if External Injury Diagnosis 7 is available on Hospital and Long Term Care claims
183	External Injury Diagnosis 8	Provide if available. Consistent with ICD Version Qualifier.
184	Present on Admission (POA) EI 8	Provide if External Injury Diagnosis 8 is available on Hospital and Long Term Care claims
185	External Injury Diagnosis 9	Provide if available. Consistent with ICD Version Qualifier.
186	Present on Admission (POA) EI 9	Provide if External Injury Diagnosis 9 is available on Hospital and Long Term Care claims
187	External Injury Diagnosis 10	Provide if available. Consistent with ICD Version Qualifier.
188	Present on Admission (POA) EI 10	Provide if External Injury Diagnosis 10 is available on Hospital and Long Term Care claims
189	External Injury Diagnosis 11	Provide if available. Consistent with ICD Version Qualifier.
190	Present on Admission (POA) EI 11	Provide if External Injury Diagnosis 11 is available on Hospital and Long Term Care claims
191	External Injury Diagnosis 12	Provide if available. Consistent with ICD Version Qualifier.
192	Present on Admission (POA) EI 12	Provide if External Injury Diagnosis 12 is available on Hospital and Long Term Care claims
193	ICD Version Qualifier	100 % Present on all Professional and Institutional claims. 100% required on all other claims when at least one ICD diagnosis code or ICD surgical procedure code is submitted.
194	Procedure Modifier 4	Provide if available
195	Service Category Type	100% present and valid
196	Ambulance Patient Count	Provide if applicable
197	Obstetric Unit Anesthesia Count	Provide if applicable
198	Prescription Number	100% present on Pharmacy claims

#	Field Name	MassHealth Standard
199	Taxonomy Code	Provide if available
200	Rate Increase Indicator	Provide if applicable
201	Bundle Indicator	100% present on bundled claims
202	Bundle Claim Number	Provide if available. Follow instructions in Section 2.0 - Data Element Clarifications
203	Bundle Claim Suffix	Provide if available. Follow instructions in Section 2.0 - Data Element Clarifications
204	Value Code	Provide on the new-born claim lines
205	Value Amount	Provide when Value Code is present in field # 203
206	Surgical Procedure Code 10	Provide if available. Consistent with ICD Version Qualifier.
207	Surgical Procedure Code 11	Provide if available. Consistent with ICD Version Qualifier.
208	Surgical Procedure Code 12	Provide if available. Consistent with ICD Version Qualifier.
209	Surgical Procedure Code 13	Provide if available. Consistent with ICD Version Qualifier.
210	Surgical Procedure Code 14	Provide if available. Consistent with ICD Version Qualifier.
211	Surgical Procedure Code 15	Provide if available. Consistent with ICD Version Qualifier.
212	Surgical Procedure Code 16	Provide if available. Consistent with ICD Version Qualifier.
213	Surgical Procedure Code 17	Provide if available. Consistent with ICD Version Qualifier.
214	Surgical Procedure Code 18	Provide if available. Consistent with ICD Version Qualifier.
215	Surgical Procedure Code 19	Provide if available. Consistent with ICD Version Qualifier.
216	Surgical Procedure Code 20	Provide if available. Consistent with ICD Version Qualifier.
217	Surgical Procedure Code 21	Provide if available. Consistent with ICD Version Qualifier.
218	Surgical Procedure Code 22	Provide if available. Consistent with ICD Version Qualifier.
219	Surgical Procedure Code 23	Provide if available. Consistent with ICD Version Qualifier.
220	Surgical Procedure Code 24	Provide if available. Consistent with ICD Version Qualifier.
221	Surgical Procedure Code 25	Provide if available. Consistent with ICD Version Qualifier.
222	Attending Prov. ID Address Location Code	Provide when Attending Prov. ID is present
223	Billing Provider ID Address Location Code	Provide when Billing Provider ID is present
224	Prescribing Prov. ID Address Location Code	Provide when Prescribing Prov. ID is present
225	PCP Provider ID Address Location Code	Provide when PCP Provider ID is present
226	Referring Provider ID Address Location Code	Provide when Referring Provider ID is present
227	Servicing Provider ID Address Location Code	Provide when Servicing Provider ID is present
228	PCC Provider ID Address Location Code	Provide when PCC Internal Provider ID is present
229	Submission Clarification Code 2	Provide on Pharmacy and Provider-Administered Drug claims
230	Submission Clarification Code 3	Provide on Pharmacy and Provider-Administered Drug claims
231	Unit of Measure	100 % Provide on Pharmacy and/or Physician-Administered Drug claims
232	Provider Payment	Provide when available
233	Filler	

9.0 Appendices

Appendix C – *Member Enrollment File Specifications*

1. ***Overview:***

MCEs are required to submit member enrollment data on a monthly basis along with Encounter data submission. Member level enrollment data are needed for multiple EHS projects.
For example, the updated Member Enrollment File captures member enrollment with a PCP and member demographics.
In addition, MassHealth would like to start obtaining Care Coordination and/or Care Management providers' information for the analysis of this aspect of care delivery.

2. ***Technical Specifications:***

MCEs should submit a full refresh of the following three files on a monthly basis.

Member File

1. Each MCE should submit a full refresh of Member File of all MassHealth and CommCare members who have been enrolled with the MCE on or after 1/1/2010 including members who ended their enrollment after 1/1/2010.
2. The Member File contains the **member** MassHealth ID and demographic information.
3. The Member File is a snapshot as of the end of the month prior to the submission date. For example, the "as of" date for data submitted end of September 2013 is August 31, 2013.
4. The Member File always contains the most current member demographic information.
5. Member records submitted by the MCEs stay in EHS DW unless the MCE sends a "delete" file with the member records that have to be removed from EHS DW system. ***This file will only be sent when the MCE determines that the member should never have been part of EOHHS population and had been erroneously sent to MassHealth.*** In this case, the member in the delete file will be deleted from both the Member File and the Member Enrollment File (See section 3 –Submission Process).

Member Enrollment File

1. Each MCE should submit a full refresh of all MassHealth and CommCare members who have been enrolled with a **PCP and/or CM Provider** (Care Coordinator, Care Coordination Program, Care Manager, or Care Management Program) on or after 1/1/2010 including members who ended their enrollment after 1/1/2010.
2. The file should include ***all*** enrollments since 1/1/2010. For example, if a member had three PCP enrollments during this period, then all three enrollments will be reported in the file.
3. Begin and End Enrollment dates must reflect changes in member ***enrollment*** with a PCP, CM Provider and changes in Practice affiliation.
4. Members who are enrolled with an MCE and are in the Member File, but do not have PCP or CM Provider enrollment should ***not*** be included in Member Enrollment file.
5. All members included in the Member Enrollment File should also be included in the Member File.
6. Any member enrollment record that existed in prior files and is not submitted in current files get "soft" deleted from MassHealth system.

A. Member Enrollment File Providers and Practices

1. Care Coordinators, Care Managers, Care Coordination and Management Programs are referred to as **CM Providers**.
2. PCPs and CM Providers are considered **"Providers**", and their IDs should be submitted in the Provider ID field.
3. The Practice that the above providers are associated with is referred to as "**Practice**", and the Practice Provider ID should be submitted in the Practice ID field.
4. If one Practice location cannot be identified for the member enrollment with a PCP then MCEs should provide the ID for the PCP's head contracting entity in the Practice ID field.
5. A "Provider Enroll Type" field indicates whether the Provider ID is for a PCP or a CM Provider.
6. A "Care Level" field indicates whether the **CM Provider IDs** are submitted **at the MCE or Practice/Provider level**.
7. If a member is enrolled with two types of providers (e.g. PCP and Care Manager), two records will be submitted with two different Provider Enroll Types for that member even if the PCP happens to be the same provider as the Care Manager.
8. MCEs would need to submit unique identifiers for the **CM Providers**. These unique identifiers must be maintained by the MCE and must be included in the **Care Management Provider File** (see below)
9. The only information required in the Member Enrollment File for a Provider and Practice is Provider ID/Provider ID Type and Practice ID/Practice ID Type.
10. Every Provider ID **for a PCP** and every Practice ID must exist in the Provider File submitted in the Encounter file.
11. Every Provider ID **for a CM Provider** must exist in the **Care Management Provider File** (see Care Management Provider File below)
12. Any change in ***Provider or Practice*** demographic information would ***not*** require the submission of any new records in the Member Enrollment File. Demographic information will be maintained in the Encounter Provider File or the Care Management Provider File.

B. Member Enrollment File Begin and End Enrollment Dates

1. The Member Enrollment File will have "Begin" and "End" Enrollment Dates to identify all enrollments with a PCP or CM Providers.
2. Any change in the member enrollment with a provider would require additional records with new "Begin" and "End" Enrollment dates.
3. "Begin" and "End" enrollment dates must be submitted with each record. End Enrollment Date for "active" enrollments with a provider will be submitted as "End of Time" (EOT – 99991231)

Care Management Provider File

1. MCE will submit a Care Management Provider File that includes all **CM Providers** (Care Coordinators, Care Managers, Care Coordination and Management Programs) ***who are not inlcuded in the Encounter Provider File.***
2. The Care Management Provider File will have "Effective" and "Term" dates for CM Providers that must be submitted with each record. Term Date for "active" records should be submitted as "End of Time" (EOT – 99991231)

3. <u>Submission Process</u>:

1. Member ZIP File must be named "MCE_MEMBER_YYYYMMDD.zip" (e.g. BMC_MEMBER_20130831.zip).
2. Member ZIP File must include Member File, Member Enrollment File, Care Management Provider File and Member Metadata File.
3. Member File, Member Enrollment File, and Care Management Provider File must be submitted as "Pipe" delimited text files.
4. The member metadata file in the Member ZIP File must be named MEM_metadata.txt.
5. Member ZIP File must be submitted at the same time the Encounter data is submitted. <u>It should be placed on SFTP server **after** the claims zip file is posted.</u>
6. A zero byte file "**mem_mce_done.txt**" must be placed on SFTP server along with the Member Zip file. The file "mem_mce_done.txt" is only needed when the Member Zip file is submitted.

Member Metadata File

Metadata Field	**Submission**
MCE_Id="Value"	Mandatory
Date_Created=" YYYYMMDD"	Mandatory
Member_File_Name="Value"	Mandatory
MemEnroll_File_Name="Value"	Mandatory
CareMgmt_File_Name="Value"	Mandatory
Total_Member_Records="Value"	Mandatory
Total_MemEnroll_Records="Value"	Mandatory
Total_CareMgmt_Records="Value"	Mandatory
Time_MemEnroll_From="Value" (YYYYMMDD)	Mandatory
Return_To="Email Address"	Mandatory

<u>Notes:</u>

i. Total_Member_Records is the total number of records in the Member File
ii. Total_MemEnroll_Records is the total number of records in the Member Enrollment File.
iii. Time_MemEnroll_From is the earliest "Begin" Enrollment Date in the Member Enrollment File.
iv. Total_CareMgmt_Records is the total number of records in the Care Management Provider File.
v. For files missing from a submission set corresponding field value to "none.txt"

Member Delete File

1. Member Delete File has the same format as Member File but will only have the member records that need to be deleted from our system. ***This file will only be sent when the MCE determines that the member should never have been part of EOHHS population and had been erroneously sent to MassHealth.***
2. The member in the delete file will be deleted from both the Member File and the Member Enrollment File.
3. Member Delete File will be submitted independently from the Member Zip file and will be named **MCE_DELETE_MEM_YYYYMMDD.txt** (e.g. BMC_DELETE_MEM_20130930.txt).
4. The Member Delete File can be submitted any time, however the MCE must send an email to MassHealth Data Warehouse to notify them about the submission of a delete file.

4. <u>Validation Rules:</u>

Member File

1. All Member IDs submitted in the Member File should exist in MMIS.
2. In the following scenarios, all records for that Member ID will be rejected:
    1. Member ID is missing
    2. Member ID is invalid
    3. Org. Code is missing
    4. Org. Code is not meeting MassHealth Standards
    5. Entity Identifier is not meeting MassHealth Standards
3. Member File data are ***not*** used in the claims validation process. Rejected Member File records do not affect encounter claims data load.

Member Enrollment File

1. All Member IDs submitted in the Member Enrollment File must exist in MMIS
2. All Member IDs submitted in the Member Enrollment File must exist in Member File
3. The records get rejected if:
    - Member ID is missing
    - Member ID is invalid
    - Provider ID is missing
    - Provider ID is not found in MCE Provider Files
    - Provider ID Type is missing
    - Provider ID Type is not found in MCE Provider Files
    - Provider ID address location code is missing
    - Practice ID Type or Practice ID Address Location Code is missing when Practice ID is provided
    - Practice ID Type not found in MCE Provider File
    - Provider Enroll Type is missing
    - Provider Enroll Type is not valid as per specification
    - Care Level is missing
    - Care Level is not valid as per specification
    - Begin Enrollment Date is missing or invalid
    - End Enrollment Date is missing or invalid
    - Org. Code is missing
4. Member Enrollment File data are not used in claims validation process. Rejected Member Enrollment File records do not affect encounter claims data load.

***Care Management Provider File* – Not currently submitted**

1. All records in the Care Management Provider File will be rejected in the following scenarios:

a. Org. Code is missing
b. Org. Code is not meeting MassHealth Standards
c. CM Provider ID is missing

5. ***Member Error File:***
   1. All records in the Member File, Member Enrollment File and Care Management Provider File not meeting validation rules described in Section 4 will be rejected.
   2. An error file for the Member File will be posted on the FTP server and will be named "ERR_MCE_MEMBER_YYYYMMDD.txt". (e.g. ERR_BMC_MEMBER_20130930.txt)
   3. An error file for the Member Enrollment File will be posted on the FTP server and will be named "ERR_MCE_MEMENROLL_YYYYMMDD.txt". (e.g. ERR_BMC_MEMENROLL_20130930.txt)
   4. An error file for Care Management Provider File will be posted on the FTP server and will be named "ERR_MCE_CAREMGMT_YYYYMMDD.txt". (e.g. ERR_BMC_CAREMGMT_20130930.txt)
   5. Records that get rejected must be corrected and sent back to MassHealth to get into the system.
   6. Member and Member Enrollment correction files should follow the same format as the original files
   7. Member and Member Enrollment correction files must be submitted with the Encounter correction/manual override file or must be corrected in the following month's member files submission.
   8. Corrected records in Member File, Member Enrollment File or Care Management Provider File that still have errors will never go into MassHealth system and will not be overridden even when submitted along with the Manual Override Encounter file.

6. ***Files Layout:***

Member File Layout

#	Field	Description	Length	Type	Required	Comments
1	Org. Code	Unique ID assigned by MH DW to each submitting organization. **This code identifies your Organization :** 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	3	N	Required	
2	Member ID	The MassHealth ID for the **member**	12	C	Required	
3	Active Status Indicator	Y/N indicates whether the member has a current "Active" enrollment status with the MCE	1	C	Required	
4	Member Birth Date	Member Date of Birth	8	Date YYYYMMDD	Required	
5	Member Death Date	Member Date of Death	8	Date YYYYMMDD	Required	
6	Member First Name	Member first name	100	C	Required	
7	Member Last Name	Member last name	100	C	Required	
8	Member Middle Initial	Member Middle Initial	1	C	Required	
9	Member Gender	The gender of the member: "Male" ; "Female", or "Other" These values should be spelled out and should not be abbreviated	8	C	Required	
10	Member Ethnicity	Please follow the US Office of Management and Budget (OMB) standards for Classification of Race and Ethnicity	75	C	Provide if available	Values should have descriptions and not codes

#	Field	Description	Length	Type	Required	Comments
11	Member Race	Please follow the US Office of Management and Budget (OMB) standards for Classification of Race and Ethnicity	75	C	Provide if available	Values should have descriptions and not codes
12	Member Primary Language	The Primary Language of the Member	75	C	Provide if available	Values should have descriptions and not codes
13	Member Address 1	Member Street Address 1	100	C	Required	
14	Member Address 2	Member Street Address 2	100	C	Provider if applicable	
15	Member City	Member City	40	C	Required	
16	Member State	Member State	2	C	Required	
17	Member Zip Code	Member Zip Code	5	C	Required	
18	Homeless Indicator	Y/N. Indicates if the member is homeless	1	C	Provide if available	
19	Communication Access Needs Indicator	Y/N. Indicates if the member has special needs for communicator	1	C	Provide if available	
20	Disability Indicator	Y/N. Indicates if the member has a disability	1	C	Provide if available	
21	Disability Type	Identifies the disability type for a member. This is a place holder until the disability types are clearly defined. Values TBD	30	C	Provide if available	

Member Enrollment File Layout

#	Field	Description	Length	Type	Required	Comments
1	Org. Code	Unique ID assigned by MH DW to each submitting organization. **This code identifies your Organization :** 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	3	N	Required	
2	Member ID	The MassHealth ID for the member	12	C	Required	
3	Provider Enroll Type	This field indicates the Type of Provider a member is enrolled with. It should reflect the information entered in the Provider ID and ID Type. For example, if Provider Enroll Type is entered as '02' then the Provider ID and ID Type should be for the "Geriatric Coordinator" the member is enrolled with. **The values are as follows:** **01 = PCP** **02 = Geriatric Coordinator** **03 = LTSS Coordinator** **04 = Care Coordinator** **05 = Care Coordination Program (if no assigned care coordinator but member is enrolled in a care coordination program)** **06 = Care Manager**	2	C	Required	This is a key field and it indicates whether the provider fields are for a PCP or CM providers.

#	Field	Description	Length	Type	Required	Comments
		07 = Care Management Program (if no assigned care manager but member is enrolled in a care management program)				
4	Provider Enroll Type Description	The Description of the Provider Enroll Type. The description should be consistent with the value selected in Provider Enroll Type. If the value entered in Provider Enroll Type is **"01"** the description should be "PCP" If the value entered in Provider Enroll Type is **"02"** the description should be " Geriatric Coordinator" and so on	40	C	Required	
5	Care Level	This field is required with all CM Providers to indicate whether the Provider ID submitted is at the MCE or Practice/Provider level. If the Provider is a PCP, value "NA" **must** be entered in this field. Values are: "MCE" "PRV" "NA" for "Not Applicable"	3	C	Required	
6	Begin Enrollment Date	This is the beginning enrollment date with a PCP or CM Providers	8	Date YYYYMMDD	Required	
7	End Enrollment Date	This is the end enrollment date with a PCP or CM Providers	8	Date YYYYMMDD	Required	This value should be "99991231" for "active" enrollment which represents End of Time (EOT).

#	Field	Description	Length	Type	Required	Comments
8	Provider ID	Provider ID	15	C	Required	This ID should be consistent with the ID submitted in the Encounter Provider File for a provider. Information provided in this field should be consistent with the information submitted in the "Provider Enroll Type" field above. For example, if the Provider Enroll Type was submitted on a record as "01" then the Provider ID for that record would be for a PCP. This applies to all other values in the Provider Enroll Type.

#	Field	Description	Length	Type	Required	Comments
9	Provider ID Type	Provider ID Type is required when the provider is part of prior and current provider files submitted in the encounter data. The values are: 1 for NPI 6 for MCE Internal ID	1	C	Required	This ID Type should be consistent with the ID Type submitted in the Encounter Provider File for a provider. Information provided in this field should be consistent with the information submitted in the "Provider Enroll Type" field above. For example, if the Provider Enroll Type was submitted on a record as "01" then the Provider ID Type for that record would be the ID Type associated with a PCP. This applies to all other values in the Provider Enroll Type.
10	Practice ID	Practice ID	15	C	Highly important so please provide if available	This ID should be consistent with the ID submitted in the Encounter Provider File for a Practice
11	Practice ID Type	Practice ID Type. The values are: 1 for NPI 6 for MCE Internal ID	1	C	Highly important so please provide if available	This ID Type should be consistent with the ID Type submitted in the Encounter Provider File for a Practice

#	Field	Description	Length	Type	Required	Comments
12	PCC Provider ID Address Location Code	Code to identify address location of Provider ID in Field #8	15	C		
13	PCC Practice ID Address Location Code	Code to identify address location of Practice ID in Field #10.	15	C		
14	Entity PIDSL	ACO PIDSL for the ACO claims and MCO PIDSL for the MCO claims SCO PIDSL on SCO claims One Care PIDSL on One Care claims Example: 999999999A	10	C	Required on all ACO claims	Should be consistent with ACO PIDSL submitted in the encounter provider file

Care Management Provider File Layout – Not currently submitted

#	Field	Description	Length	Type	Required	Comments
1	Org. Code	Unique ID assigned by MH DW to each submitting organization.	3	N	Required	
2	CM Provider ID	The MCE unique identifier for CM Provider	15	C	Required	
3	CM Provider Last Name	CM Provider last name	100	C	Required	
4	CM Provider First Name	CM Provider first name	100	C	Provide if Applicable	
5	CM Provider Gender	M' for Male ; 'F' for Female, and 'O' for "Other"	**1**	C	Optional	
6	CM Provider Address	CM Provider Street Address	120	C	Required	
7	CM Provider City	CM Provider City	40	C	Required	
8	CM Provider State	CM Provider State	2	C	Required	
9	CM Provider Zip Code	CM Provider Zip Code	9	C	Required	
10	CM Provider Phone	CM Provider Telephone number	13	C "9999999999"	Required	Do not include characters like dashes or brackets – e.g. 6178889900
11	CM Provider Effective Date	Begin effective date for the CM Provider	8	C – YYYYMMDD	Required	
12	CM Provider Term Date	End effective date for CM Provider	8	C – YYYYMMDD	Required	This value should be "99991231" for "active" CM Provider IDs which represents End of Time (EOT).
13	Entity PIDSL	ACO PIDSL for the ACO claims and MCO PIDSL for the MCO claims SCO PIDSL on SCO claims One Care PIDSL on One Care claims Example: 999999999A	10	C	Required	
14	CM Provider ID TYPE		1	N		
15	CM Provider ID Location code		5	C		

Appendix D-2

COMMONWEALTH OF MASSACHUSETTS

EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES
MassHealth

Denied Claims Submission Requirements (Expanded Format)

Version 2.4

Date: October 01, 2021

Table of Contents

Table of Contents 2
Acronyms 3
1. Introduction 4
2. Logic and Input: 4
2.1 DW Design Requirements 4
2.2 File Submission Requirements 5
2.3 Submission Files Format (claims and metadata) 6
2.3.1 Format 6
2.3.2 Denied Claims Reason Code File Format 7
2.3.3 Denial Reason Codes Reference File Format 7
2.3.4 Denied Claims Data Set Elements 8
Service Data 10
Provider Data 16
Financial Data 17
Medicaid Program-Specific Data 18
Other Fields 20
3. Error Handling Section 34
4. Error Reports and Notifications to the Plans 34
4.1 Error Denied Claims Summary Report Format 34
4.2 Error Denied Claims Details Report Format 35
4.3 Error Denial Reason Code Report Format 35

Acronyms

ACO	Accountable Care Organization
DW	Data Warehouse
EOHHS	Executive Office of Health and Human Services
MCE	Managed Care Entity (MCO, SCO, One Care, and BH Vendor collectively)
MCO	Managed Care Organization
MH	MassHealth
PCC	Primary Care Clinician
PIDSL	Provider ID Service Location
SCO	Senior Care Options Plan

1. Introduction

There has been a business need to collect denied claims to allow for accurate analysis of risk adjustment, utilization, and healthcare quality measurement. EOHHS is adding a requirement to have all MCOs and the BH Vendor submit denied claims.

Denied claim lines should be included, even if they are part of the paid claim.

Please note that denied claims process is independent of paid claims process. Denied and Paid claims are submitted in separate files on different schedules and posted in different directories on SFTP server. Current process of paid claims continues to exist as usual, where the MCOs submit voids and replacements to paid claims loaded in MH DW.

The intent of this document is to outline formats of the files, data validation, and submission process requirements. Changes to the Denied Claims Data Set format introduced in Version 2.0 of the document reflect the changes applied to the Paid Encounter Data Set Expanded file format that were made for the implementation of the ACO program.

2. Logic and Input:

2.1 DW Design Requirements

2.1.1 DW implements minimal editing logic since denied claims can be denied for many reasons.

2.1.2 Individual claim lines might have several denial reasons.

2.1.3 When Billing Provider internal ID is not known, submit NPI number in place of Billing Provider ID with Billing Provider ID Type = 1. Billing Provider ID field should never be null.

2.1.4 Claims with invalid "New Member ID" values must not be submitted.

2.1.5 The following fields are critical for the load process and must have valid values:

#	Field Name	Field Number
1	Org. Code	# 1
2	Entity PIDSL	# 3
3	Claim Number	# 5
4	Claim Suffix	# 6
5	Billing Provider ID	# 58
6	Billing Provider ID Type	# 93
7	Billing Provider ID Address Location Code	# 223
8	New Member ID	# 76
9	Adjudication date	# 229

2.1.6 Format standards should be followed for all fields.

2.1.7 Email notifications will be sent to the MCOs with the status of submission.

2.2 File Submission Requirements

2.2.1 The denied claims files have to be placed on SFTP server by the 6th day of the submission month

2.2.2 The denied claims zip files should be placed on SFTP server in/mce/ehs_dw/**denied claims** folder. Error reports will be provided at the same location- /mce/ehs_dw/**denied claims** folder.

2.2.3 An initial production file contained denied claims with From Service Date since 1/1/2014, adjudicated through March 31, 2017 in their most recent state as of the date of submission. All the claims were sent as Original (Record Type = 'O') in July of 2017.

2.2.4 All the subsequent submissions should have denied claims adjudicated in the prior **quarter** with a 3 month lag.

For example, October 6, 2017, submission files contained denied claims with adjudication date from April 1, 2017, through June 30, 2017.

Few other examples

Submission Date	Claims Adjudication Dates
04/06/2018	10/01/2017 – 12/31/2017
07/06/2018	01/01/2018 – 03/31/2018
10/06/2018	04/01/2018 – 06/30/2018
01/06/2019	07/01/2018 – 09/30/2018

2.2.5 All denied claims must have values in the following fields:

#	Field #	Field Name	Error	Result
1	1	Org. Code	Null or Invalid	File rejection
2	3	Entity PIDSL	Null or Invalid	Record rejection
3	5	Claim Number	Null	Record rejection
4	6	Claim Suffix	Null	Record rejection
5	58	Billing Provider ID	Null	Record rejection
6	223	Billing Provider ID Address Location Code	Null	Record rejection
7	93	Billing Provider ID Type	Null	Record rejection
8	76	New Member ID	Null	Record rejection
9	229	Adjudication Date	Null *or* Less than DOS *or* less than DOB *or* invalid format	Record rejection

2.2.6 MCOs must re-submit rejected files / records with corrected data <u>within a week from rejection date</u>.

2.2.7 All providers' information must have been previously submitted by the MCOs in the paid Encounter claims files and exist in MH DW provider directory.

2.2.8 All New Member IDs must exist in MH DW reference source.

2.3 Submission Files Format (claims and metadata)

2.3.1 Format

2.3.1.1 MCOs should submit Zip file named in **"MCO_Denied_Claims_YYYYMMDD.zip"** format where "MCO" stands for the plans' name (i.e. "BMC_Denied_Claims_20170716")

2.3.1.2 Zip File must be accompanied by a zero byte file called ***mce_denied_done.txt***.

2.3.1.3 Denied Claims zip files should contain the following:

- Denied Claims File
- Denied Claims Reason Code File
- Denied Reason Codes Reference File
- Metadata File

2.3.1.4 All submitted files should be pipe-delimited and compressed using PKZIP/WINZIP or comparable program. All records in the data file should follow the record layout specified in "Denied Claims Data Set Elements" section, where the length represents the maximum length of each field. Padding fields with zeros or spaces is ***not*** required.

Each record should end with the standard MS Windows text file end-of-line marker ("\r\n" – a carriage control followed by a new line).

File Type: PKZIP/WINZIP compressed plain text file
Character Set: ASCII

2.3.1.5 MCOs will submit zip files on SFTP server in /home/mce/ehs_dw/denied_claims folder.

2.3.1.6 Multiple email addresses separated by comma can be included in the "Return_To" field in the metadata file.

2.3.1.7 Time Period ("Time_Period_From" and "Time_Period_To") in metadata should be based on adjudication date of the submission quarter.

2.3.1.8 Metadata file specifications: All denied claims submission files should have "Type_Of_Feed" value of "DENIED". All fields in metadata file are mandatory.

Metadata File Format:

	Description
MCO_ID="Value" (MCO: BMC, CAR, CHA, FLN, HNE, MBH, NHP)	The 3-letter identifier for the MCO
Date_Created=" YYYYMMDD"	Date the file was created
Denied_Claims="Value"	Name of denied claims file (#1)
Denied_Claims_Reason_Code="Value"	Name of Denied claims with reason codes file (#2)
Denied_Reason_Codes_Reference="Value"	Name of Reason code reference data file (#3)
Total_Records_Claims ="Value"	Total number of records in file #1
Total_Net_Payments_Claims="Value"	Total payment in file #1
Total_Records_Claims_Reason ="Value"	Total number of records in file #2
Total_Records_Reason_Reference ="Value"	Total number of records in file #3
Time_Period_From="Value" (YYYYMMDD)	Beginning date of Quarter based on Adjudication date

Time_Period_To="Value" (YYYYMMDD)	End date of Quarter based on Adjudication date
Return_To="email address"	List of MCO email addresses for notifications
Type_Of_Feed="DENIED"	Type of feed is always 'DENIED'

2.3.2 Denied Claims Reason Code File Format

All the Denial Reason Codes have to be submitted in agreement with Remittance Advice Remark Codes reported on 835 transactions.
All the claim lines in Claims file must have at least one match in Denied Reason Code file.
All the Claim Number & Claim Suffix combinations in Denied Claims Reason Code file should have a match in Claims file.

#	Field Name	Length	Data Type/Format
1	Org. Code	3	N
2	Claim Number	19	C
3	Claim Suffix	4	C
4	Denial Reason Code	10	C

2.3.3 Denial Reason Codes Reference File Format

All the Reason Codes in Denied Claims Reason Code file must have a match in Denial Reason Code Reference File and vice versa

#	Field Name	Length	Data Type/Format
1	Org. Code	3	N
2	Denial Reason Code	10	C
3	Denial Reason Code Description	200	C

2.3.4 Denied Claims Data Set Elements

The value 'X' indicates a Claim Category the data element is applicable under. The columns are labeled as:

- H – Facility (*except Long Term Care*)
- P – Professional
- L – Long Term Care
- R – Prescription Drug
- D – Dental

For the information on Tables A, B, C, D, F, F, G, H, I-A, I-B1, I-B2, I- C, K, M please refer to "Paid Encounter Data Set Request V4.8" specifications.

Demographic Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
1	Org. Code	Unique ID assigned by MH DW to each submitting organization. This code identifies your Organization : 465 Fallon Community Health Plan 469 Neighborhood Health Plan 997 Boston Medical Center HealthNet Plan 998 Network Health 999 Massachusetts Behavioral Health Partnership 470 CeltiCare 471 Health New England 501 Commonwealth Care Alliance 502 UnitedHealthCare 503 NaviCare 504 Senior Whole Health 505 Tufts Health Plan 506 BMC HealthNet Plan 601 Commonwealth Care Alliance 602 Network Health 603 Fallon Total	X	X	X	X	X	3	N
2	Claim Category	A code that indicates a category of the claim. Valid values are: 1 = Facility (*except Long Term Care*) 2 = Professional (includes transportation claims) 3 = Dental 4 = Vision 5 = Prescription Drug 6 = Long Term Care *(Nursing Home, Chronic Care & Rehab)*	X	X	X	X	X	1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
3	Entity PIDSL	ACO PIDSL on the ACO claims or MCO PIDSL on the MCO claims Example: 999999999A	X	X	X	X	X	10	C
4	Record Indicator	This information refers to the payment arrangement under which the rendering provider was paid. Value identifies whether the record was a fee-for-service claim, or a service provided under a capitation arrangement (encounter records). For encounter records, indicate whether there are Fee-For-Service (FFS) equivalents and payment amounts on the record. 0 Artificial record – Refers to a line item inserted to hold amounts / quantities available only at a summary (claim) level. 1 Claim Record – Refers to a claim paid on a Fee-For- Service (FFS) basis	X	X	X	X	X	1	C

Demographic Data (cont'd)

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
	Record Indicator (Continued)	2 Encounter Record with FFS equivalent - Refers to services provided under a capitation arrangement and for which an FFS equivalent is given 3 Encounter Record w/out FFS equivalent - Refers to services provided under a capitation arrangement but for which no FFS equivalent is available 4 Per Diem Payment - Refers to a record for an inpatient stay paid on a per diem basis. 5 DRG Payment - Refers to a record for an inpatient stay paid on a DRG basis 6 Bundled Summary-Level Line; this value refers to the amounts/quantities available in the MCE's source system. Use this value when none of the above Record Indicator values applies. 7 Bundled detail line with 0-dollar amount – Refers to a bundled detail claim line where the dollar amounts are 0 or not available at the detail level. Use this value when none of the above values apply ***See discussion under <u>Dollar Amounts</u> in the Data Elements Clarification Section.***							

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
5	Claim Number	A unique number assigned by the administrator to this claim (e.g., ICN, TCN, DCN). It is very important to include a Claim Number on each record since this will be the key to summarizing from the service detail to the claim level. ***See discussion under Claim Number/Suffix in the Data Elements Clarification Section***	X	X	X	X	X	19	C
6	Claim Suffix	This field identifies the line or sequence number in a claim with multiple service lines. ***See discussion under Claim Number/Suffix in the Data Elements Clarification Section***	X	X	X	X	X	4	C
7	Pricing Indicator	Pricing Indicator; currently it is a subject of internal discussion. *A notification will be sent to the MCEs when decision is made.	X	X	X	X	X	20	C
8	Recipient DOB	The birth date of the patient expressed as YYYYMMDD. For example, August 31, 1954 would be coded "19540831".	X	X	X	X	X	8	D/YYYYMMDD
9	Recipient Gender	The gender of the patient: 1= Male 2=Female 3=Other	X	X	X	X	X	1	C
10	Recipient ZIP Code	The ZIP Code of the patient's residence as of the date of service.	X	X	X	X	X	5	N
11	Medicare Code	A code indicating if Medicare coverage applies and, if so, the type of Medicare coverage. 0= No Medicare 1 = Part A Only 2 = Part B Only 3 = Part A and B	X	X	X	X	X	1	N

Service Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
12	Other Insurance Code	A Yes/No flag that indicates whether third party liability exists. 1 = Yes; 2 = No	X	X	X	X	X	1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
13	Submission Clarification Code	420-DK- Code indicating that the pharmacist is clarifying the submission. Values from 1 to 36 should be sent on pharmacy claims when available. The values and descriptions of the Submission Clarification Code are in Table N of the Paid Encounter Data Set Requirements specifications V 4.8				X		7	N
14	Claim Type	BH Vendor Specific field	X	X	X	X	X	18	C
15	Admission Date	For facility services, the date the recipient was admitted to the facility. The format is YYYYMMDD.	X		X			8	D/YYYYMMDD
16	Discharge Date	For facility services, the date the recipient was discharged from the facility. The format is YYYYMMDD. Cannot be prior to Admission Date	X		X			8	D/YYYYMMDD
17	From Service Date	The actual date the service was rendered; if services were rendered over a period of time, this is the date of the first service for this record. The format is YYYYMMDD.	X	X	X	X	X	8	D/YYYYMMDD
18	To Service Date	The last date on which a service was rendered for this record. The format is YYYYMMDD.	X	X	X		X	8	D/YYYYMMDD
19	Primary Diagnosis	The ICD diagnosis code chiefly responsible for the hospital confinement or service provided. The code should be left justified, coded to the fifth digit when applicable (blank filled when less than five digits are applicable). *DO NOT include decimal points in the code.* ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X		X	7	C/ No decimal points (780.31 must be entered as 78031)
20	Secondary Diagnosis	The ICD diagnosis code explaining a secondary or complicating condition for the service. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
21	Tertiary Diagnosis	The tertiary ICD diagnosis code. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
22	Diagnosis 4	The fourth ICD diagnosis code. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
23	Diagnosis 5	The fifth ICD diagnosis code. See above for format. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/ No decimal points
24	Type of Admission	Should be valid and present on all Hospital and Long Term Care claims with hospital admission. For the UB standard values see Table A.	X		X			1	C
25	Source of Admission	Should be valid and present on all Hospital and Long Term Care claims with hospital admission. For the UB standard values see Table B	X		X			1	C
26	Procedure Code	A code explaining the procedure performed. This code may be any valid code included in the coding systems identified in the Procedure Type field below. *Any internal coding systems used must be translated to one of the coding systems identified in field #**30** below.* Should not contain ICD procedure codes. All ICD procedure codes should be submitted in the surgical procedure code fields (#101 – #113) ***including the ICD-treatment procedure codes*** ***See discussion in Data Element Clarifications section.***	X	X	X		X	6	C
27	Procedure Modifier 1	A current procedure code modifier (CPT or HCPCS) corresponding to the procedure coding system used, when applicable.	X	X	X		X	2	C
28	Procedure Modifier 2	Second procedure code modifier, required, if used.	X	X	X		X	2	C
29	Procedure Modifier 3	Third procedure code modifier, required, if used.	X	X	X		X	2	C
30	Procedure Code Indicator	A code identifying the type of procedure code used in field#26: 2= CPT or HCPCS Level 1 Code 3= HCPCS Level II Code 4= HCPCS Level III Code (State Medicare code). 5= American Dental Association (ADA) Procedure Code (Also referred to as CDT code.) 6= State defined Procedure Code 7= Plan specific Procedure Code ICD procedure codes should go in surgical procedure code fields (Field # 103 – 111)	X	X	X		X	1	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		State defined procedure codes should be used, when coded, for services such as EPSDT procedures. ***See discussion in the Data Element Clarifications section.***							
31	Revenue Code	For facility services, the UB Revenue Code associated with the service. *Only standard UB92 Revenue Codes values are allowed; plans may* ***not*** *use "in house" codes. Revenue code less than 4 digits long should be submitted with one leading zero. For Example:* *a. Revenue code 1 should be submitted as '01';* *b. Revenue Code 23 - as '023;* *c. Revenue code 100 - as '0100';* *Revenue Code 2100 – as '2100'*	X		X			4	C
32	Place of Service	This field hosts Place of Service (POS) that comes on the Professional claim). See Table C for CMS 1500 standard		X			X	2	C
33	Type Of Bill	For encounter data, supporting UB claims submission the Type of Bill is submitted as a 3-digit bill type in accordance with national billing guideline. The first two digits denote the place of services and the third digits denotes the frequency. See Table D for UB Type of Bill values indicating place. ***Note*****:** for UB Type of Bill, use the 1st and 2nd positions only.) Frequency values can be found in Table K of the Data Set Requirements Specifications V 4.8	X		X			3	C
34	Patient Discharge Status	This is 2-digit Discharge Status Code (UB Patient Status) for hospital admissions. Values from 1 to 9 should always be entered with leading '0'. *Examples:* a. Patient Discharge Status '1' should be submitted as '01'; B. Patient Discharge Status '19' should be submitted as '19'.	X		X			2	C
35	FILLER							2	C
36	Quantity	This value represents the actual quantity and should be submitted with decimal point when applicable. For inpatient admissions, the number of days of confinement. Count the day of admission but not the day of discharge (for admission and discharge on the same day, Quantity is counted as 1). For all other procedures, the number of units performed for this procedure. For	X	X	X		X	9	SN

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		most procedures, this number should be "1". In some cases, a procedure may be repeated, in which case this number should reflect the number of times the procedure was performed. For anesthesia services, this should be the total number of minutes that make up the beginning and ending clock time of anesthesia service administered. Please make sure that the Quantity corresponds to the procedure code. For example, if the psychiatric code 90844 is used (Individual psychotherapy, 45-50 minutes), the Quantity should be "1" NOT "45" or "50". For Inpatient records, it should represent number of days of care. Values of 30, 60, or 100 are most common on drug records. *Note:* Length of this field has been increased to accommodate the actual quantity. Quantity=10 should be submitted as 10; Quantity=10.5 should be submitted as 10.5; Quantity=10.55 should be submitted as 10.55							
37	NDC Number	For prescription drugs, the valid National Drug Code number assigned by the Food and Drug Administration (FDA). For Compound drugs claims submit NDC Number for the primary drug, If primary drug is unknown, submit NDC Number for most expensive drug. NDC codes having less than 11 digits should be submitted with leading 0's. For Example NDC "603373932" should be submitted as "00603373932".	X	X		X		11	N
38	Metric Quantity	For prescription drugs, the total number of units or volume (e.g., tablets, milligrams) dispensed. Should be submitted with decimal point when applicable. *Note:* Length of this field has been increased to accommodate the actual Metric Quantity. Metric Quantity=10 should be submitted as 10; Metric Quantity=10.5 should be submitted as 10.5; Metric Quantity=10.55 should be submitted as 10.55	X	X		X		9	N
39	Days Supply	The number of days of drug therapy covered by this prescription.				X		3	N
40	Refill Indicator	A number indicating whether this is an original prescription (0) or a refill number (e.g., 1, 2, 3, etc.) on Pharmacy claims.				X		2	N
41	Dispense As Written Indicator	An indicator specifying why the product dispensed was selected by the pharmacist and should be entered in a 2 digit format with leading zero: 00 = No DAW 01 = Physician DAW 02 = Patient DAW 03 = Pharmacist DAW 04 = Generic Not In Stock				X		2	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		05 = Brand Dispensed as Generic 06 = Override 07 = Brand Mandated by Law 08 = No Generic Available 09 = Other							
42	Dental Quadrant	One of the four equal sections into which the dental arches can be divided; begins at the midline of the arch and extends distally to the last tooth. 1 = Upper Right 2 = Upper Left 3 = Lower Left 4 = Lower Right					X	1	N
43	Tooth Number	The number or letter assigned to a tooth for identifications purposes as specified by the American Dental Association. A - T (for primary teeth) 1 - 32 (for secondary teeth)					X	2	C
44	Tooth Surface	The tooth surface on which the service was performed: M = Mesial D = Distal O = Occlusal L = Lingual I = Incisal F = Facial B = Buccal A = All 7 surfaces This field can list up to six values. When multiple surfaces are involved, please list the value for each surface without punctuation between values. For example, work on the mesial, occlusal, and lingual surfaces should be listed as "MOL "(three spaces following the third value).					X	6	C
45	Paid Date	For encounter records, the date on which the record was processed. For services performed on a fee-for-service basis, the date on which the claim was paid. The format is YYYYMMDD.	X	X	X	X	X	8	D/YYYYMMDD
46	Service Class	BH Vendor Specific field	X	X	X	X	X	23	C

Provider Data

#	Field Name	Definition/Description	H	P	L	R		Length	Data Type
47	PCP Provider ID	A unique identifier for the Primary Care Physician selected by the patient as of the date of service. ***See discussion in the Data Element Clarifications section.***	X	X	X		X	15	C
48	PCP Provider ID Type	A code identifying the type of ID provided in PCP Provider ID above. For example, *6 = Internal ID (Plan Specific)*	X	X	X		X	1	N
49	PCC Internal Provider ID	PCC Internal ID	X	X	X	X	X	15	C
50	Servicing Provider ID	A unique identifier for the provider performing the service. ***See discussion in the Data Element Clarifications section.***	X	X	X	X	X	15	C
51	Servicing Provider ID Type	A code identifying the type of ID provided in Servicing Provider ID above. For example, *6 = Internal ID (Plan Specific)* *9 = NAPB Number (for pharmacy claims only)*	X	X	X	X	X	1	N
52	Referring Provider ID	A unique identifier for the provider. ***See discussion in the Data Element Clarifications section.***	X	X	X	X	X	15	C
53	Referring Provider ID Type	A code identifying the type of ID provided in Referring Provider ID above. For example, 1 = NPI *6 = Internal ID (Plan Specific)* *8 = DEA Number (for pharmacy claims only)*	X	X	X	X	X	1	N

#	Field Name	Definition/Description	H	P	L	R		Length	Data Type
54	Servicing Provider Class	A code indicating the class for this provider: 1 = Primary Care Provider 2 = In plan provider, non PCP 3 = Out of plan provider *Note*: This code relates to the class of the provider and a PCP does not necessarily indicate the recipient has selected or assigned PCP. PCP class should be assigned only to those physicians whom the plan considers to be a participating PCP.	X	X	X	X	X	1	C
55	Servicing Provider Type	A code indicating the type of provider rendering the service represented by this encounter or claim. (Use Servicing Provider Type values, see Table G)	X	X	X	X	X	3	N
56	Servicing Provider Specialty	The specialty code of the servicing provider. (Use CMS 1500 standard, see Table H)	X	X	X		X	3	C
57	Servicing Provider ZIP Code	The servicing provider's ZIP code. The ZIP code where the service occurred is preferred.	X	X	X	X	X	5	N
58	Billing Provider ID	A unique identifier for the provider billing for the service.	X	X	X	X	X	15	C
59	Authorization Type	BH Vendor Specific field	X	X	X	X	X	25	C

Financial Data

Most of the fields below apply to services for which reimbursement is made on a fee-for-service basis. For capitated services, the record should include fee-for-service equivalent information when available. Line item amounts are required for these fields.

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
60	Billed Charge	The amount the provider billed for the service.	X	X	X	X	X	9	SN
61	Gross Payment Amount	The amount that the provider was paid in total by all sources for this service. *NOTE: This field should include any withhold amount, if applicable.*						9	SN

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
62	TPL Amount	Any amount of third party liability paid by another medical coverage carrier for this service. If the TPL amount is available only at the summary level, it must be recorded on a special line on the claim, which will have a record indicator value of 0. ***See discussion under Dollar Amounts in the Data Elements Clarification Section.***	X	X	X	X	X	9	SN
63	Medicare Amount	Any amount paid by Medicare for this service.	X	X	X	X	X	9	SN
64	Copay/ Coinsurance	Any co-payment amount the member paid for this service.	X	X	X	X	X	9	SN
65	Deductible	Any deductible amount the member paid for this service.	X	X	X	X	X	9	SN
66	Ingredient Cost	The cost of the ingredients included in the prescription.				X		9	SN
67	Dispensing Fee	The dispensing fee charged for filling the prescription.				X		9	SN
68	Net Payment	The amount the Medicaid MCE paid for this service. (Should equal Eligible Charges less COB, Medicare, Copay/Coinsurance, and Deductible.)	X	X	X	X	X	9	SN
69	Withhold Amount	Any amount withheld from fee-for-service payments to the provider to cover performance guarantees or as incentives.						9	SN
70	Record Type	A code indicating the type of record: O = Original V = Void or Back Out R = Replacement A = Amendment ***See discussion under 'Former Claim Number / Suffix' in the Data Elements Clarification Section***	X	X	X	X	X	1	C
71	Group Number	For non-MHSA MCEs 1 = MCO MassHealth 2 = MCO Commonwealth Care 3 = SCO 5 = CarePlus 6 = One Care (ICO) 7 = ACO-A 8 = ACO-B 9 = ACO-C						25	C

Medicaid Program-Specific Data

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
72	DRG	The DRG code used to pay for an inpatient confinement and should always be submitted in 3- digit format. One and two digit codes should be completed with leading zeros to comply. For example: a. DRG code '1' should be submitted as '001'; b. DRG code '25' should be submitted as '025'; c. DRG code '301' should be submitted as '301'. ***See discussion in the Data Element Clarifications section***.	X		X			3	C
73	EPSDT Indicator	A flag that indicates those services which are related to EPSDT: 1 = EPSDT Screen 2 = EPSDT Treatment 3 = EPSDT Referral						1	N
74	Family Planning Indicator	A flag that indicates whether or not this service involved family planning services, which may be matched by CMS at a higher rate: 1 = Family planning services provided 2 = Abortion services provided 3 = Sterilization services provided 4 = No family planning services provided (see Table I)						1	C
75	MSS/IS	*Please leave this field blank, it will be further defined at a later date.* A flag that indicates services related to MSS/IS: 1 = Maternal Support Services 2 = Infant Support Services						1	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
76	New Member ID	The ***"Active" Medicaid*** identification number assigned to the individual. This number is assigned by MassHealth and may change.	X	X	X	X	X	25	C

Other Fields

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
77	Former Claim Number	If this is not an Original claim [Record Type = 'O'], then the previous claim number that this claim is replacing/voiding. ***See discussion under <u>Former Claim Number / Suffix</u> in the Data Elements Clarification Section***	X	X	X	X	X	15	C
78	Former Claim Suffix	If this is not an Original claim [Record Type = 'O'], then the previous claim suffix that this claim is replacing/voiding. ***See discussion under <u>Former Claim Number / Suffix</u> in the Data Elements Clarification Section***	X	X	X	X	X	4	C
79	Record Creation Date	The date on which the record was created. ***See discussion under <u>Record Creation Date</u> in the Data Elements Clarification Section.***	X	X	X	X	X	8	D
80	Service Category	Service groupings from financial reports like 4B (see Table I)	X	X	X	X	X	3	C
81	Prescribing Prov. ID	Federal Tax ID, UPIN, or other State assigned provider ID for the prescribing provider on the Pharmacy claim.				X		15	C
82	Date Script Written	Date prescribing provider issued the prescription.				X		8	D/YYYYMMDD
83	Compound Indicator	Indicates that the prescription was a compounded drug. 1 = Yes 2 = No				X		1	C
84	Rebate Indicator	PBM received rebate for drug dispensed. 1 = Yes 2 = No				X		1	c
85	Admitting Diagnosis	Diagnosis upon admission. May be different from principal diagnosis. Should not be External Injury codes. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
86	Allowable Amount	Amount allowed under the Health Plan formulary.	X	X	X	X	X	9	N
87	Attending Prov. ID	Provider ID of the provider who attended at facility. Federal Tax ID, UPIN, or other State assigned provider ID.	X					15	C
88	Non-covered Days	Days not covered by Health Plan.	X		X			3	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
89	External Injury Diagnosis 1	If there is an External Injury Diagnosis code 1 (ICD E-Code) present on the claim, it should be submitted in this field. See above for format. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C
90	Claim Received Date	Date claim received by Health Plan, if processed by a PBM.				X		8	D/YYYYMMDD
91	Frequency	The third digit of the UB92 Bill Classification field.	X		X			1	C
92	PCC Internal Provider ID_Type	A code identifying the type of ID provided in PCC Internal Provider ID in field #49 above: *Example:* *6 = Internal ID (Plan Specific)* 8 = DEA Number 9 = NABP Number 1 = NPI	X	X	X	X	X	1	N
93	Billing Provider ID _Type	A code identifying the type of ID provided in Billing Provider ID above. For example, *6 = Internal ID (Plan Specific)* 9 = NABP Number *(for pharmacy claims only)*	X	X	X	X	X	1	N
94	Prescribing Prov. ID _Type	A code identifying the type of ID provided in Prescribing Provider ID above. For example, 1 = NPI *6 = Internal ID (Plan Specific)* *8 = DEA Number*				X		1	N
95	Attending Prov. ID _Type	A code identifying the type of ID provided in Attending Prov. ID above. For example, *6 = Internal ID (Plan Specific)*	X					1	N
96	Admission Time	For inpatient facility services, the time the recipient was admitted to the facility. If not an inpatient facility, the value should be missing. This field ***must*** be in HH24MI format. For example, 10:30AM would be 1030 and 10:30PM would be 2230.	X		X			4	N/HH24MI
97	Discharge Time	For inpatient facility services, the time the recipient was discharged from the facility. If not an inpatient facility, the value should be missing. This field ***must*** be in HH24MI format. For example, 10:30AM would be 1030 and 10:30PM would be 2230.	X		X			4	N/HH24MI
98	Diagnosis 6	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
99	Diagnosis 7	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
100	Diagnosis 8	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
101	Diagnosis 9	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
102	Diagnosis 10	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
103	Surgical Procedure code 1	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
104	Surgical Procedure code 2	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
105	Surgical Procedure code 3	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
106	Surgical Procedure code 4	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
107	Surgical Procedure code 5	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
108	Surgical Procedure code 6	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
109	Surgical Procedure code 7	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
110	Surgical Procedure code 8	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
111	Surgical Procedure code 9	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
112	Employment	Is the patient's condition related to Employment Y N	X	X	X	X	X	1	C
113	Auto Accident	Is the patient's condition related to an Auto Accident Y N	X	X	X	X	X	1	C
114	Other Accident	Is the patient's condition related to Other Accident Y N	X	X	X	X	X	1	C
115	Total Charges	This field represents the total charges, covered, and uncovered related to the current billing period.	X	X	X	X	X	9	N
116	Non Covered charges	This field represents the uncovered charges by the payer related to the revenue code. This is the amount, if any, that is not covered by the primary payer for this service.	X	X	X	X	X	9	N
117	Coinsurance	Any coinsurance amount the member paid for this service.	X	X	X	X	X	9	N
118	Void Reason Code	The reason the claim line was voided 1 TPL 2 accident recovery 3 provider audit recoveries 4 Other						1	C
119	DRG Description	Description of DRG Code	X		X			132	C
120	DRG Type	*Values:* 1=Medicare CMS-DRG 2=Medicare MS-DRG 3=Refined DRGs (R-DRG) 4=All Patient DRGs (AP-DRG) 5=Severity DRGs (S-DRG) 6=All Patient, Severity-Adjusted DRGs (APS-DRG) 7=All Patient Refined DRGs (APR-DRG) 8=International-Refined DRGs (IR-DRG) 9=Other ***Please use the accurate and specific DRG type and avoid using the value "Other". Please communicate to MassHealth any DRG types you are using that are missing from the above list***	X		X			1	C
121	DRG Version	DRG Version number associated with DRG type	X		X			3	C/ No decimal points (26.1 must be entered as 261)

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
122	DRG Severity of Illness Level	A code that describes the Severity of the claim with the assigned DRG: Valid values are: 1 = minor 2 = moderate 3 = major 4 = extreme ***Associated with DRG Type=APR-DRG (DRT Type =7) or any other DRG that has these fields***	X		X			1	C
123	DRG Risk of Mortality Level	A code that describes the Mortality of the patient with the assigned DRG code. Valid values are: 1 = minor 2 = moderate 3 = major 4 = extreme ***Associated with DRG Type=APR-DRG (DRT Type =7) or any other DRG that has these fields.***	X		X			1	C
124	Patient Pay Amount	Patient paid amount for nursing facility stays and hospitals	X		X			9	SN
125	Patient Reason for Visit Diagnosis 1	ICD diagnosis code describing the patient's (or patient representative's) stated reason for seeking care at the time of outpatient (ER) visit ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
126	Patient Reason for Visit Diagnosis 2	ICD diagnosis code describing the patient's (or patient representative's) stated reason for seeking care at the time of outpatient (ER) visit ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
127	Patient Reason for Visit Diagnosis 3	ICD diagnosis code describing the patient's (or patient representative's) stated reason for seeking care at the time of outpatient (ER) visit ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
128	Present on Admission (POA) 1	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
129	Present on Admission (POA) 2	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
130	Present on Admission (POA) 3	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
131	Present on Admission (POA) 4	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
132	Present on Admission (POA) 5	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
133	Present on Admission (POA) 6	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
134	Present on Admission (POA) 7	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
135	Present on Admission (POA) 8	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
136	Present on Admission (POA) 9	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
137	Present on Admission (POA) 10	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
138	Diagnosis 11	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
139	Present on Admission (POA) 11	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
140	Diagnosis 12	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X			7	C/No decimal points
141	Present on Admission (POA) 12	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
142	Diagnosis 13	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
143	Present on Admission (POA) 13	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
144	Diagnosis 14	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
145	Present on Admission (POA) 14	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
146	Diagnosis 15	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
147	Present on Admission (POA) 15	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
148	Diagnosis 16	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
149	Present on Admission (POA) 16	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
150	Diagnosis 17	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
151	Present on Admission (POA) 17	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
152	Diagnosis 18	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
153	Present on Admission (POA) 18	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
154	Diagnosis 19	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
155	Present on Admission (POA) 19	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
156	Diagnosis 20	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
157	Present on Admission (POA) 20	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
158	Diagnosis 21	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
159	Present on Admission (POA) 21	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
160	Diagnosis 22	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
161	Present on Admission (POA) 22	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
162	Diagnosis 23	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
163	Present on Admission (POA) 23	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
164	Diagnosis 24	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
165	Present on Admission (POA) 24	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
166	Diagnosis 25	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
167	Present on Admission (POA) 25	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
168	Diagnosis 26	The ICD diagnosis code. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
169	Present on Admission (POA) 26	This indicator clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
170	Present on Admission (POA) EI 1	This indicator is associated with External Injury Diagnosis 1 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
171	External Injury Diagnosis 2	If there is an External Injury Diagnosis code 2 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
172	Present on Admission (POA) EI 2	This indicator is associated with External Injury Diagnosis 2 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
173	External Injury Diagnosis 3	If there is an External Injury Diagnosis code 3 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
174	Present on Admission (POA) EI 3	This indicator is associated with External Injury Diagnosis 3 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
175	External Injury Diagnosis 4	If there is an External Injury Diagnosis code 4 (ICD- E-Code) present on the claim, it should be submitted in this field.	X		X			7	C/No decimal points

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							
176	Present on Admission (POA) EI 4	This indicator is associated with External Injury Diagnosis 4 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
177	External Injury Diagnosis 5	If there is an External Injury Diagnosis code 5 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
178	Present on Admission (POA) EI 5	This indicator is associated with External Injury Diagnosis 5 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
179	External Injury Diagnosis 6	If there is an External Injury Diagnosis code 6 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
180	Present on Admission (POA) EI 6	This indicator is associated with External Injury Diagnosis 6 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
181	External Injury Diagnosis 7	If there is an External Injury Diagnosis code 7 (ICD- E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
182	Present on Admission (POA) EI 7	This indicator is associated with External Injury Diagnosis 7 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
183	External Injury Diagnosis 8	If there is an External Injury Diagnosis code 8 (ICD-E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
184	Present on Admission (POA) EI 8	This indicator is associated with External Injury Diagnosis 8 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
185	External Injury Diagnosis 9	If there is an External Injury Diagnosis code 9 (ICD E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
186	Present on Admission (POA) EI 9	This indicator is associated with External Injury Diagnosis 9 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
187	External Injury Diagnosis 10	If there is an External Injury Diagnosis code 10 (ICD-E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
188	Present on Admission (POA) EI 10	This indicator is associated with External Injury Diagnosis 10 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
189	External Injury Diagnosis 11	If there is an External Injury Diagnosis code 11 (ICD-E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
190	Present on Admission (POA) EI 11	This indicator is associated with External Injury Diagnosis 11 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
191	External Injury Diagnosis 12	If there is an External Injury Diagnosis code 12 (ICD-E-Code) present on the claim, it should be submitted in this field. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X		X			7	C/No decimal points
192	Present on Admission (POA) EI 12	This indicator is associated with External Injury Diagnosis 12 that clarifies if the diagnosis was present at admission. This only applies to UB-04 claims (See Table M for values)	X		X			1	C
193	ICD Version Qualifier	ICD9 or ICD10. The value "ICD9" must be populated on claim records with either ICD-9-CM diagnosis codes or ICD-9-CM procedure codes. The value "ICD10" must be populated on claim records with either ICD-10-CM diagnosis codes or ICD-10-CM procedure codes. One claim record must ***never*** have a combination of ICD9 and ICD10 codes. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X	X	X		X	5	C
194	Procedure Modifier 4	4th procedure code modifier, required if used.	X	X	X		X	2	C
195	Service Category Type	This field describes the Type of Financial reports the service category is based on. The values are: '4B' for MCO Service Categories 'ACO' for ACO Categories 'SCO' for SCO Service Categories						3	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		'ICO' for Care One (ICO) Service Categories							
196	Ambulance Patient Count	AMBULANCE PATIENT COUNT. REQUIRED WHEN MORE THAN ONE PATIENT IS TRANSPORTED IN THE SAME VEHICLE FOR AMBULANCE OR NON-EMERGENCY TRANSPORTATION SERVICES.						3	N
197	Obstetric Unit Anesthesia Count	The number of additional units reported by an anesthesia provider to reflect additional complexity of services.						5	N
198	Prescription Number	Rx Number.				X		15	C
199	Taxonomy Code	This is the Taxonomy code for Servicing Provider identified on the claim. Taxonomy codes are National specialty codes used by providers to indicate their specialty. These codes can be found on the Website of Centers for Medicare & Medicaid Service (CMS)	X	X	X		X	10	C
200	Rate Increase Indicator	Indicates if the provider is eligible to receive the enhanced primary care rate ***for this service***, as specified in the Affordable Care Act – Section 1202 final regulations. 1=Yes 2=No 3=Unknown 4=Not Applicable ***Note:*** **If a service is considered eligible based on the ACA regulations, then the value should be equal to "1" even if the MCE is already paying the provider at the higher rate.**						1	C
201	Bundle Indicator	Indicates if the claim line is part of a bundle. Values: Y=Yes, the claim line is part of a bundle. All bundled lines including the line with the bundled payment should have a value of 'Y' N=No, the claim line is not part of a bundle.						1	C
202	Bundle Claim Number	This is the claim number of the claim line with the bundled payment. ***See discussion in Data Element Clarifications section.***						15	C
203	Bundle Claim Suffix	This the claim suffix of the claim line with the bundled payment. ***See discussion in Data Element Clarifications section.***						4	C
204	Value Code	Code used to relate values to identify data elements necessary to process a UB92 claim. Submit only when the value=54 for Newborn claims	X					2	AN
205	Value Amount	Weight of a newborn in grams. Must be present on all newborn claims when the value code "54"is submitted in Field#204	X					9	N

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
206	Surgical Procedure Code 10	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
207	Surgical Procedure Code 11	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
208	Surgical Procedure Code 12	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
209	Surgical Procedure Code 13	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
210	Surgical Procedure Code 14	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
211	Surgical Procedure Code 15	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
212	Surgical Procedure Code 16	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
213	Surgical Procedure Code 17	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
214	Surgical Procedure Code 18	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
215	Surgical Procedure Code 19	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank.	X					7	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
		See discussion in Data Element Clarifications section, including clarification on ICD-10							
216	Surgical Procedure Code 20	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
217	Surgical Procedure Code 21	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
218	Surgical Procedure Code 22	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
219	Surgical Procedure Code 23	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
220	Surgical Procedure Code 24	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
221	Surgical Procedure Code 25	For surgical revenue codes, the ICD surgical procedure code. If a surgical revenue code is not applicable, the value should be left blank. ***See discussion in Data Element Clarifications section, including clarification on ICD-10***	X					7	C
222	Attending Prov. ID Address Location Code	Code to identify address location of Attending Provider ID in field #87	X					15	C
223	Billing Provider ID Address Location Code	Code to identify address location of Billing Provider ID in field # 58	X	X	X	X	X	15	C
224	Prescribing Prov. ID Address Location Code	Code to identify address location of Prescribing Provider ID Provider ID in field # 81				X		15	C
225	PCP Provider ID Address Location Code	Code to identify address location of PCP Provider ID in field # 47	X	X	X	X	X	15	C
226	Referring Provider ID	Code to identify address location of Referring Provider ID in filed # 52	X	X	X			15	C

#	Field Name	Definition/Description	H	P	L	R	D	Length	Data Type
	Address Location Code								
227	Servicing Provider ID Address Location Code	Code to identify address location of Servicing Provider ID in field # 50	X	X	X	X	X	15	C
228	PCC Provider ID Address Location Code	Code to identify address location of PCC Internal Provider ID in field # 49	X	X	X	X	X	15	C
229	Adjudication Date	The date when the record was adjudicated	X	X	X	X	X	8	D/YYYYMMDD

3. Error Handling Section

The submission will be rejected if:

- The data elements do not meet format and layout requirements
- The metadata file is not to the specifications' requirements
- Org. Code is missing or invalid

Please refer to **2.2 File Submission Requirements** segment for data elements validation/ error/result information.

MH DW will reject records based on the following error codes:

Error Code	Description
1	Incorrect Data Type
2	Invalid Format
3	Missing value
4	Code missing from reference data
5	Invalid Date
72	Claim Number/Suffix in Denied Claims Reason Code file not in Denied Claims file
73	Claim Number/Suffix in Denied Claims file not in Denied Claims Reason Code file
74	Correction to a claim that is not in MH DW

4. Error Reports and Notifications to the Plans

When denied claims files are loaded, three error reports are placed on MCOs SFTP servers:

- Error Denied Claims Summary Report
- Error Denied Claims Details Report
- Error Denial Reference Report

4.1 Error Denied Claims Summary Report Format

Example:

MCO_Denied_Claims_20180716.zip file processed on MM/DD/YYYY (07/18/2018)
Report Name - "err_MCO.2018.07.18.13.41.01.denied_claim_summary.txt"

Field #	Field Name	Frequency	Error Code	Error Description
5	CLAIM NUMBER	25	73	Claim Number/Suffix in Denied_Claims file not in Denied_Claims_Reason_Code file
58	BILLING_PROVIDER_ID	2	3	Missing Value
73	NEW_MEDICAID_ID	3	4	Code missing from reference data

4.2 Error Denied Claims Details Report Format

MCO_Denied_Claims_20180716.zip file processed on MM/DD/YYYY (07/18/2018)
Report Name - "err_MCO.2018.07.18.13.41.02.denied_claim_detail.txt"

The report consists of 14 fields:

1. MCO
2. ORG. Code
3. Entity PIDSL
4. Claim Number
5. Claim Suffix
6. Billing Provider ID
7. Billing Provider ID Type
8. Billing Provider ID Address Location Code
9. Medicaid ID (New Member ID)
10. Adjudication Date
11. Field #
12. Field Name
13. Error Code
14. Error Description

4.3 Error Denial Reason Code Report Format

Example:

MCO_Denied_Claims_20180716.zip file processed on MM/DD/YYYY (07/18/2018)
Report Name - "err_MCO.2018.07.18.13.41.03.rsnm2m.txt"

Error Denied Reason Code Report format repeats the format of the Denied Claims Reason Code file format with two extra columns on the right – "Error Code" and "Error Description"

MCO	CLAIM_NUMBER	CLAIM_FUFFIX	Denial Reason Code	Error Code	Error Description
CAR	5555555555RX	25	DINCORRT	72	Claim Number/Suffix in Denied_Claims_Reason_Code file not in Denied_Claims file

APPENDIX E-1

PROGRAM REPORTING REQUIREMENTS

This Appendix summarizes the programmatic reporting requirements described in the Contract. In accordance with **Section 2.14** of the Contract, the Contractor shall submit the report and corresponding Certification Checklist of all reports/submissions listed in **Appendix E** within the timelines specified herein.

For reports that have a performance target, the Contractor shall complete a narrative that includes the results, an explanation as to how the Contractor met the target or why it did not meet the target, and the steps the Contractor is taking to improve performance going forward.

The Contractor shall provide all reports in the form and format specified by EOHHS and shall participate with EOHHS in the development of detailed specifications for these reports. These specifications shall include benchmarks and targets for all reports, as appropriate. Targets shall be changed to reflect improvement in standards over time.

All exhibits referenced herein pertain to **Appendix E**, unless otherwise noted. Such exhibits set forth the form and format the Contractor shall use for each report. These exhibits shall be provided to the Contractor and may be updated by EOHHS from time to time, without a Contract amendment. EOHHS shall notify the Contractor of any updates to the exhibits.

The Contractor shall prepare and submit to EOHHS the reports described in this Appendix, as well as ad hoc reports that may be requested by EOHHS. General requirements for report submissions, including instructions on formatting and data handling, are set forth in **Section 2.14** of the Contract. In the event of any inconsistency between the descriptions in this Appendix and the provisions in the Contract, the Contract controls.

Reporting Timetables

The Contractor shall provide reports to EOHHS according to the following timetable, unless otherwise specified or approved by EOHHS. Claims-based reports shall allow for a 90-day (three month) Claims lag and report time. If a due date falls on a non-business day, submission shall take place by the next business day. All references to "annual" or "year-to-date" reports or data refer to the Contract Year, unless otherwise specified.

Report Cadence	Reports Due (*by close of business*)
Reportable Adverse Incidents	Use secure e-mail system to send Reportable Adverse Incident reports to EOHHS by 5:00 p.m. (Eastern Time) on the same day that the Contractor receives Reportable Adverse Incident notification by 3:00 p.m. on a business day, in accordance with the established protocol. Submit Reportable Adverse Incident reports to EOHHS by the next business day if the Contractor receives Reportable Adverse Incident notification after 3:00 p.m. or on a non-business day, in accordance with the established protocol, unless otherwise approved by EOHHS.
Daily Deliverables	Deliverables due by close of business/COB on the next business day following the day reported
Weekly Deliverables	Deliverables due by close of business/COB on Fridays
Monthly Deliverables	Deliverables due on a monthly basis, by the last business day of the month, following the month included in the data, unless otherwise specified by EOHHS. Claims-based reports due on the last day of the third month following the month included in the data (*e.g.* January reporting period due last day of April)
Quarterly Deliverables	Deliverables due on a contract year (CY) quarterly basis, by the last business day of the month following the end of each quarter, unless otherwise specified. o CY Quarter 1: January 1 – March 31 o CY Quarter 2: April 1 - June 30 o CY Quarter 3: July 1 – September 30 o CY Quarter 4: October 1 – December 31
Semi-Annual Deliverables	Deliverables due by the last business day of the month following the end of the reporting period, unless otherwise specified. The semi-annual reporting periods are as follows: o January 1 – June 30 o July 1 – December 31
Annual Deliverables	Deliverables due by the last business day of the month following the end of the reporting period (Contract Year: January 1 -- December 31), unless otherwise specified by EOHHS.

Report Cadence	Reports Due (*by close of business*)
Biennial Deliverables	Deliverables due in designated biennial years, by the last business day of the month following the end of the reporting period, unless otherwise specified. Specific years are noted in the report descriptions.
Ad-Hoc Deliverables	Deliverables are due whenever the Contractor has relevant changes or information to report, or upon EOHHS request related to Behavioral Health, Contract Management, Financial, Quality, Pharmacy, and Operations deliverables as applicable.

Filenaming Convention

All reports submitted to EOHHS shall adhere to the following filenaming convention:

1. **File Upload Folders** shall include the reporting year, reporting cadence, and reporting period. For example:
    - Quarterly: CY24_Quarterly-1, CY24_Quarterly-2, etc.
    - Monthly: CY24_Monthly_01-Jan, CY24_Monthly_02-Feb, etc.
    - CY24_Annual, CY24_Semi-Annual
2. **Filenames** shall be identical to the report titles in this appendix, inclusive of the Contract Exhibit numbers. For example:
    - BH-27_ Provider-Concerns-Report
    - PI-05_ Summary-of-Provider-Overpayments
3. **Sub-Deliverables** assigned a letter/number designation shall follow the filename to indicate the specific sub-deliverable. If sub-deliverables include a title, the title should be included following an underscore. For example:
    - BH-18_BH-Provider-Network-Access-and-Availability_A
    - Quarterly-MCPAP-Program-Utilization-stratified-by-Month_A_MCPAP-Activity-3Yr-Trending
4. **Character Usage:** For the purpose of data storage, spaces shall not be used in filenames. Underscores shall be instead of spaces to separate data elements, while dashes shall be used in place of spaces within report filenames and sub-deliverables.

By adhering to this filenaming convention, the Contractor will ensure consistent and efficient organization of report submissions.

*** Adverse Incident Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-01	**BH-01 Behavioral Health Reportable Adverse Incidents and Roster of Reportable Adverse Incidents – Daily Incident Delivery Report** Report of Reportable Adverse Incidents that comes to the attention of the Contractor.	Same Day
BH-02	**BH-02 Behavioral Health Adverse Incident Summary Report** Summary report of Reportable Adverse Incidents. Incidents are categorized by sentinel, major, moderate, and minimal. Report includes graphs and an analysis of the incidents along with action items/next steps.	Annual

*** ABA Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
ABA-01	**ABA-01 Behavioral Health Clinical Operations and Acute Service Authorization, Diversions, Modification and Denial Report (ABA)** Summary report, including Clinical Ops Data and Graphs, on ABA authorizations, diversions, modifications, and service denials.	Semi-Annual

*** BHUC Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BHUC-01	**BHUC-01 Behavioral health urgent care – ad hoc reports** Provide any Behavioral Health Urgent Care ad hoc reports further specified by EOHHS.	Ad-Hoc

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BHUC-02	**BHUC-02 Behavioral Health Urgent Care – Quarterly** A summary, stratified by month, of BHUC provider-reported information as described in contract Section 2.6.D.10.a.6.	Quarterly

<u>* CANS Reports</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-14	**BH-14 CANS Compliance:** CANS Compliance. This report is required when CANS data is made available through the Virtual Gateway *BH-14 CANS Compliance_by_LOC:* Summary of members receiving outpatient/ICC/IHT in time frame, with CANS assessment marked with appropriate LOC, and compliance rate and summary of members receiving discharges for CBAT and inpatient, number of discharges with CANS assessment with appropriate LOC, and compliance	Quarterly

<u>* Care Coordination Reports</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CC-10	**CC-10 Care Management – PBCM Report** The Contractor shall calculate and report on the number of Participants in Practice Based Care Management on a monthly basis.	Monthly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CC-11	**CC-11 Care Management Report** Report of all Care Management, Integrated Care Management and Practice-Based Care Management, stratified by month, which includes but is not limited to the requirements found **in Section 2.5.A-H** in a form and format to be determined by EOHHS and the Contractor. 1. *ICMP PBCM:* Excel sheet detailing count and percentage 2. *ICMP PBCM Narrative:* Details engagement, disenrollment, high-risk identification, noticeable changes, opportunities for improvement, interventions/next steps for ICMP and PBCM	Quarterly

<u>* CBHC Reports</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CBHC-01	**CBHC-01 CBHC E-Reporting** ** Due on the 15th of the month following the month being reported on (I.E. Apr 15th for March data)* Site-Reported E-Reporting provides an overview of CBHCs ability to meet access standard thresholds for Core Clinic Services (MOUD Initiation Appointment, Urgent Appointment, Urgent Pyschopharm, and Non-Urgent Appointment) and Mobile Crisis Intervention Services for adult and youth (Overall, Overnight, & In-Person Access Standards)	Monthly
CBHC-02	**CBHC-02 Police Drop-off and Direct Admits** The total count of weekly police drop-offs at CBHCs, by site and region, as well as total count of direct admissions from CBHCs to an inpatient psychiatric unit.	Monthly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CBHC-03	**CBHC-03 CCS Utilization** ** Due on the 15th of the month following the month being reported on (I.E. Apr 15th for March data)* Report detailing the number of available beds, by week, and the daily census (occupancy rates) for CBHC Adult Community Crisis Stabilization (ACCS) and Youth Community Crisis Stabilization (YCCS) programs.	Monthly
CBHC-04	**CBHC-04 CBHC Staffing Report** ** Due on the 15th of the month following the month being reported on (I.E. Apr 15th for March data)* Assessment of vacant positions which CBHCs are hiring for, including the role (i.e. nursing, prescribers, clinicians, supervisors, peer support specialists, etc), the service type (Core, MCI, CCS), the shift, and the number of FTE's needed.	Quarterly
CBHC-05	**CBHC-05 Secret Shopper Summary** ** Due on the 15th of the month following the month being reported on (I.E. Apr 15th for March data)* Overview of Secret Shopper calls completed within the quarter for CBHC Core Clinic and Mobile Crisis Intervention services. The report includes quantitative and qualitative experience ratings, as well as narratives and descriptions of the calls completed.	Quarterly

<u>* CBHI & CSA Reports</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CBHI-01	**CBHI-01 Authorization Reports for CBHI Services** Summary report of authorizations units of services requested, approved and denied for CBHI Services.	Ad-Hoc

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CBHI-02	**CBHI-02 CBHI access reporting** Ensure that the Behavioral Health Service Access System is updated at least once a week for CBHI Services (ICC, FIT, IHBS, TM, and IHT) to show access and availability. CBHI Service reporting must be available to the public on the system.	Weekly
CBHI-03-A	**CBHI-03-A CBHI Services Provider Monitoring Reports** Provider access reports: Aggregated by Region and by service - including In-Home Therapy, Therapeutic Mentoring and In-Home Behavioral Services. *MABH Access (Availability and Waitlist Reports):* 1. FST Self-reported provider-level data 2. IHBS Self-reported provider-level data 3. IHT Self-reported provider-level data 4. TM Self-reported provider-level data *5. Provider Detail Report:* Summary of IHT/IHBS/FST/TM providers by region	Monthly
CBHI-03-B	**CBHI-03-B CBHI Services Provider Monitoring Reports** Provider access reports: Provider-specific data on capacity, access and wait times for In-Home Therapy, Therapeutic Mentoring and In-Home Behavioral Services. 1. *IHT/TM/IHBS Monthly Provider Report*: Self-reported by providers. Provider-level data on availability of services inclusive of data on total capacity, slots, available and total youth waiting. 2. *IHT/TM/IHBS Monthly Provider Report Addendum* 3. *Waitlist F/U Report:* Provider detail on the follow-up providers have with clients on the waiting list. Contractor gathers this detail through phone calls to providers and manually produces the report.	Monthly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CBHI-03-C	**CBHI-03-C CBHI Services Provider Monitoring Reports** CSA Monthly Provider-level report and CSA waitlist follow-up report, Provider-specific. 1. *CSA Monthly Provider Report:* Self-reported by CSAs. Includes data on members being served, total # members waiting, waiting by # days, average length of time from request to start of service 2. *CSA Waitlist Follow-up Report:* Self-reported by CSAs. Includes provider-level data on youth waiting for service for CSAs with waitlists inclusive of total # of youth waiting and youth who started the service at the time of the follow-up call from Contractor.	Monthly
CBHI-04	**CBHI-04 MBHP IHD Discharge reports** Youth discharged from IHD with disposition.	Monthly
CSA-01	**CSA-01 CSA Enrollment data** Admits and Discharges to Intensive Care Coordination for the purposes of creating a flag in EVS to avoid duplicate TCM services enrollments (e.g. CARES, CP, etc.)	Weekly
CSA-02	**CSA-02 CSA Reported and Aggregated Data (Monthly)** CSA-reported data on referrals, discharges, enrollment and staffing, as described in CSA Operations Manual. 1. *IHT Response Time:* Average time to first IHT appointment. 2. *Monthly Bed and Boarding Report:* A chart which outlines the number of youth involved with Contractor awaiting inpatient hospital placement and the number of available inpatient beds.	Monthly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CSA-03	**CSA-03 CSA reported and aggregated data (Quarterly)** 1. *IHT Key Indicator:* Includes the percentage of enrollees who use TT&S, percentage of enrollees who receive services from a MA clinician, percentage of enrollees using other LOC, and average units billed per month 2. *IHBS Key Indicator:* Includes the total youths enrolled by age group, enrollment by Hub type, number of enrollees receiving services by either a MA or BA-level clinician. Point-in-time data. 3. *TM Key Indicator:* Includes the total youth enrolled by age group and enrollment by Hub type. There are three different versions of the report based on provider enrollment size.	Quarterly
CSA-04	**CSA-04 CSA reported and aggregated data (Semi-Annual)** *Wraparound Fidelity Index:* Set of four interviews that measure the nature of the wraparound process that an individual family receives to measure fidelity to principles.	Semi-Annual

<u>* Contract Management Reports</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CM-15-A	**CM-15-A Notification of Scheduled Board of Hearing Cases** Notification of Board of Hearing Cases (Notification: Same Day)	Ad-Hoc
BH-17	**BH-17 Grievance and Internal Appeals Report** A report on the number of Grievances and Internal Appeals, including the type of Grievance or Internal Appeal, type of resolution, and the timeframe for resolution. Includes analysis and next steps.	Monthly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-27	**BH-27 Provider Quality Concerns Report** Report of all concerns reported by Network Providers to the vendor or directly to EOHHS; stratified by PCC Network Providers and BH Network Providers. "Provider Concern Report Month YYYY": Includes a summary about: whether the concern regards Contractor, the provider, or MassHealth; reason category and subcategory (quality of service, quality of care, access to care, billing/finance, or other issues); concern resolution type; an analysis of concerns; and management actions/next steps	Monthly
CM-12	**CM-12 Claims Processing Report** Behavioral Health Claims report that includes: • Total Current Open Claims Inventory • Number of claims submitted last month • Percentage of claims paid / denied / pended • Percentage of pended claims by age: 0-30 / 31-59 / 60+ days • Top 3 claims denial and pend reason codes • If contract deliverables for claims processing were not met, a written analysis explain the cause should be included	Monthly
BH-19	**BH-19 Telephone Statistics** Report including a separate section for clinical calls and Provider and Covered Individual services calls that includes the number of calls, received, answered and abandoned, as well as the measures of Contract performance standards on calls answered within 30 seconds, and average speed of answer.	Quarterly
CM-15-B	**CM-15-B BOH Appeals Report** A report that includes but is not limited to, for each category of Adverse Action, the number, nature, resolution and time frame for resolution of BOH Appeals, stratified by level of Appeal, Region, and Level of Care.	Annual

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-18	**BH-18 BH Provider Network Access and Availability Reports:** Reports on the list of behavioral health providers in the Contractors network across the state and on the ability of MBHP to comply with the time and distance standards set forth in Section 2.9.C. The BH-18 reports shall include the below information in a form and format specified by EOHHS. a. An analysis of the Contractors BH Network Geographic Access b. Lists of contracted providers and a summary of significant changes to the provider network c. A summary of appointment availability d. A summary of the use of out-of-network providers e. For each of the contracted service areas (as specified by EOHHS): 1. A summary of the methods used to collect and examine network adequacy data 2. An analysis and summary of the reports 3. A summary of the management actions or next steps that will be taken based on the findings of the analysis	Annual
CM-25	**CM-25 Material Subcontractors** Submit annually to EOHHS a list of all Material Subcontractors. Such annual report shall include notification if any of its Material Subcontractors are certified Minority Business Enterprises. The Contractor shall submit an updated list at least 30 days in advance of any changes to the list or as otherwise directed by EOHHS	Annual

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
CM-26	**CM-26 Coordination of Benefits/Third-Party Liability Report** • Third-party health insurance cost avoidance Claims amount. • Third-party health insurance total recovery savings. 1. *Coordination of Benefits:* Contractor's actual savings via Third Party Insurance Benefit Coordination and the actual cost of avoidance via the denial of claims 2. *353_ORA:* Historical list of savings 3. *4669_ORA:* Quarterly report of total claim lines and total claimed 4. *5630_ORA:* Monthly payment timeliness report including total claims, average days for payment, SD days for payment, and #/% claims paid within 30 days	Semi-Annual
CM-34	**CM-34 Network Management Strategies Report** A summary description of the Contractor's network management strategies and activities related to access, appropriateness of care, continuity of care, cost efficiency, and treatment outcomes; including an analysis of the effectiveness of the Contractor's strategies and activities; and the Contractor's plans for implementing new strategies or activities.	Annual

*** CSP Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-24	**BH-24 Community Support Program Reports - HI** Provide annually the Community Support Program – Homeless Individuals (CSP-HI) report as specified by EOHHS.	Annual
BH-25	**BH-25 Community Support Program Reports - JI** Provide annually the Community Support Program – Homeless Individuals (CSP-JI) report as specified by EOHHS.	Quarterly
BH-26	**BH-26 Community Support Program – TPP** Provide annually the Community Support Program – Tenancy Preservation Program (CSP-TPP) report as specified by EOHHS.	Annual

*** Incentives Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
INC-01	**INC-01 Pay for Performance Incentive Reporting** Report on selected Pay-for-Performance measures, as defined in **Appendix G**.	Annual

*** Inpatient Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-03	**BH-03 - Behavioral Health Readmission Rates Report** ** This annual report is due at the end of the Fiscal Year (Due in July)* Report of the number and rate of readmissions to 24-hour Level of Care within 7, 30, 60 and 90 days of discharge from a 24-hour Level of Care setting, stratified by type of service, DMH involvement, PCC Plan enrollment, and age.	Annual
BH-05	**BH-05 Covered Individuals on Administratively Necessary Days (AND) Status** Covered Individuals on Administratively Necessary Days (AND) Status.	Daily
BH-13	**BH-13 Behavioral Health Clinical Operations/Inpatient and Acute Service Authorization, Diversions, Modification and Denial Report** Summary report on authorizations, diversions, modifications, and service denials of mental health inpatient services and substance use disorder acute services. In addition, summary report of number of Covered Individuals: • enrolled in PACT; • enrolled in PACT who assessed psychiatric inpatient level of care; • enrolled in PACT who assessed Crisis Stabilization Services; and • enrolled in PACT who assessed Community Crisis Stabilization.	Quarterly

*** MCPAP Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
MCPAP-01	**MCPAP-01 EC - Massachusetts Child Psychiatry Access Project Report** Report of Early Childhood BH Encounters by MCPAP Providers statewide stratified by months and year to date **(Section 2.6.D.2.f-j)**	Quarterly
MCPAP-02	**MCPAP-02 Quarterly MCPAP Program Utilization, stratified by Month** Other program utilization data elements that may be identified by EOHHS and DPH. 1. *MCPAP Activity 3Yr Trending:* Includes aggregate counts, activity by team (BH advocacy, face-to-face, phone, practice education, and resource-referral), and activity for ASDID for MCPAP team. 2. *MCPAP Utilization Report with ASD:* Includes utilization summaries by region, by region and practice, and by practice and provider type for ASD.	Quarterly
MCPAP-03	**MCPAP-03 MCPAP Average Encounter** Average number of encounters per unduplicated Covered Individuals by month, by ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team.	Quarterly
MCPAP-04	**MCPAP-04 MCPAP Quarterly Encounter** For each ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team: number of encounters by type of encounter by month, diagnosis, reason for contact, and insurance status of the child. For ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team, must include location of individual (e.g., home, school, emergency department, community-based behavioral health provider), the email address of the individual/ family, name of the AMCI/YMCI Team or ED seeking consult, and patient demographic data including race, ethnicity, and primary language. Quarterly and annual reports should show quarterly trends in number of encounters by type of encounter for three years.	Quarterly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
MCPAP-05	**MCPAP-05 MCPAP Quarterly Unduplicated Count** For each ASD-ID for MCPAP Team (i.e., Boston North, Boston South, and Central/West), Site/Institution, and statewide ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team: unduplicated monthly count of Covered Individuals served, by type of encounter and insurance status of the Covered Individual. Quarterly and annual reports should show quarterly trends in number of Covered Individuals served for three years.	Quarterly
MCPAP-06	**MCPAP-06 MCPAP Quarterly Response Time** For each ASD-ID Behavioral Team and ASD-ID Statewide Physician Consult Team, percentage of providers that receive advice within 30 minutes of their contact (for those providers that do not request call back later than 30 minutes) stratified by month.	Quarterly
MCPAP-07	**MCPAP-07 MCPAP and ASD-ID Appointment Availability** For each ASD-ID team, the wait time for the first and next available appointments for face-to-face assessment with a MCPAP psychiatrist or with a MCPAP Behavioral Health clinician, stratified by month. If an ASD-ID team fails to meet one or both of the wait time standards described in **Section 2.6.D.2.e.** for three consecutive months, the Contractor shall submit a report detailing the reasons why they are unable to meet the standards. The report must describe the number of face-to-face visits completed by each institution, reason for assessments, and the age, gender, diagnoses, and insurance coverage of children receiving the assessments.	Quarterly
MCPAP-08	**MCPAP-08 EC-MCPAP and ASD-ID Outreach and Training** The number of outreach and training activities for MCPAP providers including: 1. Number and type of outreach and training activities conducted by ASD-ID for AMCI/YMCI teams and EDs as in **Section 2.6.D.2.f.6**. Number, if known, of individuals reached. Number of public awareness activities conducted by ASD-ID for families of individuals with ASD/IDD, pediatric providers, staff at Autism Support Centers, and parent resource groups, or other stakeholders on topics described in **Section 2.6.D.2.f.7.** Number, if known, of individuals reached. 2. Number and type of outreach and training activities conducted for EC-MCPAP	Quarterly

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
MCPAP-09	**MCPAP-09 MCPAP Teams** Composition of MCPAP Teams for ASD-ID for MCPAP including staffing and their FTEs (Full Time Equivalents). "FTE YYYY"	Annual
MCPAP-10	**MCPAP-10 MCPAP Annual Encounters** For ASD-ID for MCPAP Behavioral Team and Statewide Team: number of encounters by type of encounter, diagnosis, reason for contact, and insurance status of the child. For ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team, must include location of individual (e.g., home, school, emergency department, community-based behavioral health provider), the email address of the individual/ family, name of the AMCI/YMCI Team or ED seeking consult, and patient demographic data including race, ethnicity, and primary language. Quarterly and annual reports should show quarterly trends in number of encounters by type of encounter for three years. "MCPAP Encounter Report"	Annual
MCPAP-11	**MCPAP-11 MCPAP Annual Unduplicated Count** For ASD-ID for MCPAP Behavioral Team and Statewide Team: unduplicated count of Covered Individuals served, by type of encounter and insurance status of the Covered Individual. Quarterly and annual reports should show quarterly trends in number of Covered Individuals served for three years. 1. *MCPAP FYXXQX Insurance Report* 2. *MCPAP Unduplicated Mbrs 3Yr Trending:* Chart showing unduplicated members served overall and by team	Annual
MCPAP-12	**MCPAP-12 ASD-ID for MCPAP Children Consultation** For each ASD-ID for MCPAP Behavioral Team and Statewide Physician Consult Team, the number of children and young adults whom AMCI/YMCI teams or EDs request consultation for at least two or more times during the contract year (i.e., episodes of care). This episode report must describe the demographics of the patient (e.g., age, gender, diagnoses, insurance, race, ethnicity, primary language, etc.), type and average number of encounters provided to AMCI/YMCI or ED and family (if relevant), reasons for consultation, type of intervention advised/ provided, and outcome of consultation.	Annual

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
MCPAP-13	**MCPAP-13 MCPAP Annual Provider Experience Survey** Results of annual Provider Experience Surveys for ASD-ID for MCPAP.	Annual

*** MCSTAP Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
MCSTAP-01	**MCSTAP-01 Massachusetts Consultation Services for the Treatment of Addiction and Pain (MCSTAP)** Quarterly summary (stratified by months and year to date) including Total Consultation, % of Substance Use Disorder (SUD), % of Chronic Pain, % of SUD and Chronic Pain, % of Chronic Pain and Mental Health, and SUD and Mental Health.	Quarterly

*** Medical Records Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BH-11	**BH-11 Medical Records Review Report** Report that includes requirements found in **Section 2.14.K** as will be developed by EOHHS and Contractor.	Annual

*** PCC Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
PCC-01	**PCC-01 Additional Reports and Reporting Activities (for PCC Plan)** The Contractor shall produce additional PMSS reports, including but not limited to analysis of trends identified from PMSS data, data and analytics on population health management, and other supplemental and management reports that support quality and integration activities as negotiated by the parties.	Ad-Hoc
PCC-02	**PCC-02 PCC Clinical Advisory Committee** The PCC Clinical Advisory Committee shall report on minutes to the meeting and provide follow-up on action items established.	Ad-Hoc
PCC-03	**PCC-03 PCC Plan Support Services Report** Report of PCC Plan Support deliverables. "Month YYYY Plan Support Services Report": Comprehensive summary of the activities related to the PCC Plan Support Services Program including site visits, internal and external meetings, related data	Monthly
PCC-04	**PCC-04 PCC Plan Management Support Services Report** Summary report of PMSS activities and integration efforts for the previous Contract Year that includes efforts to enhance integration and PCC health delivery, goals, and results as required by but not limited to **Section 2.19.A.**	Annual
PCC-05	**PCC-05 PCC Compliance with PCC Provider Agreement** Report of PCCs' compliance with the PCC Provider Agreement as required by but not limited to **Section 2.19.B.**	Annual
PCC-06	**PCC-06 Quality Management Plan for PCC Plan Management Support Services** The Contractor must submit a single plan, on an annual basis, that reflects the Contractor's organizational QM philosophy and structure and includes PCC Plan Management Support Services-related activities, as required in **Section 2.13.G.1**.	Annual

*** BH Pharmacy Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
BHPH-01	**BHPH-01 Pharmacy Quarterly Activities Report** The pharmacy director's quarterly activities report to EOHHS on pharmacy-related activities as described in **Section 2.6.D.1.a.6.**	Quarterly

*** Program Integrity Reports**

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
PI-01	**PI-01 Fraud and Abuse Notification (within 5 business days) and Activities** Fraud and Abuse ad-hoc notification for overpayments related to suspected fraud.	Ad-Hoc
PI-02	**PI-02 Notification of For-Cause Provider Suspensions and Terminations (within 3 business days)** Ad-hoc notification of for-cause provider suspensions and/or terminations of the Provider's contract with the Contractor.	Ad-Hoc
PI-03	**[RETIRED]**	
PI-04	**PI-04 Notification of Provider Overpayments** Overpayments identified or recovered, specifying the overpayments due to potential fraud in PI-01.	Ad-hoc
PI-05	**PI-05 - Summary of Provider Overpayments** Detailed summary of provider overpayments (cover letter with instructions and template to be provided by EOHHS).	Semi-annually
PI-06	**PI-06 Response to Overpayments Identified by EOHHS Report** Response to overpayments identified by EOHHS in response to EOHHS ad-hoc notifications of overpayments identified by EOHHS.	Ad-hoc

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
PI-07	**PI-07 Agreed Upon Overpayments Collection Report** Agreed upon overpayments collection report in response to EOHHS ad-hoc notification of overpayments identified by EOHHS.	Ad-hoc
PI-08	**PI-08 Self-Reported Disclosures** Ad-hoc notification of provider self-reported disclosures of overpayments.	Ad-Hoc
PI-09	**PI-09 Program Integrity Compliance Plan and Anti-Fraud, Waste, and Abuse Plan** Compliance plan and anti-fraud, waste, and abuse plan	Annual
PI-10	**PI-10 Payment Suspension** Notification of payment suspensions for a provider.	Quarterly

<u>* Quality Reports</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
QR-01	**QR-01 Quality Management Plan for BH Management** The Contractor must submit a single plan, on an annual basis, that defines the quality management program, details the Contractor's quality activities, and provides for self-assessment of the Contractor's responsibilities under the Contract, as required by **Section 2.13.F**.	Annual
QR-11	**QR-11 Provider Preventable Conditions** Report on Provider Preventable Conditions as required in **Section 2.7.F.7.b.**	Annual
HQ-24	**Health Quality and Equity Strategic Report** Report on items related to the Contractor's Health Quality and Equity Strategic Plan, including but not limited to the requirements set forth in **Section 2.20.C**.	Annual

<u>* Satisfaction Survey Summaries</u>

MBHP Contract Exhibit Number	Name of Report	Deliverable Frequency
Periodic reports as described in **Section 2.13.F.5.d-f** due within 60 calendar days following the end of the survey period, the results and analysis of the findings report of satisfaction survey conducted with Network Providers, PCCs, and Covered Individuals.		
SS-01	**SS-01 Covered Individual Satisfaction Survey** Assessment and analysis of Covered Individual's satisfaction with the Contractor, at least biennially as required in **Section 2.13.F.5**.	Annual
SS-02	**SS-02 Network Provider Satisfaction Survey** ** Due in odd-numbered years (e.g. 2023, 2025, etc.)* Assessment and analysis of Network Provider satisfaction with the Contractor's administration and management of the BHP and Care Management Program stratified by Provider type and specialty, at least biennially as required in **Section 2.13.F.5**.	Biennial
SS-03	**SS-03 PCC Provider Satisfaction Survey** ** Due in even-numbered years (e.g. 2024, 2026, etc.)* Assessment and analysis of PCC satisfaction with the Contractor's administration and management of the BHP, PCC Plan Management Support Services, and the Care Management Program stratified by Provider type and specialty, at least biennially as required in **Section 2.13.F.5**.	Biennial

APPENDIX E-2
CERTIFICATION OF DATA ACCURACY

I, _____ (name and title), of _____ (name of Contractor), pursuant to **Section 2.14.M** of the Contract, certify that the information and data contained in the attached submission is true, accurate, and complete to the best of my knowledge, information, and belief, based on my reasonable inquiry.

_____
Signature of Chief Executive Officer or Chief Financial Officer, or their Authorized Signatory

_____
Print/Type Name

_____
Title of Signatory

_____
Date

APPENDIX E-3
ANNUAL CERTIFICATION

I, _____ (name and title),

of _____ (name of Contractor)

certify that after a diligent inquiry, to the best of my knowledge and belief,

_____ (name of Contractor) is in compliance with **Section 2.3.D.3.e.1.d** of the Contract.

I have not been made aware of any instances of Fraud and Abuse in any program covered by this Contract other than those that have been reported by my organization in writing to EOHHS.

_____
Signature of Chief Executive Officer, Chief Financial Officer, or Compliance Officer

_____
Print/Type Name

_____
Title of Signatory

_____
Date

ATTACHMENT A
APPENDIX E-4

FINANCIAL REPORTS

1. FINANCIAL STABILITY AND INSOLVENCY PROTECTION REPORT

a. **Annual** report, due 60 calendar days after the start of each Contract Year. The report includes:

   1. Documentation of the Contractor's current liability protection policies, including professional liability, worker's compensation, comprehensive liability and property damage; and
   2. Documentation from the Contractor on how it intends to meet the financial stability requirements as described in Contract.

b. **Annual** Insolvency Reserve report, due within one month after the start of each Contract Year. The report includes documentation of the Contractor's financial insolvency insurance, reserves, or a combination of both, in an amount reasonably determined by EOHHS to be adequate to both:

   1. Provide to Covered Individuals for a period of 60 days following the date of insolvency all Covered Services and all other services required under this Contract; and
   2. Continue to provide all such services to Covered Individuals confined in an acute hospital on the date of insolvency, until the date of the Covered Individual's discharge.

2. CAPITATION REVENUE/EXPENSE REPORTS FOR ALL COVERED SERVICES

Monthly report of expense data for all Covered Services, submitted in accordance with the format specified by EOHHS. The report shall include but not be limited to:

a. a summary of the Contractor's monthly and fiscal year-to-date service expenditures for each Rating Category (RC) as well as for the Contractor's total membership;

b. the per-Covered Individual per-month (PMPM) cost, as determined by EOHHS, and total dollars spent for every classification of service, in accordance with the format specified by EOHHS;

c. an indication whether expenses apply to capitated or FFS arrangements with Network Providers, if applicable;

d. incurred but not reported (IBNR) claims adjustments to the service expenditure data, applying the most recent available IBNR adjustments to the following categories:

   1. Inpatient;
   2. Outpatient, including Outpatient day;

3. Diversionary, including 24-hour Diversionary, and all other services. Expenses for these categories shall be reported with and without the application of IBNR adjustments;
4. Substance Use Disorder (SUD)services; and
5. Applied Behavior Analysis (ABA) services

e. detailed description of and possible explanations for large variations in IBNR adjustments between reporting months;
f. a statement of the gains or losses that the Contractor expects the Contractor and EOHHS to experience for the fiscal year, based on the Contractor's monthly expenditure experience, and IBNR estimates and risk-sharing arrangements.

3. QUARTERLY FINANCIAL REPORT IN A FORMAT SPECIFIED BY EOHHS

4. ADMINISTRATIVE REPORT

Annual report of the administrative expenses, by line item, incurred by the Contractor for the Contract Year, including but not limited to:

a. detailed information, by line item, on the Contractor's administrative Direct Costs, Indirect Costs, and Earnings;
b. supporting documents to justify the Contractor's calculations; and
c. a detailed cost summary for components of the Administrative Budget including Care Management.
d. Monthly administrative costs report as specified by EOHHS.

5. IBNR METHODOLOGY REPORT

Annual report, due within 60 calendar days after the start of each Contract Year, providing a detailed description of the Contractor's IBNR methodology for each RC, if available, or if not available, for all Rating Categories for Covered Individuals in the aggregate and for each of the following categories:

a. Inpatient Services;
b. Outpatient Services, including Outpatient Day;
c. Diversionary and all other services;
d. Substance use Disorder Services; and
e. Applied Behavior Analysis services

6. RECONCILIATION REPORT FOR RISK SHARING

Annual report, due within 210 calendar days after the end of each Contract Year, detailing actual expenditures for each applicable RC for the Contract Year, in accordance with the Contract and the format specified by EOHHS for the Capitation Revenue/Expense Report.

7. RECONCILIATION PROCESS FOR CRISIS SERVICES PROVIDED TO UNINSURED INDIVIDUALS AND PERSONS WITH MEDICARE ONLY

Annual report, due within 210 calendar days after the end of the Contract Year, the Contractor shall provide EOHHS with a report of the Contractor's actual expenditures for AMCI/YMCI and CCS services provided to Uninsured Individuals and persons with Medicare only.

8. CONTINUING SERVICES DURING APPEAL RECONCILIATION REPORT

Annual report, due within 210 days after the end of each Contract Year, detailing actual expenditures for each applicable RC for the Contract Year in accordance with the Contract and in the format specified by EOHHS.

9. DSRA/CASH MANAGEMENT REPORTS

a. **Quarterly** Cash Management Report that includes but is not limited to:
   1. statement of deposits from EOHHS and payments by the Contractor, by month, for the quarter reported, stratified by:
      a. type of deposit; and
      b. type of payment.
   2. cash requirements for Covered Services paid from the DSRA that display estimated payroll totals against projected cash balances.

b. **Semiannual** submission of copies of reconciled monthly bank statements that show interest credited to the DSRA for the period reported.

c. **Annual** Cash Reconciliation Report, due within 60 calendar days after the end of each state fiscal year, that indicates the total deposits into and total payments and transfers from the DSRA. The report and format shall be based on the methodology for separately tracking the various types of deposits into the DSRA from EOHHS, as described in **Section 2.18.B**.

10. INDEPENDENT AUDIT REPORT

Copy of the **Annual** report for the Contractor and its parent corporation, if applicable, due within 30 calendar days after its publication.

a. Provides EOHHS with the Contractor's most recent audited financial statement in accordance with Generally Accepted Accounting Principles (GAAP)

11. ATTESTATION REPORT

The Contractor shall provide to EOHHS an attestation report from its independent auditor on the effectiveness of the internal controls over operations of the Contractor related to this Contract in accordance with statements and standards for attestation engagements as promulgated by the American Institute of Certified Public Accountants. The Contractor shall

provide such report annually and within 30 days of when the independent auditor issues such report; provided, however, if the Contractor is Service Organization Control (SOC) compliant, the Contractor shall annually submit a copy of the SOC report in lieu of the attestation report described above within 30 days of the Contractor's independent auditors issuing its SOC report.

12. MEDICAL LOSS RATIO REPORT (MLR)

Provide **annually** the Medical Loss Ratio report as specified in Section 2.15.C of the Contract.

13. RATIO ANALYSIS REPORT

The Contractor shall submit **annually** by June 30th, a Financial Ratio Analysis, that describes the Contractor's performance for financial ratios required by EOHHS in accordance with the definitions in **Exhibit 1** and the format in **Exhibit 2** below. The report shall be generated from the Contractor's audited financial statements.

14. ENCOUNTER VALIDATION REPORT

Provide **quarterly** financial encounter Validation Report as specified in Section 5.3.L and in a format specified by EOHHS.

15. QUARTERLY REPORT FOR SERVICES PROVIDED TO INDIVIDUALS WITHOUT MOBILE CRISIS COVERAGE

Quarterly the Contractor shall provide EOHHS with a report of the Contractor's actual expenditures for AMCI/YMCI, CCS, and three units of urgent outpatient CBHC bundle services provided to Individuals without Mobile Crisis Coverage.

16. QUARTERLY REPORT FOR EMERGENCY DEPARTMENT CRISIS EVALUATION SERVICES PROVIDED TO UNINSURED PERSONS AND PERSONS WITH MEDICARE ONLY

Quarterly the Contractor shall provide EOHHS with a report of the Contractor's actual expenditures for crisis intervention services provided to Uninsured Persons and Persons with Medicare Only in an emergency department.

17. QUARTERLY REPORT FOR URGENT OUTPATIENT CBHC BUNDLE SERVICES PROVIDED TO UNINSURED INDIVIDUALS AND PERSONS WITH MEDICARE ONLY

Quarterly the Contractor shall provide EOHHS with a report of the Contractor's actual expenditures for urgent outpatient CBHC bundle services provided to Uninsured Persons and Persons with Medicare Only, up to three units per individual following an initial crisis evaluation.

18. Behavioral Health Access and Crisis Intervention Trust Fund Report

Provide monthly the Behavioral Health Access and Crisis Intervention Trust Fund Report in a form and format specified by EOHHS.

EXHIBIT 1: FINANCIAL RATIO DEFINITIONS

FINANCIAL INDICATOR	FORMULA
RATE OF RETURN	
ASSETS	Net Income/Total Assets (%)
REVENUES	Net Income/Total Revenue (%)
EQUITY	Net Income/Equity (%)
LIQUIDITY	
CURRENT RATIO	Current Assets / Current Liabilities
ACID TEST	(Current Assets - Accounts Receivable) / Current Liabilities
WORKING CAPITAL	Current Assets - Current Liabilities ($)
CASH TO CLAIMS AND PAYABLES	(Cash and Cash Equivalents) / Claims and Payables
DAYS OF TOTAL IBNR	Total IBNR Claims (Estimated) / (Total Medical Claims / 365) (# Days)
CLAIMS AS A % OF REVENUE	Claims Payable / Total Revenue (%)
CAPITAL STRUCTURE	
DEBT RATIO	Total Debt / Total Assets (%)
DEBT SERVICE COVERAGE	(Net Income + Depreciation + Interest) / (Interest Expense + Current Loans + Notes Payable)
RECEIVABLES TO CURRENT ASSETS	Premium Receivables / Current Assets (%)
CASH TO CURRENT ASSETS	Cash / Current Assets (%)
EQUITY PER ENROLLEE	Total Equity / Total Enrollees ($)
PROFITABILITY	
OPERATING MARGIN	Operating income/Premium revenue (exclude investment income and non-Healthcare related revenue)
NET PROFIT MARGIN	Net Income / Total Revenue (include income from all sources including investments)
GROSS PROFIT MARGIN	(Premiums Revenue - Total Medical Costs) / Premiums Revenue (%)
NET WORTH	Total Assets - Total Liabilities ($)

FINANCIAL INDICATOR	FORMULA
BEHAVIORAL HEALTH EXPENSE RATIO / BEHAVIORAL HEALTH LOSS RATIO	Total Behavioral Health Costs / Total Revenue (%)
BEHAVIORAL HEALTH EXPENSE PMPM	Total Behavioral Health Costs / Member Months ($)
BEHAVIORAL HEALTH EXPENSE PMPD	Total Behavioral Health Costs / Member Days ($)
ADMINISTRATIVE EXPENSE RATIO	Total Administrative Costs / Total Revenue (%)

EXHIBIT 2
FINANCIAL RATIO ANALYSIS

Plan:
Fiscal Year **Contract Year Ending December 31, 2023**

Financial Indicator	**Fiscal Year Ending** 20XX	20XX	20XX
1 RATE OF RETURN			
ASSETS			
REVENUE			
EQUITY			
2 EQUITY			
CURRENT RATIO			
ACID TEST			
CASH TO CLAIMS AND OTHER PAYABLES			
DAYS OF TOTAL IBNR			
CLAIMS PAYABLE AS A % OF REVENUE			
3 CAPITAL STRUCTURE			
DEBT RATIO			
DEBT SERVICE COVERAGE			
RECEIVABLES TO CURRENT ASSETS			
CASH TO CURRENT ASSETS			
EQUITY PER ENROLLEE			
4 PROFITABILITY			
NET PROFIT MARGIN			
GROSS PROFIT MARGIN			
NET WORTH ($000)			
BEHAVIORAL HEALTH EXPENSE RATIO			
BEHAVIORAL EXPENSE PMPM			
ADMINISTRATIVE EXPENSE RATIO (1)			

APPENDIX F
INCIDENT REPORT FORM

Please send by secure email to MassHealth Office of Behavioral Health

Adverse Incident Report

Notifications: ☐ (Contractor's Name) ☐ DMH ☐ DCF ☐ DYS ☐ DPPC ☐ DDS ☐ Other

Client: **Social Security #**:

☐ **M** ☐ **F** **DOB**: **Age**:

Facility: **Unit**: **City**:

☐ **24-hour facility** ☐ **Non 24-hour facility**

Date and Time of Incident: mm/dd/yyyy@hh:mm

Date and Time of Discovery: mm/dd/yyyy@hh:mm

Type of Incident:

Describe Incident. If AWA, please include search, notification and commitment status:

Describe Immediate Response to the Incident:

Restraints Used? ☐ None ☐ Mechanical ☐ Chemical ☐ Physical **Time in Restraints**:

Please Check if Recommended: ☐ Internal Investigation ☐ Policy and Procedure Review ☐ Staff training ☐ Disciplinary action to staff

☐ **Please check if additional information is attached.**

Person Reporting: **Telephone #**:

Signature: **Date:**

MassHealth Office of Behavioral Health

Please send by secure email

Appendix A, Exhibit BH-1

Behavioral Health Adverse Reportable Incident - Daily Roster

Health Plan Name: _____

Date: _____

Please see DMH requirements for Restraint and Seclusion at 104 CMR 27

**** For complete list of BH covered services see plan's contract***

Please note that the shaded columns, starting with row 21 there is a drop down menu. For a full list of options, please see Key tab.

Behavioral Health AIs by Facility, Gender, Service, Age, Type

Facility	Date Received by Plan	Date of Incident	Gender	* Service	AGE Group	Plan's Incident ID code for member	Type of Incident	Type of Incident if Other, briefly describe

APPENDIX G
MANAGED BEHAVIORAL HEALTH VENDOR QUALITY INCENTIVE PROGRAM & QUALITY & EQUITY INCENTIVE PROGRAM (MBHV-QEIP)

Effective Calendar Year 2026

Introduction

This Appendix details how EOHHS will determine the Contractor's Quality and Health Equity Performance as described in the Contract. EOHHS may modify the methodology set forth herein after the execution of the Contract by written amendment. The following information is included. For the purposes of this document, "Performance Year" or "PY" shall mean "Contract Year" as defined in Section 1 of the Contract, unless otherwise specified by EOHHS.

The performance-based quality incentive program and Quality and Equity Incentive Program (QEIP) for the managed behavioral health vendor (MBHV) Contractor for Calendar Years 2023-2027 (henceforth referred to as CY23-27) is summarized below. The summary includes strategic goals, methodology, specific performance targets, and associated available earnings. The earnings associated with each performance-based incentive correspond with the degree of the Contractor's success in meeting the established goals. The measure of the Contractor's success for each performance-based incentive is described in detail below. The Contractor shall only be paid the single amount calculated for each measure based on the measurement methodologies, and not to exceed the maximum annual incentive for each performance incentive.

Section I. Quality Incentive Program

A. <u>Measure Benchmarks and Goals</u>

The Contractor shall produce all required baseline measurements and shall use the same methodology when assessing performance for the measurement period. For HEDIS measures, HEDIS Technical Specifications will be used for the performance-based incentives corresponding to each measurement year. For all non-HEDIS measures, the Contractor shall follow the technical specifications for each measure steward identified by EOHHS. In CY24, EOHHS set the benchmark (threshold, goal, and improvement targets) for each measure in performance incentive 1 based on national, regional, and state benchmarks, historical performance of Contractor, baseline Contractor performance, and spread, distribution, or variation in historical performance. Benchmarks (threshold, goal and improvement targets) will be established for a five-year period (CY23-27). EOHHS does not anticipate changing benchmark values from year to year (or based on Contractor performance or ranking from year-to-year). However, benchmarks will be monitored and reviewed annually, with flexibility to address extenuating circumstances, including, but not limited to: benchmarks that are excessively high or low relative to overall Contractor performance, significant changes to practice standards, significant changes to measure specifications impacting results, and other unforeseen events impacting performance.

B. Methodology

The Contractor shall assess their performance for CY26 on the measures outlined below. Goals for each measure have been set for a five-year period (CY23-CY27) and a modified gap-to-goal analysis will determine the improvement targets for each of the five performance years.

For all HEDIS measures, EOHHS has used 2021 data for the benchmarks outlined below. For the CMS IPFQR Measure, EOHHS has used the most recently available data (2019) to set the benchmarks, though prior to final performance calculation, EOHHS will compare 2019 CMS IPFQR data with 2020 CMS IPFQR data, to determine if the impact of the COVID pandemic necessitates flexibility, as described above, in revising the benchmarks. For the CMS Adult Core Set Measure, EOHHS has used 2022 data for the benchmarks outlined below. For the HEDIS and IPFQR measure, the Contractor shall calculate its performance for CY23, which shall serve as the base year performance for the purpose of improvement goal calculation for CY26. The Contractor shall receive two thirds of the maximum eligible incentive ($1,000,000) at the end of CY26, with the last one third ($500,000) reserved for reconciliation of the final CY26 performance calculation, to be conducted by the end of Q2 2027 when all claims from calendar year 2026 can be reviewed. Data should be stratified by PCC members, Primary Care ACO, and others.

C. Peformance Assessment Methodology

In CY26, incentive payments for Performance-Based Incentive 1 will be calculated using the Performance Assessment Methodology (PAM). According to the PAM, the Contractor will have the opportunity to achieve its full eligible quality incentive amount for excellent quality performance. This may be achieved by establishing a clear threshold and goal benchmark for measures, in effect over the duration of the performance year periods set (e.g., five years); providing opportunity to earn incentive for year-over-year self-improvement (e.g., using gap to goal targets); and providing opportunity to earn incentive payments for each measure based on attainment (e.g., meeting threshold, in-between threshold and goal, and goal performance), and for meeting targets for improvement.

As part of the PAM, the Contractor earns points for performance on each measure. The Contractor earns 10 points for meeting the goal for the assigned time period and can earn 1-9 points proportional for performance between the threshold performance and the goal performance. The Contractor earns zero points for performance below the assigned threshold performance for each measure. The Contractor can earn 5 bonus points for meeting the improvement target over the base year, whether or not the Contractor has met threshold or goal performance targets. Bonus points are designed to reward improvements in performance regardless of their starting rate of performance. No partial credit is awarded for bonus points for improvement that does not meet improvement target.

The Contractor can earn a maximum of 15 points per eligible measure through goal attainment and improvement (bonus points). The maximum allowable total points is 10 multiplied by the number of measures (5 x 10= 50). Strong performance on one measure can

offset weaker performance of other measures. The proportional score for the Contractor is equal to the sum of the Contractor's earned points divided by the maximum allowable points. Proportional scores are between 0-1. The highest proportional performance score for the Contractor is 1. The payment amount is equal to the proportional score multiplied by the eligible payment amount.

D. Measures

Measure	Goal	Threshold Benchmark	Goal Benchmark	Improvement Goal per Year	Maximum Eligible Incentive
M1-a	FUM-7 day: Youth (<18 years old)[1]	69%	88%	1.5%	$1,500,000
M1-b	FUM-7 day: Adult (18+ years old)[1]	61%	75%	1.5%	
M2-a	FUH- 7 day: Youth (<18 years old)[1]	60%	71%	2%	
M2-b	FUH- 7 day: Adult (18+ years old)[1]	41%	55%	2%	
M3	30-Day All-Cause Unplanned Readmission Following Psychiatric Hospitalization in an Inpatient Psychiatric Facility[2]	23%	19%	0.5%	
M4	Pharmacotherapy for Opioid Use Disorder (POD)[1]	28%	33%	0.5%	
M5	Use of Pharmacotherapy for Opioid Use Disorder (OUD)[3]	74%	81%	1%	

1= HEDIS Measure (or subset); Contractor to use HEDIS Technical Specifications
2= CMS IPFQR Measure; Contractor to use CMS IPFQR Technical Specifications
3= CMS Adult Core Set Measure; Contractor to use CMS Technical Specifications

Section II. Quality and Equity Incentive Program (QEIP)

A. Background and Overview of the Managed Behavioral Health Vendor Quality and Equity Incentive Program (MBHV-QEIP)

Massachusetts shifted the delivery system at scale to value-based care under the previous MassHealth section 1115 demonstration approval period, transitioning over 80 percent of eligible Medicaid members into accountable care organizations (ACOs) that are at risk to deliver better health outcomes, lower cost, and improved member experience through integrated, coordinated care.

A key goal of the Commonwealth's in this demonstration period is to improve quality of care and advance health equity, with a focus on initiatives addressing health-related social needs (HRSN) and health disparities demonstrated by variation in quality performance. To support achievement of this goal, Massachusetts is centering equity alongside quality as a pillar of value-based care and as a priority for the state's health care system.

To that end, MassHealth will implement aligned quality and equity initiatives across delivery system settings including but not limited to MassHealth's Managed Care Organizations (MCOs), Accountable Care Partnership Plans (ACPPs) and Primary Care ACOs (together "ACOs"), Managed Behavioral Health Vendor (MBHV), and acute hospitals.

Together, this constellation of coordinated quality and equity initiatives will support Massachusetts in achieving its demonstration goal to improve quality of care and advance health equity.

B. PY1 Implementation Plan for the MBHV-QEIP

1. Scope of this Implementation Plan

   This Performance Year 1 Implementation Plan provided additional details related to implementation of MassHealth's MBHV-QEIP for the first Performance Year (PY) from January 1, 2023-December 31, 2023. Information pertaining to subsequent performance years (PY) 2-5, representing Calendar Years 2024-2027, will be forthcoming.

2. MBHV Quality and Equity Incentive Program (MBHV-QEIP) Domains and Goals

   a. Overview of Targeted Domains for Improvement in the MBHV-QEIP

      For the MBHV-QEIP, the MBHV is incentivized to pursue performance improvements in the domains specified in Table 1.

Table 1. Overview of Targeted Domains for Improvement for the MBHV-QEIP

Domain 1: Demographic and Health-Related Social Needs Data	The MBHV will be assessed on the completeness of beneficiary-reported demographic and health-related social needs data submitted in accordance with the Commonwealth's data requirements. Demographic and health-related social needs data will include at least the following categories: race, ethnicity, primary language, disability status, sexual orientation, gender identity, and health-related social needs. Data completeness will be assessed separately for each data element.
Domain 2: Equitable Quality and Access	The MBHV will be assessed on performance and demonstrated improvements on access and quality metrics, including associated reductions in disparities. Metrics will focus on overall access.
Domain 3: Capacity and Collaboration	The MBHV will be assessed on improvements in metrics such as provider and workforce capacity and collaboration with health system partners to improve quality and reduce health care disparities.

b. Goals for each Domain of the MBHV-QEIP

Anticipated goals for the period from 2023-2027 for each MBHV-QEIP domain are summarized below:

1) Demographic and Health-Related Social Needs Data Collection Domain Goals

a) The MBHV is incentivized to achieve certain milestones to meet an interim goal of 80 percent data completeness for self-reported race and ethnicity data for attributed MassHealth members by the end of Performance Year 3 (CY 2025).

b) The MBHV is incentivized to achieve certain milestones to achieve at least 80 percent data completeness for beneficiary-reported other demographic data (including but not limited to primary language, disability status, sexual orientation, and gender identity) for attributed MassHealth members by the end of Performance Year 5 (CY 2027).

c) The MBHV is incentivized to meaningfully improve rates of HRSN screenings from the baseline period (CY 2024) by the end of Performance Year 5 (CY 2027). To meet this goal, the MBHV must not only conduct screenings of beneficiaries, but also establish the capacity to track and report on screenings and referrals.

2) Equitable Quality and Access Domain Goals

   a) The MBHV is incentivized for performance on metrics such as those related to access to care (including for individuals with limited English proficiency and/or disability); care for behavioral health conditions; care coordination; and patient experience.

   b) For up to the first three Performance Years (PY 2023 through PY 2025), MBHV performance will be based on:

      i. Reporting on access and quality metric performance, including reports stratified by demographic factors (such as race, ethnicity, language, disability, sexual orientation, and gender identity); health related social needs; and/or defined by other individual- or community-level markers or indices of social risk;

      ii. Developing and implementing interventions aimed at improving quality and reducing observed disparities on metrics that account for clinical and social risk factors.

   c) For at least the last two Performance Years (PY2026 and PY2027), MBHV performance will be based on improving quality and/or closing disparities as measured through performance on a subset of access and quality metrics.

3) Capacity and Collaboration Domain Goals

   The MBHV is incentivized to improve service capacity, workforce development, and health system collaboration to improve quality and reduce disparities. The metrics that assess improvement in this domain may relate to provider cultural competence, support for language needs, disability accommodations, and achievement of externally validated equity standards.

3. MBHV-QEIP Performance Year 1 Metrics

To establish a robust foundation for quality and equity improvement and to begin making progress towards five-year health equity goals, the first performance year of the MBHV-QEIP holds the MBHV accountable to metrics listed in Table 2 evaluating contributory health system level interventions in each performance domain.

Table 2. MBHV-QEIP Performance Year 1 Metrics

Subdomain	Metric (*Steward)*	Performance Year 1 status*
Domain 1. Demographic and Health-Related Social Needs Data		
Demographic Data Collection	Race, Ethnicity, Language, Disability, Sexual Orientation, & Gender Identity Data Completeness (*EOHHS)*	Pay for Reporting (P4R)
Health-Related Social Needs Screening	Screening for Social Drivers of Health (*CMS*): *Preparing for Reporting Beginning in PY2*	P4R
Domain 2. Equitable Quality and Access		
Equity Reporting	Stratified Reporting of Quality Data (*EOHHS*)	P4R
Access	Meaningful Access to Healthcare Services for Persons with Limited English Proficiency (*Oregon Health Authority*)	P4R
Access	Disability Competencies (*EOHHS*)	P4R
Access	Accommodation Needs Met *(EOHHS)*	P4R
Domain 3. Capacity and Collaboration		
Capacity	Achievement of External Standards for Health Equity (EOHHS)	P4R
	Member Experience Survey: Cultural Competency, Language Services, and Disability Accommodations	P4R

*Reporting/performance requirements for each measure described in relevant metric technical specifications.

Recognizing that taking on accountability for equity is new for the MBHV, interim and annual goals for Performance Year 1 are designed to promote essential foundational capacity and readiness to assume progressive risk for health quality and equity performance in Performance Year 2-5. Summarized performance expectations are described in Table 3; detailed performance expectations are described in metric technical specifications.

Table 3. Summary of MBHV-QEIP Metric Performance Requirements Performance Year 1

Metric	Performance Expectations for Performance Year 1	Deadline
Domain 1. Demographic and Health-Related Social Needs Data		
Race, Ethnicity, Language, Disability, Sexual Orientation, & Gender Identity Data Completeness (*EOHHS)*	Race, Ethnicity, Language, Disability status (RELD) Sexual Orientation, Gender Identity (SOGI) Assessment – Timely and complete submission to EOHHS of an initial assessment of: 1) beneficiary-reported demographic data adequacy and completeness, and 2) a plan for collecting demographic data including data sources and collection questions.	August 31, 2023
	Complete and timely submission to the MassHealth Data Warehouse (DW) of monthly Member Files as specified (beginning no later than August 31, 2023). The DW will reject monthly Member File submissions that are non-compliant with the specified format (e.g. previously compliant formats) anticipated no later than Q4 2023. Data collected by the MBHV will be submitted via the existing encounter submission process, using the enhanced Member File Specification.	Anticipated beginning no later than Q4 2023
Screening for Social Drivers of Health (*CMS): Preparing for Reporting Beginning in PY2*	Complete and timely submission of a report to EOHHS describing: Health-Related Social Needs (HRSN) Assessment – Timely and complete submission to EOHHS of an initial assessment of 1) beneficiary-reported HRSN data adequacy and completeness, and 2) strategies employed to provide information about referrals including to community resources and support services 2) One or more health-related social needs screening tool(s) selected by MBHV for	Anticipated October 27, 2023

	intended use in screening members beginning in PY2; the selected tool(s) must meet requirements for screening tools for the "Screening for Social Drivers of Health" metric; and 3) An implementation plan to begin screening for health-related social needs in Q1 2024 in order to have capacity to report on the "Screening for Social Drivers of Health" metric beginning in Performance Year 2.	
Domain 2. Equitable Access and Quality		
Stratified Reporting of Quality Data (*EOHHS*)	Complete and timely submission to EOHHS of performance data, including member-level race and ethnicity for clinical measures selected by EOHHS for stratification from the Appendix G-Incentive 1, Promotion of High Quality Care measure slate.	No earlier than April 1, 2024
Meaningful Access to Healthcare Services for Persons with Limited English Proficiency (*Oregon Health Authority*)	Complete and timely reporting of an organizational self-assessment of capacity related to providing access to high quality language services to members.	December 31, 2023.
Disability Competencies (*EOHHS*)	Complete and timely submission to EOHHS of MBHV's DCC Team's completed RIC **Disability-Competent Care Self-Assessment Tool (DCCAT)** report	Anticipated December 1, 2023
Accommodation Needs Met (*EOHHS)*	Complete and timely submission to EOHHS of a report describing MBHV's current practice and future plans for the following: • Screening members for accommodation needs at least annually, including at time of enrollment or Health Needs Assessment, and how the results of this screening is documented. • Other methods, if any, for documenting accommodation needs, at least annually. • Asking members to report if their accommodation needs were met during behavioral health care encounters.	Anticipated December 1 2023

	• Analyses that are performed at the organizational level to understand whether accommodation needs have been met.	
Domain 3. Capacity and Collaboration		
Achievement of External Standards for Health Equity (*EOHHS)*	Complete and timely submission to EOHHS a report outlining the ways in which MBHV has started the process of attaining NCQA Health Equity Accreditation status by the end of PY3 (2025)	December 31, 2023
Member Experience Survey: Cultural Competency, Language Services, and Disability Accommodations	Complete and timely submission to EOHHS of draft version of MBHV Member Experience Survey for PY2 (Measurement Year 2024), and comprehensive plan for survey administration	October 1, 2023
	Complete and timely submission to EOHHS of final version of MBHV Member Experience Survey for PY2 with newly incorporated questions submitted by EOHHS.	December 31, 2023

4. MBHV-QEIP Payment for Performance Year 1

EOHHS will pay MBHV the full maximum eligible incentive amount for each metric described in Table 4 if the specified requirements are met. If any of the specified requirements are not met, or if any of the requirements are not met by the outlined deadline, the MBHV may be ineligible to earn full incentive payment for that specific measure, as determined by EOHHS.

5. MBHV-QEIP Accountability Framework for Performance Year 1

EOHHS will hold MBHV individually accountable for its performance on the MBHV-QEIP performance measures. Total incentive amounts for MBHV for Performance Year 1 will be distributed according to the weighting described in Table 4. Performance expectations for each metric are summarized in Table 3 above and detailed further in technical specifications.

Table 4. Performance Year 1 MBHV-QEIP

***Metric Weights* Subdomain**	**MBHV Quality and Equity Incentive Program Metric (*Steward)***	**Performance Year 1 Weight (%)**	**Maximum Eligible Incentive**
Domain 1. Demographic and Health-Related Social Needs Data		**27.8**	**$278,000**

Demographic Data Collection	Race, Ethnicity, Language, Disability, Sexual Orientation, & Gender Identity Data Completeness (*EOHHS)*	16.7	$167,000
Health-Related Social Needs Screening	Screening for Social Drivers of Health (*CMS*)	11.1	$111,000
Domain 2. Equitable Access and Quality		**44.4**	**$444,000**
Equity Reporting	Stratified Reporting of Quality Data (*EOHHS*)	11.1	$111,000
Access	Meaningful Access to Healthcare Services for Persons with Limited English Proficiency (*Oregon Health Authority*)	16.7	$167,000
	Disability Competencies (*EOHHS*)	8.3	$83,000
	Accommodation Needs Met (EOHHS)	8.3	$83,000
Domain 3. Capacity and Collaboration		**27.8**	**$278,000**
Capacity	Pending Further Guidance From NCQA	13.9	$139,000
	Member Experience Survey: Cultural Competency, Language Services, and Disability Accommodations	13.9	$139,000

C. PY2-5 Implementation Plan for the MBHV-QEIP

1. Scope of this PY2-5 Implementation Plan for the MBHV Quality and Equity Incentive Program

This MBHV Quality and Equity Incentive Program (MBHV-QEIP) Implementation Plan provides additional detail related to implementation of MassHealth's MBHV-QEIP for MBHV Performance Years (PYs) 2-5 from January 1, 2024 – December 31, 2027 of the MBHV contract. Additional detail may be forthcoming for future program years.

2. MBHV Quality and Equity Incentive Program (MBHV-QEIP) Domains and Goals

A. Overview of Targeted Domains for Improvement in the MBHV-QEIP

For the MBHV-QEIP, the MBHV is incentivized to pursue performance improvements in the domains specified in Table 1.

Table 1. Overview of Targeted Domains for Improvement for the MBHV-QEIP

Domain 1: Demographic and Health-Related Social Needs Data	The MBHV will be assessed on the completeness of beneficiary-reported demographic and health-related social needs data submitted in accordance with the Commonwealth's data requirements. Demographic and health-related social needs data will include at least the following categories: race, ethnicity, language, disability status, sexual orientation, gender identity, and health-related social needs. Data completeness will be assessed separately for each data element.
Domain 2: Equitable Quality and Access	The MBHV will be assessed on performance and demonstrated improvements on access and quality metrics, including associated reductions in disparities. Metrics will focus on overall access; access for individuals with disabilities and/or a preferred language other than English; care for behavioral health; and care coordination.
Domain 3: Capacity and Collaboration	The MBHV will be assessed on improvements in metrics such as provider and workforce capacity and collaboration with health system partners to improve quality and reduce health care disparities.

B. Goals for each Domain of the MBHV-QEIP

Goals for each MBHV-QEIP domain are summarized below:

1) Demographic and Health-Related Social Needs Data Collection Domain Goals

a) The MBHV is incentivized to achieve certain milestones to meet an interim goal of 80 percent data completeness for self-reported race and ethnicity data for attributed MassHealth members by the end of Performance Year 3 (CY 2025).

b) The MBHV is incentivized to achieve certain milestones to achieve at least 80 percent data completeness for beneficiary-reported other demographic data (including at least preferred written and spoken

language, disability status, sexual orientation, and gender identity) for attributed MassHealth members by the end of Performance Year 5 (CY 2027).

c) The MBHV is incentivized to meaningfully improve rates of HRSN screenings from the baseline period by the end of Performance Year 5 (CY 2027). To meet this goal, the MBHV must not only conduct screenings of beneficiaries, but also establish the capacity to track and report on screenings and referrals.

2) Equitable Quality and Access Domain Goals

a) The MBHV is incentivized for performance on metrics such as those related to access to care (including for individuals with a preferred language other than English and/or disability); behavioral health; care coordination; and patient experience.

b) Metric performance expectations shall include, at a minimum:

i. Reporting on access and quality metric performance, including stratified by demographic factors (such as race, ethnicity, language, disability, sexual orientation, and gender identity); health-related social needs; and/or defined by other individual- or community-level markers or indices of social risk;

ii. Improving quality and/or closing disparities as measured through performance on a subset of access and quality metrics.

c) For up to the first three PYs, performance will be based on expectations described in 2(b)(i) above. For at least the last two PYs, performance will also be based on expectations described in 2(b)(ii), above.

3) Capacity and Collaboration Domain Goals

a) The MBHV is incentivized to improve service capacity, workforce development, and health system collaboration to improve quality and reduce disparities. The metrics that assess improvement in this domain may relate to provider communication, courtesy, respect, and achievement of externally validated equity standards.

3. MBHV-QEIP Performance Year 2-5 Metrics

Performance Years 2-5 of the MBHV-QEIP will hold the MBHV accountable to metrics evaluating performance in each MBHV-QEIP domain. These metrics were developed with input from health systems and providers through requests for information and comment, public meetings, and ongoing stakeholder engagement. Technical specifications for the MBHV-QEIP PY2-5 metrics may be updated annually or more frequently as necessary. A summary of the MBHV-QEIP metrics and anticipated payment status in PY2-5 are provided in Table 2.

Table 2. MBHV-QEIP PY 2-5 Metrics

Subdomain	**Metric (*Steward)***	**Anticipated payment status***			
		2024	**2025**	**2026**	**2027**
Domain 1. Demographic and Health-Related Social Needs Data					
Demographic Data Collection	Race, Ethnicity, Language, Disability, Sexual Orientation, & Gender Identity Data Completeness (*EOHHS)*	P4R	P4P	P4P	P4P
Health-Related Social Needs Screening	Health-Related Social Needs Screening (EOHHS)	P4R	P4P	P4P	P4P
Domain 2. Equitable Access and Quality					
Equity Reporting	Quality Performance Disparities Reduction (*EOHHS*)	P4R	P4R	P4P	P4P
Access	Meaningful Access to Healthcare Services for Persons with a Preferred Language other than English (*EOHHS*)	P4R	P4P	P4P	P4P
	Disability Competencies (*EOHHS*)	P4P	P4P	P4P	P4P
	Disability Accommodation Needs Screening and Intervention *(EOHHS)*	P4R	P4R	P4P	P4P
Domain 3. Capacity and Collaboration					
Capacity	Achievement of External Standards for Health Equity (EOHHS/*NCQA*)	P4R	P4P	P4R	P4R
	Member Experience: Communication, Courtesy, and Respect (EOHHS*)*	P4R	P4P	P4P	P4P

*P4R= Pay for Reporting, P4P= Pay for Performance. Specific performance trajectories are subject to change. Reporting/performance requirements for each measure described in forthcoming metric technical specifications.

The anticipated reporting expectations for PY2 are summarized in Table 3; detailed reporting and performance expectations for PY2 are included in metric technical specifications. Each report outlined in Table 3 shall be submitted by the MBHV in a form, format, and frequency to be further specified by EOHHS. Additional and/or revised reporting expectations for PY3-5 will be provided prior to the start of each performance year.

Table 3. Anticipated Reporting Expectations for PY2

Measure Name	Anticipated Reporting Expectations for PY2 (to be further specified by EOHHS)
Domain 1: Demographic & HRSN Data	
RELDSOGI Data Completeness	1. Submission of "Member Data and Member Enrollment" file 2. Submission of RELDSOGI Mapping Report inclusive of a plan to develop capacity to capture date stamps by PY5
Health-Related Social Needs Screening	1. Submission of administrative and/or supplemental HRSN data
Domain 2: Equitable Access & Quality	
Quality Performance Disparities Reduction	1. Submission of quality data stratified by race and ethnicity
Meaningful Access to Healthcare Services for Persons with a Preferred Language other than English	1. Submission of Language Access Self-Assessment Survey 2. Submission of Provision of Interpreter Services Data
Disability Competencies	1. Submission of Disability Competency Training Plan 2. Submission of Disability Competency Training Report
Disability Accommodation Needs Screening and Intervention	1. Submission of a Disability Accommodation Needs Report
Domain 3: Capacity & Collaboration	
Achievement of External Standards for Health Equity	1. Submission of Accreditation Status Report
Member Experience: Communication, Courtesy, and Respect	*Reporting expectations are satisfied through the annual MBHV member experience survey, administered by the MBHV.*

4. MBHV-QEIP Payment for Performance Years 2-5

In PY2-5, MassHealth will pay the MBHV based on its health equity score in accordance with Section 4.6 of the MBHV Contract. EOHHS will make a one-time payment to the MBHV after the health equity score has been finalized.

5. MBHV-QEIP Accountability Framework for Performance Year 2-5

MassHealth will hold the MBHV accountable for its performance on the MBHV-QEIP performance measures. MassHealth's anticipated framework for the MBHV-QEIP Performance Assessment Methodology (PAM), which may be adjusted annually as needed (for example to transition measures from pay-for-reporting to pay-for-performance, accommodate new contextual inputs, address extenuating circumstances impacting

performance, etc.), is described below. Measure-specific PAM, including benchmarks, improvement targets and measure score calculation approach, will be described in each forthcoming measure specification.

A. **Benchmarking:** MassHealth will establish performance targets or benchmarks no later than the start of the first pay-for-performance period for the metric.

   1) Benchmarks for quantitative measures will include an attainment threshold and goal benchmark and will be set to apply to the full applicable performance period.

   2) Establishment of benchmarks will be informed by inputs such as initial MBHV-QEIP performance data, historical MBHV data/performance, external data/trends, and/or predetermined performance targets determined by MassHealth.

B. **Improvement Targets:** MassHealth will establish performance improvement targets for performance metrics, as applicable, no later than the start of the first pay-for-performance period for the metric.

   1) Specific improvement targets and the approach for each measure will be set to apply to the full applicable performance period.

   2) The approach and actual improvement target may differ by measure based on factors such as performance trends or type of measure; approaches may include year-over-year self-improvement, gap-to-goal percentage point increase, absolute percentage point increases, set milestones and/or goals for improvement.

C. **Performance Measure Score Calculation**: The performance measure scoring approach will be consistent, as applicable, with other MassHealth incentive programs or other incentive program practices. MassHealth will establish a methodology for performance measure scoring for each measure, to be specified in technical specifications, no later than the first day of the performance period to which the methodology applies.

   1) **Pay-for reporting (P4R) measures.** P4R measures will be assessed on a pass/fail basis for which the MBHV, who reports according to each measure's technical specifications, will receive full points or credit for the metric.

   2) **Pay-for-performance (P4P) measures.** The performance measure scoring and approach will be consistent, as applicable, with other MassHealth incentive programs or other incentive program practices, described below.

      a) Measure scoring will include the following components for each measure:

         i. Attainment points ranging from 0-10 points

         ii. Improvement points ranging from 0-10 points

         iii. Potential bonus points (with a cap) to ensure the MBHV has incentive to improve

      b) Performance measure scores for each measure will be defined as a ratio between 0-1. Scores will be calculated by the sum of the points earned

for each measure divided by the maximum number of points allowable for the measure. The maximum number of points allowable for the measure is the sum of the attainment, improvement and potential bonus points with a determined cap. The score will be calculated as follows:

Performance Measure Score = Points earned for each measure / Maximum number of points allowable for the measure.

c) Some performance measures may have identified sub-measures for which sub-measure performance scores will be calculated in the same manner, but then typically equally weighted to calculate a composite performance measure score. For sub-measures the score is calculated as follows:

Performance Measure Score = Sum of each (Sub-measure Score X Sub-measure Weighting).

D. **Domain Score Calculation**: The domain scoring and approach will, as applicable, be consistent with other MassHealth incentive programs or other incentive program practices. Domain scoring includes the following components:

1) Using the predetermined weights specified in Table 3, a domain score will be calculated by taking each performance measure score in the domain and calculating the sum of each performance measure score multiplied by its respective performance measure weight:

Domain Score = Sum of each (Performance Measure Score Performance Measure Weight) *100*

2) If the MBHV is not eligible for a measure (e.g., does not meet the denominator criteria or minimum volume), the weighting will be redistributed equally to the eligible performance measures in the domain.

E. **Health Equity Score Calculation**: The overall Health Equity Scoring approach will, as applicable, be consistent with other MassHealth incentive programs or other incentive program practices. The overall Health Equity Score includes the following components. Using the predetermined weights specified in Table 3, a health equity score will be calculated by taking each domain score and calculating the sum of each domain score multiplied by its respective domain weight:

*Health Equity Score = Sum of each (Domain Score * Domain Weight).*

The final Health Equity Score will be used to calculate the MBHV's earned incentive payment.

Table 4. PY 2-5 MBHV-QEIP Metric Weights

Domain*	Measure Name	Anticipated Measure Weight (%) by Performance Year				Domain Weight (%)
		2024	2025	2026	2027	
DHRSN	Race, Ethnicity, Language, Disability, Sexual Orientation, & Gender Identity Data Completeness	10	10	15	15	25
	Health-Related Social Needs (HRSN) Screening	15	15	10	10	
EAQ	Quality Performance Disparities Reduction	15	15	20	20	50
	Meaningful Access to Healthcare Services for Persons with a Preferred Language other than English	15	15	15	15	
	Disability Competent Care	10	10	5	5	
	Disability Accommodation Needs	10	10	10	10	
CC	Achievement of External Standards for Health Equity	15	15	10	10	25
	Member Experience: Communication, Courtesy, and Respect	10	10	15	15	
TOTAL						**100**

*DHRSN=Demographic and Health-Related Social Needs Data; EAQ=Equitable Access and Quality; CC=Capacity and Collaboration

APPENDIX H-1

PAYMENT AND RISK SHARING PROVISIONS

Section 1. MassHealth Capitation Payment and Related Payment Provisions

A. Per-Member Per-Month (PMPM) Capitation Rates for Contract Year 2026 (CY26)

1. PCC and TPL: PMPM ($) Rates January 1, 2026 - December 31, 2026

Rating Category	Medical services PMPM	Admin PMPM	Total PMPM
Rating Category I Child:	$ 183.30	$ 7.57	$ 190.87
Rating Category I Adult:	$ 112.13	$ 7.22	$ 119.35
Rating Category I TPL:	$ 22.76	$ 6.77	$ 29.53
Rating Category II Child:	$ 687.78	$ 15.29	$ 703.07
Rating Category II Adult:	$ 356.87	$ 13.76	$ 370.63
Rating Category II TPL:	$ 81.55	$ 12.24	$ 93.79
Rating Category IX:	$ 211.47	$ 7.73	$ 219.20
Rating Category X:	$1,287.63	$ 18.30	$1,305.93

2. Primary Care ACO: PMPM ($) Rates January 1, 2026 - December 31, 2026

Rating Category	Medical services PMPM	Admin PMPM	Total PMPM
Rating Category I Child:	$ 87.76	$ 5.26	$ 93.02
Rating Category I Adult:	$ 87.51	$ 5.27	$ 92.78
Rating Category II Child:	$ 675.53	$ 14.95	$ 690.48
Rating Category II Adult:	$ 395.64	$ 14.03	$ 409.67
Rating Category IX:	$ 186.42	$ 5.62	$ 192.04
Rating Category X:	$1,000.14	$ 16.10	$1,016.24

B. Risk Sharing Corridors for Contract Period CY26, for the Medical Services rates Component of Rating Categories Child I, Adult I, Child II, Adult II, I-TPL, II-TPL, IX, and X (pursuant to Section 4 of the Contract) for PCC and TPL programs

1. Gain on the Medical Services Capitation Rates

The amount of the Gain on the aggregate Medical Services Capitation Rates for the Contract shall be defined as the difference between the Total Medical Services Capitation Payment and the Contractor's Total Expenditures for Covered Services, if such actual expenditures are less than the Total Medical Services Capitation Payment

for Contract Year 2026. EOHHS and the Contractor shall share such gain in accordance with the table below.

Gain	MassHealth Share	Contractor Share
Less than or equal to 1.5%	0%	100%
Above 1.5% and less than or equal to 3%	50%	50%
Above 3%	100%	0%

2. **Loss on the Medical Services Capitation Rates**

   The amount of the Loss on the aggregate Medical Services Capitation Rates for the Contract shall be defined as the difference between the Total Medical Services Capitation Payment and the Contractor's Total Expenditures for Covered Services, if such actual expenditures are greater than the Total Medical Services Capitation Payment for Contract Year 2026. EOHHS and the Contractor shall share such loss in accordance with the table below.

Loss	MassHealth Share	Contractor Share
Less than or equal to 1.5%	0%	100%
Above 1.5% and less than or equal to 3%	50%	50%
Above 3%	100%	0%

C. **Risk Sharing Corridors for CY26 for the Medical Services rates Component of Rating Categories Child I, Adult I, Child II, Adult II, IX, and X (pursuant to Section 4 of the Contract) for the Primary Care ACO Program**

1. **Gain on the Medical Services Capitation Rates**

   The amount of the Gain on the aggregate Medical Services Capitation Rates for the Contract shall be defined as the difference between the Total Medical Services Capitation Payment and the Contractor's Total Expenditures for Covered Services, if such actual expenditures are less than the Total Medical Services Capitation Payment for the CY26. EOHHS and the Contractor shall share such gain in accordance with the table below.

Gain	MassHealth Share	Contractor Share
Between 0 and $100,000	99%	1%
>$100,000	100%	0%

2. **Loss on Medical Services Capitation Rates**

The amount of the Loss on the Capitation Rates for the Contract shall be defined as the difference between the Total Medical Services Capitation Payment and the Contractor's Total Expenditures for Covered Services, if such actual expenditures are greater than the Total Medical Services Capitation Payment for the CY26. EOHHS and the Contractor shall share such loss in accordance with the table below.

Loss	MassHealth Share	Contractor Share
Between 0 and $100,000	99%	1%
>$100,000	100%	0%

Section 2. MassHealth Other Payments

A. Care Management Program

The Contractor shall calculate the number of engaged enrollees in the Practice Based Care Management program (PBCM) by month and report to EOHHS on a quarterly basis. EOHHS shall issue the Engagement PPPM amount, upon review and approval.

Base Per-Participant Per-Month (PPPM) engagement rate for Practice Based Care Management:

Per Participant Per Month.....$150.00

B. Quality Incentive Program and Quality and Equity Incentive Program Arrangements

Total Quality Incentive Program and Quality and Equity Incentive Program Payments may not exceed 105 percent of approved Capitation Payments attributable to the Covered Individuals or services covered by the Contract.

The CY2026 Payments for performance incentives detailed in **Appendix G** to the Contract shall be $3,000,000.00, subject to attainment of reporting and performance measures.

C. PCC Plan Support

For CY26, EOHHS shall pay the Contractor a fixed amount of $850,000 for PCC Plan Support for PCC Plan enrollment up to 85,000 members, to be paid out in monthly installments.

EOHHS reserves the right to reduce the fixed annual amount for PCC Plan Support if the PCC Plan enrollment goes below 70,000 Enrollees and is projected to stay at or below that level, as determined by EOHHS.

If PCC Plan enrollment exceeds 85,000 Enrollees and is projected to stay above 85,000 members, as determined by EOHHS, EOHHS shall pay the Contractor an additional Per

Enrollee Per Month rate of $1 for each additional member in excess of 85,000. The payments shall be based on the monthly PCC member estimates used for prospective monthly capitation payment calculations and shall not be reconciled to actual PCC Plan enrollment.

D. HRSN Supplemental Services and HRSN Administration Payment (pursuant to Section 4.2.W of the Contract)

In CY26, EOHHS shall issue lumpsum payments to the contractor for the provision of HRSN Supplemental Services to Covered Individuals enrolled in a Primary Care ACO in the amount of $8,528,882.82. Additionally, EOHHS shall issue lumpsum payments to the Contractor for administrative costs associated with the delivery of HRSN services in the amount of $2,000,000.

The payments will be issued on a quarterly basis or in other frequency to be determined by EOHHS, as described in **Section 4.2.W.**

Section 3. Other Non-MassHealth Payments

A. [Reserved]

B. Autism Spectrum Disorder-Intellectual Disability (ASD-ID) for MCPAP (pursuant to Section 4.2.A.7 of the Contract)

EOHHS shall pay the Contractor $650,000 in Calendar Year 2026 in support of the ASD-ID for MCPAP activities. These funds may be used to support MCPAP's role in expansion of MCPAP for ASD-ID to support pediatric primary care providers, as long as the use of the funds for this purpose has no impact on MCPAP for ASD-ID's ability to fully meet all program requirements.

1. The Contractor's ASD-ID for MCPAP spending shall not exceed the funding amount set forth in this sub-section.
2. Any unspent funds shall be returned to EOHHS, unless otherwise directed by EOHHS.
3. EOHHS reserves the right to require reporting on expenditures related to this program.

C. Early Childhood MCPAP (pursuant to Section 4.2.A.7 of the Contract)

Subject to availability of funding from DPH, EOHHS shall pay the Contractor $414,274.25 in Calendar Year 2026 in support of the Early Childhood (EC) MCPAP activities.

1. The Contractor's EC MCPAP program spending in CY2026 shall not exceed the funding amount set forth in this sub-section.

2. Any unspent funds shall be returned to EOHHS, unless otherwise directed by EOHHS.

3. EOHHS reserves the right to require reporting on expenditures related to this program.

D. Crisis Service Safety Initiative – "Living Room Model" (pursuant to Section 4.2.A.8 of the Contract)

The Crisis Services Safety Initiative payment shall be $1,403,388 in Contract Year 2026. This amount will be paid out in monthly installments determined by EOHHS.

E. [Reserved]

F. Community Crisis Program for Uninsured Individuals Service Compensation Rate Payment (pursuant to Section 4.2.L of the Contract)

The Community Crisis Program for Uninsured Individuals Service Compensation Rate Payment shall be $6,880,000.00 in Contract Year 2026 and paid out in monthly installments to be determined by EOHHS.

G. Community Crisis Administration Payment

The CY26 funding for the administration of Community Crisis Program for Uninsured Individuals shall be $185,000. The payments will be issued in monthly installments to be determined by EOHHS.

H. DPH Emergency Department (ED) Boarding Grant Initiatives Payment (pursuant to Section 4.2.O of the Contract)

In CY2026 EOHHS shall not issue payments to the Contractor in support of ED boarding initiatives. The ED boarding initiatives spending shall not exceed the funding amount available from prior years. Any unspent funds at the end of the contract period shall be returned to EOHHS unless otherwise directed. EOHHS reserves the right to require reporting on expenditures related to the ED boarding initiatives in a form and frequency determined by EOHHS.

I. Mobile Crisis Intervention Uncompensated Care Payment (pursuant to Section 2.6.B.1 of the Contract)

1. For each individual for which the Contractor pays for the mobile crisis intervention initial evaluation and first day crisis interventions pursuant to **Section 2.6.B.1** of the Contract, EOHHS shall pay the Contractor either a rate of $1,024.64 for an adult mobile non-emergency department encounter, $1,075.87 for a youth non-emergency department encounter or $695.29 for a community-based encounter for such individual or the difference between the aforementioned rates and the amount covered by Third Party Liability, whichever is lower.

2. For each individual for which the Contractor pays for the mobile crisis intervention follow-up pursuant to **Section 2.6.B.1** of the Contract, EOHHS shall pay the Contractor either the following rates or the difference between the below rates and the amount covered by Third Party Liability, whichever is lower:
    i. $30.57 per 15 minutes for AMCI provided at CBHC site by a Paraprofessional or Bachelor's level staff. Follow up interventions provided up to the third day following initial evaluation.
    ii. $33.94 per 15 minutes for YMCI provided at CBHC site by a Paraprofessional or Bachelor's level staff. Follow up interventions provided up to the seventh day following initial evaluation.
    iii. $39.70 per 15 minutes for AMCI provided at CBHC site by a Master's level Clinician. Follow-up interventions provided up to the third day following initial evaluation.
    iv. $44.33 per 15 minutes for YMCI provided at CBHC site by a Master's level clinician. Follow-up interventions provided up to the seventh day following initial evaluation.
    v. $33.94 per 15 minutes for AMCI provided at a community-based site of service outside of the CBHC site by a Paraprofessional or Bachelor's level staff. Follow-up interventions provided up to the third day following initial evaluation.
    vi. $33.94 per 15 minutes for YMCI provided at a community-based site of service outside of the CBHC site by a Paraprofessional or Bachelor's level staff. Follow-up interventions provided up to the seventh day following initial evaluation.
    vii. $44.33 per 15 minutes for AMCI provided at a community-based site of service outside of the CBHC site by a Master's level clinician. Follow-up interventions provided up to the third day following initial evaluation.
    viii. $44.33 per 15 minutes for YMCI provided at a community-based site of service outside of the CBHC site by a Master's level clinician. Follow-up interventions provided up to the seventh day following initial evaluation.
3. For each individual for which the Contractor pays for Community Crisis Stabilization (CCS) pursuant to **Section 2.6.B.1** of the Contract, EOHHS shall pay the Contractor either a rate of $632.05 per unit of Adult CCS or $930.73 per unit of Youth CCS or the difference between the aforementioned rates and the amount covered by Third Party Liability, whichever is lower.
4. For each unit of outpatient CBHC bundle for which the Contractor pays pursuant to **Section 2.6.B.1** of the Contract, up to three units per individual, EOHHS shall pay the Contractor either a rate of $233.90 for a CBHC Adult Services encounter bundle or $241.86 for a CBHC Child/Adolescent Services encounter bundle or the difference between the aforementioned rates and the amount covered by Third Party Liability, whichever is lower.

5. To facilitate payment of the aforementioned claims, the Contractor shall submit invoices to EOHHS at a frequency and format specified by EOHHS in **Appendix E-4**.

J. Emergency Department Crisis Evaluation Payment (pursuant to Section 2.6.B.3 of the Contract)

1. For each individual for which the Contractor pays for the initial crisis evaluation service in the emergency department pursuant to **Section 2.6.B.3** of the Contract, EOHHS shall pay the Contractor a rate of $695.29 for such individual.
2. To facilitate payment of the aforementioned claims, the Contractor shall submit invoices to EOHHS at a frequency and format specified by EOHHS in **Appendix E-4**.

K. CBHI Provider Payments (pursuant to Section 4.2.X of the Contract)

In CY2025, EOHHS issued payments to the Contractor in the amount of $7,500,000, in support of the Children's Behavioral Health Initiative (CBHI) and Community Service Agency (CSA) provider networks. The Contractor's spending on CBHI and CSA activities described in **Section 4.2.X** shall not exceed the funding provided in Contract Year 2025. Any unspent funds shall be returned to EOHHS, unless otherwise directed by EOHHS.

L. DCF M-CAAP Training Payment (Pursuant to Section 2.7.N)

In CY25 EOHHS paid the Contractor $6,398.80 for M-CAAP training conducted in October 2024 and as described in **Section 2.7.N.**

M. Outpatient Crisis Payment (pursuant to Section 2.6.B.2 of the Contract)

1. For each unit of outpatient CBHC bundle for which the Contractor pays pursuant to **Section 2.6.B.2** of the Contract, up to three units per individual, EOHHS shall pay the Contractor either a rate of $233.90 for a CBHC Adult Services encounter bundle or $241.86 for a CBHC Child/Adolescent Services encounter bundle or the difference between the aforementioned rates and the amount covered by Third Party Liability, whichever is lower.
2. To facilitate payment of the aforementioned claims, the Contractor shall submit invoices to EOHHS at a frequency and format specified by EOHHS in **Appendix E-4**.

APPENDIX H-2
PERFORMANCE GUARANTEE REQUIREMENTS AND DOCUMENTS

The Contractor shall provide for the benefit of EOHHS documentation of any combination of: a restricted cash reserve; a performance bond of standard commercial scope issued by a surety company doing business in the State; an irrevocable letter of credit; or a written guarantee from the Contractor's parent or organization (hereafter, collectively, the Performance Guarantees) for as long as the Contractor has outstanding liabilities relating to the Contract of $500,000 or more, or for 15 months after the termination or expiration date of the Contract, whichever is later. The Performance Guarantees shall guarantee, in the event of insolvency or for any other reason that the Contractor fails to meet such obligations: (1) payment of the Contractor's obligations to Providers, Non-Network Providers, and other obligees, if any, under the Contract; and (2) performance by the Contractor of its obligations under the Contract.

All documents constituting evidence of or related to the Performance Guarantees shall be submitted to EOHHS for prior review and approval.

1. A cash reserve payable to EOHHS and maintained in a restricted, segregated escrow account in:
   a. a bank doing business in the Commonwealth and insured by the Federal Deposit Insurance Corporation, or
   b. a savings and loan association doing business in the Commonwealth and insured by the Federal Savings and Loan Insurance Corporation, or
   c. a credit union doing business in the Commonwealth and insured by the National Credit Union Association.

2. A performance bond shall be payable to EOHHS, an agency of the Commonwealth of Massachusetts. In the event that the performance bond obtained by the Contractor must be renewed on a periodic basis, Contractor agrees that at least ninety (90) days prior to the expiration of the then current term of the performance bond, Contractor shall pursue extension of the performance bond through the next succeeding term, and by thirty (30) days prior to said expiration, shall obtain a Continuation Certificate from the surety company, and shall immediately thereafter provide a copy of said Continuation Certificate and other written evidence of such continuation of the performance bond to EOHHS. In the event Contractor is unable to obtain a continuation of the then-current performance bond, Contractor shall immediately notify EOHHS and shall obtain another form of financial guarantee prior to the expiration of the performance bond.

3. An irrevocable letter of credit shall be payable to EOHHS, an agency of the Commonwealth of Massachusetts, and issued by:
   a. a bank doing business in the Commonwealth and insured by the Federal Deposit Insurance Corporation, or
   b. a savings and loan association doing business in the Commonwealth and insured by the Federal Savings and Loan Insurance Corporation, or

c. a credit union doing business in the Commonwealth and insured by the National Credit Union Association.

4. A written guarantee from the Contractor's parent or organization indicating that the Contactor's parent or organization agrees to undertake the Contractor's complete obligations under the Contract in the event of default in the Contractor's performance.

In the event of the Contractor's insolvency or a default by the Contractor under the Contract, EOHHS shall, in addition to any other remedies it may have under the Contract, obtain payment under the Performance Guarantees for the purposes of the following:

1. paying any damages sustained by Providers, Non-Network Providers and other obligees,if any, under the Contract by reason of a breach of the Contractor's obligations under the Contract;
2. reimbursing EOHHS for any payments made by EOHHS on behalf of the Contractor; and
3. reimbursing EOHHS for any extraordinary administrative expenses incurred by reason ofa breach of the Contractor's obligations under the Contract, including, but not limits to, expenses incurred after termination of the Contract by EOHHS for reasons other than the convenience of the State.

In the event EOHHS agrees to accept substitute security in lieu of the Performance Guarantees as defined herein, the Contractor agrees to execute any and all documents and perform any and all acts necessary to secure and enforce EOHHS's security interest in such substitute security including, but not limited to, security agreements and necessary UCC filing pursuant to the Massachusetts Uniform Commercial Code. In the event such substitute security is agreed to and accepted by EOHHS, the Contractor acknowledges that it has granted EOHHS a security interest in such substitute security to secure performance of its obligations under the Contract. The Contractor is solely responsible for establishing the credit-worthiness of all forms of substitute security. EOHHS may, after written notice to the Contractor, withdraw its permission for substitute security, in which case the Contractor shall provide EOHHS with the Performance Guarantees as herein described.

AMOUNT

The Contractor may, subject to EOHHS's review and approval, obtain in any combination a performance bond, letter of credit or cash reserve. The combination of all such Performance Guarantees must be maintained in an amount equal to 45 days of the Contractor's covered services capitation payment revenue for the Contract Year, as projected by EOHHS.

1. The amount of the Performance Guarantees shall be established by EOHHS prior to the start of each Contract Year. This requirement must be satisfied by Contractor not later than 15 days after notification by EOHHS of the amount required.
2. EOHHS may require an increase in the amount of the financial stability requirement throughout the Contract Year. The Contractor shall have 15 days after notification by EOHHS to meet the new requirement.

The Performance Guarantees that must be maintained after the Contract term shall be the lesser of (1) the amount of the Performance Guarantee on the last day of the Contract; or (2) the total amount of outstanding liabilities related to the Contract, as determined by EOHHS in its sole discretion.

GUARANTEES OF THE CORPORATE PARENTS OR GENERAL PARTNERS OF THE CONTRACTOR

Without limiting any of the foregoing, EOHHS reserves the right to require that shareholders, general partners of the Contractor, its parent(s), or all of the foregoing provide personal guarantees or stock pledges, or both, in order to guarantee and secure any obligations set forth in this section in excess of the amounts of the Performance Guarantees.

REPORTING

If the Performance Guarantee is fulfilled with a cash reserve according to **Section 2.15.B.1.d.1** of the Contract, the Contractor shall submit monthly documentation (including bank statements) to EOHHS confirming that a cash reserve meeting the requirements of this section is maintained on the same schedule as the monthly financial reports required under **Appendix E-4**.

APPENDIX J
CREDENTIALING WEBSITES

CMS Website or Database	Go to:	What is checked	Frequency
NPI – National Provider Identifier Verify Provider's NPI 6401 required	https://npiregistry.cms.hhs.gov/	NPI Number, First Name, Last Name may be entered to verify that the provider is on the NPI database.	At enrollment & revalidation and as needed for all provider types
OIG – CMS Office of Inspector General Verify exclusions 6401 required	http://exclusions.oig.hhs.gov	Last name and first name are entered to see if there are any findings under the provider's name	At enrollment, revalidation & monthly for all provider types
MedFile Verify exclusions 6401 required	This file is downloaded from the DEX server. Contractor receives the files from MassHealth.	Last name, first name are searched from the drop down option to ensure the provider's name is not listed and that there are no current findings against them.	At enrollment, revalidation & monthly for all provider types
Adverse Actions Report Verify exclusions 6401 required	This file is downloaded from the DEX server. Contractor receives the files from MassHealth.	View by FEIN, last name, first name, business name, adverse action and termination program to view termination data from CMS	At enrollment, revalidation & monthly for all provider types
SAM – System for Award Management 6401 required	https://sam.gov/search	Enter the provider's last name then first name to verify that the provider is not on the SAM website	At enrollment, revalidation & monthly for all provider types
Death Master File Verify a provider is not listed as deceased 6401 required	Download file with a subscription	Enter the provider's name and/or social security number to verify that any applicant or Reval provider is not on the death file	At enrollment & revalidation for all individual providers and individuals listed on a FRDF
BORIM – Mass. Medical Board Validate licenses, suspensions and actions	https://findmydoctor.mass.gov	You may search by Name, Specialty, License Number or ZIP Code to validate the license and verify if findings that would prevent them from practicing in MassHealth	At enrollment, revalidation & weekly for all provider types
DEA Number Verify DEA number	webforms2/spring/validationLogin?execution=e1s1	Last name, State if the provider is found, verify that the provider's DEA number is current and without issue	At enrollment & revalidation for all providers with a DEA

DIA – Debarment List Verify debarments	https://www.mass.gov/service-details/debarment-list-businesses-ineligible-to-bid-on-state-or-muncipally-funded-contracts	View debarment information by company name, address, city, and state to assure a provider is not listed	At enrollment & revalidation for all provider types
Licenses Verify exclusions	https://www.mass.gov/info-details/check-a-health-profession-license	Verify individuals' licenses by number / business info / personal info to verify the license is current and there are no findings against the ID	At enrollment & revalidation for all provider types when there is a hit on Sam, LEIE, MedFile, OIG
JCAHO (Joint Commission) Verify provider's accreditation/certification status	http://www.qualitycheck.org/consumer/searchQCR.aspx#	You may search a provider based on name, zip code or state. JCAHO is checked for hospital that are applying or being revalidated as is required for complete credentialing.	At enrollment, revalidation and monthly for hospitals
NBCOT (Nat'l Board for Certification in Occupational Therapy Validate licenses and suspensions and actions	https://www.nbcot.org/home/VerifyCredentials	The certification page requests either the certification number or last name, first name. The results are reviewed for whether the provider is Active and if there are any actions against them currently or in the past.	At enrollment, revalidation and monthly for therapists
ASHA (American Speech-LanguageHearing Assn.) Validate licenses and suspensions and actions	http://www.asha.org/eweb/ashadynamicpage.aspx?webcode=ccchome	The ASHA certification page requires either the 8-digit ASHA account number or the provider's first and last name as well as their state. The provider must be licensed by the Board of Speech and Language Pathology as well as be accredited by ASHA.	At enrollment, revalidation & monthly for hearing instrument specialists
CHAP (Community Health Accreditation Program) Validate licenses and suspensions and actions	https://locator.chaplinq.org/	The CHAP website is used to find an accredited Community Health Provider. The home page may be searched by either the Agency Name or by State. The results display the Organization, City and	At enrollment, revalidation & monthly for CHCs

		State, Accreditation Dates, and Services.	
American Board of Opticianry Certification Validate licenses and suspensions and actions	https://www.abo-ncle.org/ABONCLE/ABONCLE/Certification/Searchable-Certification-Database.aspx	The ABO certification database is searched by last name, first name, city, state and zip. The results will display the Certificate holder, Company, Certification, City, State, ZIP, Status, and Expiration date.	At enrollment, revalidation & monthly for opticians
National Examining Board of Ocularists Validate licenses and suspensions and actions	https://neboboard.org/registry	This website displays the National Registry of Board Certified Ocularists. There is no way to search by individual name.	At enrollment, revalidation & monthly for Ocularists
State of New Hampshire Board Actions Validate licenses and suspensions and actions	https://www.oplc.nh.gov/board-medicine-board-actions#:~:text=The%20Board%20of%20Medicine%20retains%20disciplinary%20documents%20on,documents%20and%20the%20current%20status%20of%20the%20license	The provider's name and /or license number is listed on the home page and then searched. Results will indicate the provider's license, start date, end date, expiration date, specialty, and schooling. It will also show "Remarks" indicating "status" such as inactive or dead.	At enrollment, revalidation & weekly verifications
State of Rhode Island Board Actions Validate licenses and suspensions and actions	http://www.health.ri.gov/lists/disciplinaryactions/	The disciplinary actions page has 3 options for search; License type, Find by Name, or Filter by Date. Results are reviewed for matches to any Massachusetts providers.	At enrollment, revalidation & weekly verifications
State of Connecticut Board Actions Validate licenses and suspensions and actions	https://portal.ct.gov/dcp/verify-a-license?language=en_US	The CT DPH displays a Regulatory Action Report that posts actions taken against providers by calendar year and quarter. There are 25 quarters posted which have to be searched individually.	At enrollment, revalidation & weekly verifications Usually updated quarterly

State of New York Board Actions Validate licenses and suspensions and actions	https://eservices.nysed.gov/professions/verification-search	The NY BOH has a search page for Board Action regarding a particular Physician or Physician Assistant. The physician or PA may be entered with the last name; the license number may be searched; the license type may be searched; or the search may be done by entering the effective date of the disciplinary action.	At enrollment, revalidation & weekly verifications
State of Vermont Board Actions Validate licenses and suspensions and actions	http://healthvermont.gov/hc/med_board/actions.aspx	The Vermont DPH site has a page that is for Board Actions by Month. Yearly actions may be reviewed historically back to 2006 by month. There is no board action search by individual alone.	At enrollment, revalidation & weekly verifications
State of Maine Board Actions Validate licenses and suspensions and actions	https://www.maine.gov/md/complaint/adverse-licensing-actions	The State of Maine Board of Licensure in Medicine displays a page titled "Adverse Licensing Actions". These actions are displayed by year with no search ability by individual alone.	Weekly verifications
MA Nursing Board Actions Validate licenses and suspensions and actions	https://www.mass.gov/info-details/disciplinary-action-taken-by-the-massachusetts-board-of-registration-in-nursing	The MA License Verification Site has search options for Profession, License Type, Name, License Number, and Status. For nursing searches the top three options for license status will be Suspension, Revocation and Probation.	Monthly verifications

APPENDIX K

DATA MANAGEMENT AND CONFIDENTIALITY AGREEMENT

This Data Management and Confidentiality Agreement (this "**Agreement**") is made by and between the Executive Office of Health and Human Services, Office of Medicaid ("**EOHHS**" or "**MassHealth**"), and the Massachusetts Behavioral Health Partnership (the "**Contractor**"). EOHHS and the Contractor are sometimes referred to herein individually as a "**Party**" and together as the "**Parties**."

SECTION 1. BACKGROUND, SCOPE, AND DEFINITIONS

Section 1.1 Background/Scope

On March 17, 2022, EOHHS posted on the Commonwealth of Massachusetts procurement website, COMMBUYS, a Request for Responses (Bid Number: BD-22-1039-EHS01-EHS01-70615) ("RFR") to solicit bids from qualified parties to provide BH covered services through the Managed Behavioral Health Vendor Contract to Covered Individuals who are enrolled in the Primary Care Clinician (PCC) Plan and in Primary Care ACOs, and certain fee-for-service (FFS) enrollees.

EOHHS selected the Contractor to administer the Managed Behavioral Health Vendor Contract and, on or about the date hereof, the Contractor entered into a contract with EOHHS in accordance with the terms of the RFR pursuant which the Contractor shall provide such services to, or perform functions or activities for or on behalf of, EOHHS (the "**Contract**").

In accordance with the RFR and the Contract, the Parties are entering into this Agreement to establish certain privacy, security and related obligations of the Contractor with respect to PI and Commonwealth Security Information (each as defined below) that the Contractor uses, maintains, discloses, receives, creates, transmits or otherwise obtains in connection with its provision of a service to, and/or its performance of a function or activity for or on behalf of, EOHHS under the Contract.

Section 1.2 Definitions

When used in this Agreement, the following capitalized terms shall have the meanings ascribed to them below:

"**Activities**" shall mean the activities, functions and/or services to be performed or provided by the Contractor for, on behalf of and/or to EOHHS under the Contract.

"**Applicable Law**" shall mean M.G.L. c. 66A, M.G.L. c. 93H, 801 CMR 3.00, 201 CMR 17, the Health Insurance Portability and Accountability Act (HIPAA) Rules (inclusive of 45 CFR Parts 160, 162, and 164), 42 CFR Part 431, Subpart F, 42 CFR Part 2, 45 CFR §155.260 and any other applicable federal or state law or regulation pertaining to the use, disclosure, maintenance, privacy, confidentiality or security of PI or Commonwealth Security Information.

"**Breach Notification Rule**" shall mean the Breach Notification Rule at 45 CFR Part 164, Subpart D.

"**Commonwealth Security Information**" shall mean all data that pertains to the security of the Commonwealth's information technology, specifically, information pertaining to the manner in which the Commonwealth protects its information technology systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats.

"**Enforcement Rule**" shall mean the HIPAA Enforcement Rule at 45 CFR Part 160, Subparts C, D and E.

"**EOTSS**" shall mean the Massachusetts Executive Office of Technology Services and Security.

"**Event**" shall mean the following, either individually or collectively: 1) any use or disclosure of PI not permitted under this Agreement; 2) any Security Incident; or 3) any other event that would trigger notification obligations under the Breach Notification Rule, M.G.L. c. 93H, other similar Applicable Law, or Third Party Agreement (defined below) requiring notice to consumers and/or oversight agencies in connection with an impermissible use or disclosure or breach of PI.

"**HIPAA Rules**" shall mean 45 CFR Parts 160, 162, and 164, inclusive of the Privacy Rule, the Security Rule, the Breach Notification Rule and the Enforcement Rule.

"**Individual**" shall mean the person to whom the PI refers and shall include a person or organization who qualifies as a personal representative in accord with 45 CFR § 164.502(g).

"**Privacy Rule**" shall mean the Standards of Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

"**PI**" shall mean any Protected Health Information, any "personal data" as defined in M.G.L. c. 66A, any "patient identifying information" as used in 42 CFR Part 2, any "personally identifiable information" as used in 45 CFR §155.260, "personal information" as defined in M.GL. c. 93H, and Third Party Data (defined below in **Section 2.1.B**) and any other individually identifiable

information that is treated as confidential under Applicable Law or agreement (including, for example, any state and federal tax return information) that the Contractor uses, maintains, discloses, receives, creates, transmits or otherwise obtains in connection with its performance of the Activities. Information, including aggregate information, is considered PI if it is not fully de-identified in accord with 45 CFR §§164.514(a)-(c).

"**Security Rule**" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

"**System**" shall mean any EOHHS system, database, application or other information technology resource.

When used in this Agreement, the following terms shall have the same meaning as those terms have in the HIPAA Rules: Business Associate, Limited Data Set, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident and Workforce.

All other capitalized terms used in this Agreement but not otherwise defined herein or elsewhere in this Agreement shall be construed in a manner consistent with the HIPAA Rules, M.G.L. c. 66A and all other Applicable Laws.

SECTION 2. DATA MANAGEMENT AND CONFIDENTIALITY

Section 2.1 Data Management and Confidentiality Obligations of the Contractor

A. **Compliance with Applicable Laws.** The Contractor must comply with all Applicable Laws that may be in effect upon execution of, or as may be effective during the course of, this Agreement, including, but not limited to, the Privacy and Security Rules, 42 CFR 431, Subpart F, 42 CFR Part 2 and M.G.L. c. 66A. Without limiting the generality of the foregoing, the Contractor acknowledges and agrees as follows:

1. Obligations under M.G.L. c. 66A. The Contractor acknowledges that in performing the Activities it will create, receive, use, disclose, maintain, transmit or otherwise obtain "personal data" (as defined in M.G.L. c. 66A) and that, in so doing, it becomes a "holder" of such data for purposes of M.G.L. c. 66A. The Contractor agrees that in performing the Activities and otherwise complying with this Agreement it shall, in a manner consistent with the Privacy and Security Rules and other Applicable Laws, comply with M.G.L. c. 66A.

2. Business Associate. In performing the Activities, the Contractor acknowledges and agrees that it is acting as EOHHS' Business Associate and agrees to comply with all

requirements of the HIPAA Rules applicable to a Business Associate. To the extent that the Contractor is to carry out an obligation of EOHHS under the Privacy Rule pursuant to this Agreement or the Contract, the Contractor agrees that it shall comply with the requirements of such Rule that apply to the Contractor as EOHHS's Business Associate in the performance of such obligation.

3. 42 CFR Part 2. The Contractor agrees that to the extent it receives, stores, processes, uses, creates or transmits drug or alcohol abuse information that was obtained by a Part 2 Program, Lawful Holder, or EOHHS (as such terms are used in 42 CFR Part 2), it is bound by 42 CFR Part 2 and shall not use or disclose information except as permitted under 42 CFR Part 2 by a contractor receiving such information under 42 CFR §2.33(b). For example, the Contractor shall not use such information for the purposes of treatment, care coordination, or case management, or further redisclosure such information to law enforcement, unless authorized under 42 CFR Part 2.

4. Telephonic Laws. To the extent the Activities involve outreach to or other contact with consumers (including Individuals), such contact shall be compliant with all applicable federal and state laws and regulations, including the Telephonic Consumer Protection Act of 1991 (47 U.S.C. §227) and its attendant regulations. To the extent the Activities involve call recording activities, the Contractor shall comply with all federal and state wiretapping and recording laws and regulations, including M.G.L. c. 272 §99.

B. Compliance with Third Party Agreements. The Contractor agrees that it shall comply (and shall cause its employees and other workforce members to comply) with any other privacy and security obligation that is required as the result of EOHHS (or EOTSS or another third party, on EOHHS' behalf) having entered into an agreement (any such agreement, a "**Third Party Agreement**") with a third party (such as the Social Security Administration, the Department of Revenue or the Centers for Medicaid and Medicare Services) to obtain or to access PI from a third party (any such PI, "**Third Party Data**") or to access any System containing Third Party Data or through which Third Party Data could be accessed, including, by way of illustration and not limitation, signing a written compliance acknowledgment or confidentiality agreement, undergoing a background check or completing training. The Parties acknowledge and agree that Third Party Data includes, without limitation, all data that EOHHS receives or obtains from Massachusetts Department of Revenue, the Social Security Administration, the Internal Revenue Service, the Department of Homeland Security or through the Federal Data Services Hub and, notwithstanding anything herein to the contrary, the Contractor may not access any

such Third Party Data unless disclosure of such data to the Contractor is permitted under the applicable Third Party Agreement(s), all conditions for disclosure under such Agreement(s) have been satisfied and the Contractor's access to such data is otherwise permitted under the terms of this Agreement. For the purpose of this Agreement, Third Party Agreements in place as of the date hereof include, by way of illustration and without limitation, include the Information Exchange Agreement between CMS and EOHHS. Such agreements are contained in **Exhibit C** for the Contractor's review.

C. **Ownership and Control of Data.** EOHHS is the lawful owner, lawful holder or license holder of all PI and Commonwealth Security Information (each as defined herein) provided to the Contractor in connection with the Contractor's performance of the Services contemplated under the Contract and has the right to permit the Contractor access to or use of the PI and Commonwealth Security Information in connection with its performance of the Services, subject to the Contractor's obligations under this the Contract (including this Agreement). The Contractor acknowledges that its access to, receipt, creation, use, disclosure, transmission and maintenance of any PI, and any data derived or extracted from such PI, arises from and is defined by the Contractor's obligations under the Contract, and that the Contractor does not possess any independent rights of ownership to such data. Any PI and Commonwealth Security Information is provided "as is" and EOHHS hereby disclaims all warranties, whether express, implied, statutory, or otherwise. EOHHS specifically disclaims all implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, and all warranties arising from course of dealing, usage, or practice. EOHHS makes no warranty of any kind that the PI and Commonwealth Security Information, will be secure, accurate, complete, free of harmful code, or error free. In no event will EOHHS be liable under or in connection with this Agreement under any legal or equitable theory, including breach of contract, tort (including negligence), strict liability, and otherwise, regardless of whether licensor was advised of the possibility of such losses or damages or such losses or damages were otherwise foreseeable.

D. **Sanctions for Improper Access, Use or Disclosure of PI.** The Contractor acknowledges that PI subject to this Agreement is highly regulated and the Contractor and its subcontractors, agents, employees and other workforce members may be subject to civil and criminal penalties under state and federal law for accessing, using or disclosing PI in violation of this Agreement or Applicable Law.

E. **Requirements Applicable to Subcontractors, Agents, Employees and other Workforce Members.**

1. Generally. Access to PI (including potential access) must be limited to subcontractors and agents approved by EOHHS, and employees and other workforce members who have been approved by the Contractor. Such individuals are only permitted to access PI if they require access to such data for purposes of carrying out the Activities. Subcontractors, agents, employees and other workforce members with access to PI must receive appropriate privacy and security training, must be informed of the confidential nature of PI, must agree to comply with limitations of this Agreement and other applicable terms required under the Contract and must be informed of the civil and criminal penalties for misuse or unauthorized disclosure of PI under Applicable Law. Without limiting the generality of the foregoing, all subcontractors, agents, employees and other workforce members with access to unencrypted PI or an encryption key used to secure such PI must sign the Confidentiality Acknowledgement attached hereto as **Exhibit A** prior to being granted such access.

2. CORI Regulations. The Contractor shall, pursuant to and in accordance with 101 CMR 15.03(1)(B), require and consider the criminal history information pertaining to all employees and workforce members of the Contractor who will be given access or potential access to PI, and all applicants for employment with the Contractor where the position applied for entails access or potential access to PI. The Contractor shall otherwise comply with all applicable terms of 101 CMR 15.00 in connection with the review and consideration of employee and applicant criminal records.

3. Additional Requirements for Subcontractors and Agents.

    a. The Contractor shall enter into written agreements memorializing the requisite terms of the Agreement with each subcontractor and agent that will have access to PI (each, a "Subcontract"), and shall maintain such Subcontracts.

    b. All such Subcontracts must contain all requisite terms of this Agreement and the Contract (including the Commonwealth Terms and Conditions) related to the privacy and security of PI, and otherwise must be consistent with all such terms and conditions. Without limiting the generality of the foregoing, the Contractor shall ensure that any such Subcontract satisfies all applicable requirements under the Privacy and Security Rules for a contract or other arrangement with a Business Associate.

    c. The Contractor shall require that any subcontractor or agent that needs access to Third Party Data or a System containing such Third Party Data or through which it may be accessed to comply (and to cause its employees and other workforce members to comply) with any privacy and/or security obligation that may be

required under a Third Party Agreement. The Contractor shall ensure that any such subcontractor or agent has satisfied all such obligations prior to being granted access to the Third Party Data or System. The Contractor shall work with EOHHS to ensure that all such obligations are satisfied.

d. The Contractor is fully responsible for any subcontractor's or agent's performance and for meeting all terms and requirements of this Agreement. The Contractor will not be relieved of any legal obligation under this Agreement, regardless of whether the Contractor subcontracts for performance of any Agreement responsibility or whether PI or other information was in the hands of a subcontractor or agent.

4. Assignment. The Contractor shall not assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of EOHHS. Any purported assignment or delegation in violation of this Section is null and void. No assignment or delegation relieves Contractor of any of its obligations under this Agreement.

F. Data Security.

1. Administrative, Physical and Technical Safeguards. As of the Contract effective date, the Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PI and that prevent use or disclosure of such PI other than as provided for by this Agreement. All such safeguards must meet, at a minimum, and the Contractor shall otherwise comply with, all standards set forth in the Contract, Privacy and Security Rules, as applicable to a Business Associate, and all applicable EOHHS, EOTSS, other Commonwealth security and information technology resource policies, processes and mechanisms, including the EOHHS Enterprise Information Security Standards (attached in **Exhibit B**) and the EOTSS Enterprise Information Security Policies and Standards (found online at Mass.gov[1]), and any standards contained in any applicable Third Party Agreement (collectively, the "**Standards**"). Contractor shall comply with any new or updated Standards issued by federal, state, or other issuing agency or entity.

---

[1] EOTSS, Enterprise Information Security Policies and Standards, https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards (last visited July 1, 2021).

The Contractor shall notify EOHHS of any change in its administrative, technical, or operational environments that compromise or otherwise impact the confidentiality, integrity, or availability of PI or any changes to the Contractor's information controls which alters its conformance with the Standards.

2. Access to Facilities, Books, and Records. Upon reasonable notice, the Contractor agrees to allow representatives of EOHHS or, with respect to Third Party Data, other data owners, access to premises where PI is stored (including Contractor's premises or its hosting facility) for the purpose of inspecting privacy and physical security arrangements implemented by the Contractor to protect such PI, compliance with Applicable Law or compliance with Federal grant requirements. EOHHS retains the right to further inspect the Contractor's books and records, including without limitation, Contractor's information security plan, business continuity plan, disaster recovery plan, or other documentation required to be maintained pursuant to the Standards or otherwise in this Agreement.

3. Periodic Review. The Contractor shall monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls. Contractor must represent its conformance to the Standards by conducting an internal review of its compliance with the Standards on an annual basis. Such internal review will include an industry-standard vulnerability of the Contractor's environment. Such internal review will also include attestation to and a demonstrable validation review of the ongoing functionality of the Contractor's controls in its response to the RFR. In the event Contractor is not compliant with some aspect of the Standards, Contractor agrees to remediate such gap(s) in compliance within a reasonable timeframe. If Contractor cannot remediate such gap(s) within a reasonable timeframe, EOHHS reserves the right to implement a pro-rated modification of payments to the Contractor until compliance is reached.

4. Contractor Responsibilities. Contractor understands that it is solely responsible for meeting the Standards, as applicable, and for managing its information security program.

5. Commonwealth Security Information. If the Contractor obtains access to any Commonwealth Security Information in connection with this Agreement, the Contractor may only use such information for the purposes for which it obtained access. In using the information for such permitted purposes, the Contractor shall limit access to the information only to its employees and other workforce members as necessary to perform the permitted purposes. The Contractor shall not release or disclose such information except in accord with EOHHS's express written instructions,

unless such disclosure is Required by Law and then only in accordance with this Agreement (including **Section 2.2B** hereof). While in possession of such information, the Contractor shall apply all applicable privacy and security requirements set forth in this Agreement to maintain the confidentiality, security, integrity and availability of such information. Notwithstanding any other provision in this Agreement, the Contractor shall report any non-permitted use or disclosure of Commonwealth Security Information to EOHHS within twenty-four (24) hours following the date upon which the Contractor becomes aware of the use or disclosure (or such earlier time as may be required under a Third Party Agreement). The Contractor shall immediately take all reasonable actions to retrieve such information if disclosed to any non-permitted person or entity; shall include a summary of such retrieval actions in its required report of the non-permitted disclosure; and shall take such further retrieval action as EOHHS may reasonably require. Notwithstanding any other provision in this Agreement regarding termination, the Contractor may not retain any Commonwealth Security Information upon termination of this Agreement unless such information is expressly identified in any retention permission granted in accord with **Section 3.2B**. If retention is expressly permitted, all data protections stated herein survive termination of this Agreement and shall apply for as long as the Contractor retains the information.

6. Written Information Security Program. The Contractor shall ensure that it maintains a written information security Program (WISP) in compliance with the terms of this Agreement, including, but not limited to, M.G.L. c. 93H.

G. Obligations upon a Non-Permitted Use or Disclosure of PI or other Event.

1. Mitigation and Other Activities. Immediately upon becoming aware of an Event, the Contractor shall take all reasonable and appropriate action necessary to:

   a. retrieve, to the extent practicable, any PI involved in the Event;

   b. mitigate, to the extent practicable, any harmful effect of the Event known to the Contractor; and

   c. take such other action(s) as may be required in connection with the Event to comply with any Applicable Law.

   Upon request, the Contractor shall take such further actions as EOHHS may reasonably request, or shall take such reasonable additional action to assist EOHHS, to further mitigate any harmful effect of the Event. Any actions to mitigate harmful

effects of such Event undertaken by the Contractor on its own initiative or pursuant to EOHHS' request shall not relieve the Contractor of its obligations to report such Event or otherwise comply with this **Section 2.1.G,** any other provisions of this Agreement or the Contract or Applicable Law.

2. Notification and Reporting Activities. As soon as possible, but in any event no later than twenty-four (24) hours after Contractor becomes aware of the Event, the Contractor shall verbally report the Event to EOHHS Privacy Office with as much of the details listed below as possible, and shall follow such verbal report within three (3) business days with a written report outlining the Event with the following information:

    a. The date of the Event or the estimated date (if date unknown);

    b. The date of the discovery of the Event;

    c. The nature of the Event, including a root cause analysis, containing as much specific detail as possible (e.g., cause, contributing factors, chronology of events);

    d. The nature of the PI involved in the Event (e.g., the types of identifiers and other information involved), together with samples of any forms or documents that were involved in the Event to illustrate the type of PI involved (with personal identifiers removed or redacted);

    e. The exact number of individuals whose PI was involved in the Event if known or, if unknown, a reasonable estimate based on known facts (categorized according to the type of PI involved, if different types of PI was involved for different individuals), together with a description of how the number of individuals was determined;

    f. A summary of the nature and scope of the Contractor's investigation into the Event;

    g. The harmful effects of the Event known to the Contractor, all actions the Contractor has taken or plans to take to mitigate such effects, and the results of all mitigation actions already taken;

    h. A summary of steps taken to prevent such Event in the future, including copies of revised policies and procedures, changes in business processes and staff training; and

i. Any additional information and/or documentation that the Contractor is required to provide to EOHHS under 45 CFR §164.410, M.G.L. c. 93H, §3(a) or other similar Applicable Law.

If an Event is the result of a Security Incident, such as hacking, ransomware, or other related Event, the Contractor shall prepare and provide a written forensics report to EOHHS that shall, at a minimum, describes the attack, security vulnerabilities, and any other information EOHHS deems necessary. Such information, documents, and deliverables shall not be redacted or withheld by the Contractor.

To the extent that any such information is not available at the time of the report, the Contractor shall provide such information to EOHHS as such information becomes available in one or more subsequent written reports. The Contractor shall provide EOHHS with such additional information regarding the Event as EOHHS may reasonably request, which additional information may include a written risk analysis rebutting any presumption that the Event constituted a breach for purposes of the Breach Notification Rule. *Notwithstanding the foregoing, any Event involving "return information" (as defined in 26 U.S.C. §6103(b)(2)) must be reported to EOHHS within one (1) hour of discovery.*

3. Obligations under Consumer Notification Laws. If EOHHS determines, in its sole discretion, that it is required to provide notifications to consumers or state or federal agencies under the Breach Notification Rule, M.G.L. c. 93H, other Applicable Law, or Third Party Agreement as a result of the Event, the Contractor shall, at EOHHS's request, assist EOHHS in drafting such notices for EOHHS's review and approval, and shall take such other action(s) as EOHHS may reasonably request in connection with EOHHS's compliance with the Breach Notification Rule, M.G.L. c. 93H, other Applicable Law, or Third Party Agreement, but in no event shall the Contractor have the authority to give any such notifications on EOHHS's behalf unless EOHHS authorizes and directs the Contractor to do so in writing. Additionally, at EOHHS's direction, the Contractor shall provide credit monitoring services to affected Individuals as required under M.G.L. c. 93, §3A or other Applicable Law.

4. Reimbursement for Costs. The Contractor shall reimburse and indemnify, defend and hold harmless EOHHS for all costs incurred or sustained by EOHHS in responding to, and mitigating damages caused by, any Event or third party claims or causes of action brought or asserted against EOHHS involving:

   a. the Contractor's failure to meet its responsibilities under, or in violation of, any provision of this Agreement or the Contract;

b. the Contractor's violation of Applicable Law;

c. the Contractor's negligence;

d. the Contractor's failure to protect data under its control with encryption or other security measures that constitute an explicit safe-harbor or exception to any requirement to give notice under Applicable Law; or

e. any activity or omission of the Contractor resulting in or contributing to an Event.

Such costs may include, for example and without limitation, losses, damages, liabilities, deficiencies, awards, penalties, fines, costs or expenses, including reasonable attorneys' fees and the costs associated with any notification required under subsection 3, above, including staffing and materials costs. Alternatively, at EOHHS' direction, in lieu of reimbursing EOHHS for such any such costs the Contractor shall, at Contractor's expense, conduct any such notification or other mitigation related activity on EOHHS' behalf. This provision shall apply in addition and separate to any generally applicable indemnification provision applicable to the Contractor.

H. Response to Legal Process. The Contractor shall report to EOHHS, both verbally and in writing, any instance where PI or any other data obtained in connection with this Agreement is subpoenaed or becomes the subject of a court or administrative order or other legal process (including a public records request under Massachusetts law). The Contractor shall provide such report to EOHHS as soon as feasible upon receiving or otherwise becoming aware of the legal process; *provided*, *that* the Contractor shall provide such report no later than five (5) business days prior to the applicable response date. In response to such legal process, and in accordance with instructions from EOHHS, the Contractor shall take all reasonable steps, including objecting to the request when appropriate, to comply with M.G.L. c. 66A § 2(k), 42 CFR § 431.306(f), 42 CFR Part 2 and any other Applicable Law. If EOHHS determines that it shall respond directly, the Contractor shall cooperate and assist EOHHS in its response.

I. Individual's Privacy Rule Rights. With respect to any relevant PI in the Contractor's possession, the Contractor shall take such action as may be requested by EOHHS to meet EOHHS' obligations under 45 CFR §§ 164.524, 164.526 or 164.528 or other Applicable Law pertaining to an Individual's right to access, amend or obtain an accounting of uses and/or disclosures of its PI, in sufficient time and manner for EOHHS to meet its obligations under such Privacy Rule provisions or other Applicable Law. If an Individual contacts the Contractor with respect to exercising any rights the Individual may have

under 45 CFR §§ 164.524, 164.526 or 164.528 or similar Applicable Law with respect to PI in the Contractor's possession, the Contractor shall respond to such requests in accordance with Applicable Law and cooperate with EOHHS to meet any of its obligations with respect to such request.

With respect to an Individual's right to an accounting under 45 CFR § 164.528, the Contractor shall document all disclosures of, and access to, PI as would be necessary for EOHHS to respond to a request by an Individual for an accounting in accord with 45 CFR § 164.528. The Contractor shall also document uses and disclosures of PI and other data access activities to the extent required under M.G.L. c. 66A, § 2(f).

J. **Individual's Direct Authorization to Disclose PI to Third Party.** In the event Contractor receives a request from the Individual or from a third party to release PI to a third party pursuant to a consent, authorization, or other written document, Contractor shall, respond to such requests in accordance with Applicable Law and cooperate with EOHHS to meet any of its obligations with respect to such request.

K. **Record Access.** The Contractor shall make its internal practices, books and records, including policies and procedures, relating to the protection, security, use and disclosure of PI and Commonwealth Security Information obtained under this Agreement, and the security and integrity of Systems containing PI or Commonwealth Security Information or through which it may be accessed, available to EOHHS and the Secretary, in a time and manner designated by the requesting party, for purposes of enabling EOHHS to determine compliance with this Agreement or for purposes of enabling the Secretary to determine compliance with the HIPAA Rules.

L. **Inventory of Systems/PI.** Within thirty (30) days of the effective date of this Agreement, the Contractor shall provide EOHHS an accurate list of electronic and paper databases and other Systems containing PI, together with a description of the type(s) of PI contained in such databases and Systems and the various uses of the databases and Systems. The Contractor shall update such lists as necessary to reflect the addition or termination of such databases and Systems or changes to the PI stored therein or uses thereof.

M. **Compliance Officer.** The Contractor shall designate a Compliance Officer, who shall be responsible for overseeing the Contractor's compliance with this Agreement. Such designation shall be provided to EOHHS on the effective date of the Contract and may be changed during the period of this Agreement only by written notice.

N. **Destruction of PI and Commonwealth Security Information during Contract Term**. The Contractor shall retain PI and Commonwealth Security Information during the course of the Contract in accordance with the terms of this Contract and all applicable state and federal retention laws and regulations. If, in accordance with such requirements, Contractor determines that, during the course of the Contract, it is appropriate to destroy PI or Commonwealth Security Information, it shall do so only after obtaining EOHHS' written permission. In the event destruction is permitted, Contractor shall destroy PI in accord with standards set forth in NIST Special Publication 800-88, Guidelines for Media Sanitization, M.G.L. c. 93I and other Applicable Laws relating to the destruction of confidential information, including PI, all applicable state and federal retention laws and regulations, and all state data security policies including policies issued by EOHHS and EOTSS. Within five (5) days of destroying PI or Commonwealth Security Information in accordance with the requirements of this paragraph, Contractor shall provide EOHHS with a written certification that destruction has been completed in accord with the required standards set forth herein.

Section 2.2 **Permitted Uses and Disclosures of PI by the Contractor**

Except as otherwise limited in this Agreement, including in this **Section 2.2**, the Contractor may use or disclose PI only as follows:

A. **Activities.** The Contractor may use or disclose PI to perform the Activities or as otherwise required by, and in accordance with, the provisions of this Agreement; *provided*, *that* such use or disclosure would not: (i) violate the Privacy Rule or other Applicable Law if done by EOHHS; (ii) violate the EOHHS' Minimum Necessary policies and procedures that are known to the Contractor or that EOHHS advises the Contractor of; or (iii) conflict with statements in the MassHealth Notice of Privacy Practices. When using or disclosing PI or when requesting PI from EOHHS or another party in performing the Activities, the Contractor represents that it shall make reasonable efforts to limit the amount of PI used, disclosed or requested to the minimum necessary to accomplish or perform the particular Activity for which the PI is being used, disclosed or requested.

B. **Required by Law.** The Contractor may use or disclose PI as Required by Law, consistent with the restrictions of the HIPAA Rules, 42 CFR Part 431, Subpart F, 42 CFR Part 2, M.G.L. c. 66A, any other Applicable Law or any applicable Third Party Agreement.

C. **Restriction on Contacting Individual.** The Contractor shall not use PI to contact or to attempt to contact an Individual unless such contact is a permitted Activity, or made in accordance with EOHHS' written instructions.

D. **Publication and Research Restriction.** The Contractor shall not use PI for any publication, statistical tabulation, research, report or similar purpose, regardless of whether or not the PI can be linked to a specific individual or has otherwise been de-identified in accord with the standards set forth in 45 CFR §164.514, unless the Contractor has obtained EOHHS' prior written consent and the Contractor provides EOHHS a license to such information. In no event shall any resulting publication, report or other material contain PI unless the publication, report or other material is made available only to EOHHS or the Contractor has obtained the specific written approval of EOHHS' Privacy Officer.

Section 2.3 Data Management and Confidentiality Obligations of EOHHS

A. **Notice of Privacy Practices.** EOHHS shall make the MassHealth Notice of Privacy Practices is available online at: https://www.mass.gov/service-details/masshealth-brochures-and-pamphlets. EOHHS may notify the Contractor in writing of any change in the MassHealth Notice of Privacy Practices to the extent that such change may affect the Contractor's use or disclosure of PI under this Agreement.

B. **Notification of Changes in Authorizations to Use or Disclose PI.** EOHHS shall notify the Contractor in writing of any change in, or revocation of, permission by an Individual to use or disclose PI that is known to EOHHS, to the extent that such change may affect the Contractor's use or disclosure of PI under this Agreement.

C. **Notification of Restrictions.** EOHHS shall notify the Contractor in writing of any restriction to the use or disclosure of PI that EOHHS has agreed to in accord with 45 CFR §164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PI under this Agreement.

D. **Requests to Use or Disclose PI.** EOHHS shall not request that the Contractor use or disclose PI in a manner that would violate the Privacy Rule or other Applicable Law if done by EOHHS.

SECTION 3. TERM, TERMINATION AND EFFECT OF TERMINATION

Section 3.1 Term and Termination

A. This Agreement shall be effective upon execution by each party and shall terminate upon the termination or expiration of the Contract, unless earlier terminated by EOHHS in accordance with subsection B, below.

B. If EOHHS determines, in its sole discretion, that the Contractor has violated any material term of this Agreement or the Contract pertaining to the privacy or security of PI, EOHHS may terminate this Agreement and the Contract immediately upon written notice to the Contractor.

Section 3.2 <u>Effect of Termination</u>

A. Except as provided in subsection B immediately below, upon termination of this Agreement for any reason whatsoever (including expiration), the Contractor shall, at EOHHS' direction, either return or destroy all PI and Commonwealth Security Information, and the Contractor shall not retain any copies of such PI or Commonwealth Security Information in any form. In no event shall the Contractor destroy any PI or Commonwealth Security Information without first obtaining EOHHS' approval. In the event destruction is permitted, the Contractor shall destroy PI and Commonwealth Security Information in accord with standards set forth in NIST Special Publication 800-88, Guidelines for Media Sanitization, all Applicable Laws and applicable retention laws and regulations and all data security policies including policies issued by EOHHS and EOTSS. This provision shall apply to all PI and Commonwealth Security Information in the possession of the Contractor's subcontractors, and the Contractor shall require that all such information in the possession of its subcontractors and agents be returned or destroyed and that no subcontractor or agent shall be permitted to retain any copies of such information in any form, in accord with EOHHS' instructions. The Contractor shall, within three (3) business days of the return or destruction of PI and Commonwealth Security Information, certify to EOHHS in writing that all PI and Commonwealth Security Information has been returned or destroyed in accordance with this **Section 3.2** and neither the Contractor nor any of its subcontractors or agents retains any PI or Commonwealth Security Information.

B. If the Contractor determines that returning or destroying PI or Commonwealth Security Information is not feasible, the Contractor shall provide EOHHS written notification of the conditions that make return or destruction not feasible. If, based on the Contractor's representations, EOHHS concurs that return or destruction is not feasible, the Contractor shall extend all protections pertaining to PI and/or Commonwealth Security Information set forth in this Agreement to all such information and shall limit further uses and disclosures of such information to those purposes that make its return or destruction not feasible, for as long as the Contractor (or any of its subcontractors) maintains any PI or Commonwealth Security Information.

SECTION 4. ADDITIONAL TERMS AND CONDITIONS

Section 4.1 Notices

Unless otherwise specified herein, all notices, reports, requests, consents, claims, demands, waivers and other communications provided under this Agreement (each, a "Notice") shall be in writing and shall be deemed to have been given to a Part: (i) when delivered by hand; (ii) on the date sent by facsimile or by e-mail if sent during normal business hours of the Party, and on the next business day if sent after normal business hours of the Party; or (iii) on the third day after the date deposited in the U.S. Mail, first class, postage pre-paid, *provided*, *that*, in each case, the Notice is delivered or addressed to the Party's contact person(s) at the address(es) identified below (or to such other contact person(s) at such other address(es) as the recipient may from time to time specify in a notice given in accordance with this **Section 4.1**):

EOHHS:

General Counsel
Executive Office of Health and Human Services
One Ashburton Place, 11th Floor
Boston, MA 02108
Privacy.Officer@mass.gov

Contractor:

Massachusetts Behavioral Health Partnership
1000 Washington Street, Suite 310
Boston, MA 02118
Attention: Chief Executive Officer

With copies to:

Beacon Health Options, Inc.
200 State Street, Suite 302
Boston, MA 02109
Attention: General Counsel

Section 4.2 Amendment

This Agreement may be amended by the Parties at any time; *provided*, *that* any amendment must be in writing and must be signed by each Party. The Contractor shall promptly execute and comply with any amendment to this Agreement that EOHHS determines is necessary to

ensure compliance with all applicable statutes, orders, and regulations promulgated by any federal, state, municipal, Third Party Agreements, or other governmental authority pertaining to the privacy or security of PI, including any Applicable Law. Such requisite amendment may cover all activities and PI collected under the original Contract. The Contractor's failure to amend this Agreement in accordance with the foregoing sentence shall be considered a breach of a material provision for purposes of **Section 3.1B**. The Parties agree to negotiate in good faith to cure any omissions, ambiguities, or manifest errors herein.

Section 4.3 Survival

Notwithstanding any other provision concerning the term of this Agreement or the Contract, all protections and other obligations of the Contractor pertaining to PI and/or Commonwealth Security Information set forth herein and in the Contract shall survive the termination of this Agreement and shall continue to apply until such time as all such information is returned or destroyed in accordance with **Section 3.2** or, if later, until any outstanding obligation of the Contractor with respect to such information has been satisfied.

Section 4.4 Interpretation.

A. Any ambiguity in this Agreement shall be resolved to permit EOHHS to comply with the HIPAA Rules, 42 CFR Part 431, Subpart F, M.G.L. c. 66A and any other Applicable Law.

B. For purposes of this Agreement, (i) the words "include," "includes" and "including" shall be deemed to be followed by the words "without limitation"; (ii) the word "or" is not exclusive; and (iii) the words "herein," "hereof," "hereby," "hereto" and "hereunder" refer to this Agreement as a whole. The definitions given for any defined terms in this Agreement shall apply equally to both the singular and plural forms of the terms defined. Whenever the context may require, any pronoun shall include the corresponding masculine, feminine and neuter forms.

C. Unless the context otherwise requires, references herein to: (i) Sections, Attachments, Exhibits, and Appendices mean the Sections of, and Attachments, and Exhibits, and Appendices attached to, this Agreement; (ii) an agreement, instrument or other document means such agreement, instrument or other document as amended, amended and restated, supplemented and modified from time to time to the extent permitted by the provisions thereof; and (iii) a statute or regulation, including an Applicable Law, refers to that law or regulation as in effect or as amended from time to time and includes any successor legislation or regulation.

D. The Attachments, Exhibits, and Appendices referred to herein shall be construed with, and as an integral part of, this Agreement to the same extent as if they were set forth verbatim herein.

Section 4.5 Counterparts.

This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. A signed copy of this Agreement delivered by email, facsimile or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

Exhibit A

ACKNOWLEDGMENT REGARDING CONFIDENTIALITY OF PROTECTED INFORMATION

I, the undersigned, understand that in the course of my work for _____, (name or organization) relating to a contract with the Executive Office of Health and Human Services (EOHHS), I may have access to protected information- ("PI")-including protected health information, other personally identifiable information or security information--either provided by EOHHS or created or obtained on its behalf.

I understand that PI is confidential and access to, use of and disclosure of PI is regulated by federal and state law including, without limitation, the privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and M.G.L. c. 66A, and the terms of the EOHHS contract.

I recognize that the unauthorized access, use or disclosure of PI may cause serious harm to individuals. Unauthorized access, use or disclosure of PI may also violate the terms of the EOHHS contract and/or federal or state law, which may result in civil or criminal penalty including, without limitation, fines and imprisonment.

Acknowledged and agreed:

Protected Information User's name (printed or typed): _____

Protected Information User's Signature: _____

Date: _____

Contractor:_____

NOTE: **Exhibit A** need not be submitted to EOHHS. Appendix A must be retained by the Contractor and made available EOHHS upon request.

Exhibit B

EOHHS ENTERPRISE INFORMATION SECURITY STANDARDS

Exhibit C

INFORMATION EXCHANGE AGREEMENT BETWEEN CMS AND EOHHS

ENTERPRISE INFORMATION SECURITY STANDARDS

Commonwealth of Massachusetts
Executive Office of Health and Human Services

I. CONTENTS

II. PURPOSE AND INTRODUCTION 2

III. REQUESTS FOR NON-CONFORMANCE..... 4

IV. SECURITY PLANNING..... 5

V. ACCEPTABLE USE AND INFORMATION SECURITY TRAINING 6

VI. ACCESS CONTROL..... 9

VII. AUDIT AND ACCOUNTABILITY..... 17

VIII. INVENTORY AND CLASSIFICATION 20

IX. ASSESSMENT AND MONITORING 25

X. AUTHORIZATION TO OPERATE AND OPERATIONAL RISK ASSESSMENT 28

XI. INCIDENT RESPONSE AND SECURITY INCIDENT RESPONSE TEAM 32

XII. CONTINGENCY PLANNING 45

XIII. CONFIGURATION MANAGEMENT..... 47

XIV. IDENTITY AND AUTHENTICATION 50

XV. MEDIA PROTECTION 53

XVI. SYSTEM AND COMMUNICATIONS 54

XVII. PHYSICAL AND ENVIRONMENTAL PROTECTIONS 59

XVIII. PERSONNEL SECURITY..... 64

XIX. SYSTEM AND SERVICES ACQUISITION..... 67

XX. SYSTEM AND INFORMATION INTEGRITY 69

XXI. DEFINITIONS..... 69

II. PURPOSE AND INTRODUCTION

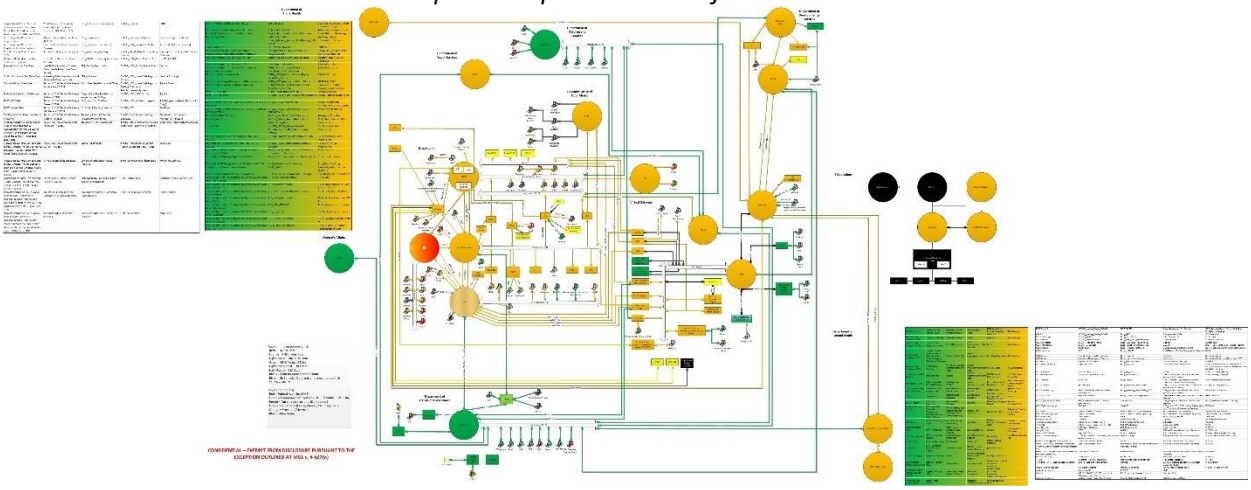
The EOHHS Information Security Office's mission is to safeguard EOHHS's and its Agencies' collective data in any form and prevent the inappropriate use, exfiltration, or manipulation of that data. The Security Office works constantly to maximize preservation of the confidentiality, availability, and integrity of EOHHS data through the promulgation, implementation, and enforcement of administrative, physical, and technical safeguards.

This document outlines the specific ways such data should be preserved. It provides the bare minimum standards that apply to all Information Resources in the EOHHS Environment and within third party environments contracted for by EOHHS or which use, process, or maintain EOHHS data. These have been drafted with an eye towards:

- Federal and State legal requirements
- Specific data source contractual requirements
- Commonwealth enterprise policies and standards (available at: https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards)
- Extant good practice at Agencies and within Information Systems
- Other factors as appropriate

The need for this broadly applicable set of standards is clear when looking at the EOHHS Environment in its entirety.

Table 1: Graphical Representation of EOHHS Environment



As illustrated in Table 1, all Information Systems in the EOHHS Environment are connected, either directly or through other Information Systems which share data downstream. Few systems in the EOHHS Environment are truly independent of that environment. To the extent those applications are used to support Agency operations alongside other applications and their data can impact Agency operations, they are not independent.

Additionally, very little—if any—physically held data (e.g.: paper documents, filing cabinets holding documents, etc.) maintained in the EOHHS Environment exists independently of EOHHS's Information Systems. Those physical data stores either come from Information Systems or are used to populate

information into Information Systems. As such, all physical instances of data—or physical instances of information— maintained in the EOHHS Environment or by a third party fall within the purview of these Information Security standards.

Because of the extreme interconnectedness of all data held (in any form) at EOHHS, and to promote the common security of data shared among the EOHHS enterprise, these common controls are designed to protect all data with the same high standards no matter where it is used, processed, or maintained within the EOHHS Environment. However, due to the state of standardization across EOHHS, not all applications existing or in development can strictly adhere to this *Enterprise Information Security Standards* (also referred to as "Document"). The Security Office strongly recommends that all Information Systems strive to achieve compliance with this Document, however any gaps will be identified and tracked through gap assessments being conducted of the EOHHS Environment. EOHHS and Agency process must be updated to achieve compliance with applicable standards within twenty-four (24) months from publication of this Document. Compliance timelines have been included with each standard. Achieving compliance may be completed by implementing a corrective action plan with additional reasonable timelines for conformance—supported by business necessity and technical requirements—outlining why compliance cannot be attained within the timelines outlined in this Document. Such corrective action plans must follow the guidelines outlined in *Section III, Requests for Non-Conformance*. Additionally, all applications procured or developed after the publication date of version 1.0 of this Document must be developed in conformance with these requirements.

Additionally, EOHHS is bound by state and federal laws, contracts, and processes to comply with various notification procedures in the event of a loss of data, an impact of service, or a data breach, whether it happens at EOHHS or with one of its third party vendors, providers or other teaming partners. EOHHS will also face associated negative press, fines, and other penalties associated with loss of confidentiality, integrity, or availability of the data. As such, these standards also act as a guideline with regard to the security requirements EOHHS must push down to any third party vendor.

The Security Office has been tasked with preserving the confidentiality, integrity, and availability of all EOHHS Information Resources. As such, this Document outlines the minimum acceptable requirements at EOHHS for the information security controls outlined herein. Agencies may develop their own documentation to supplement and exceed these requirements, which are generic for the EOHHS Environment at large, and are encouraged to do so. Agencies may not undertake any action or promulgate documentation to supplant or undermine the controls or activities described in this Document, whether specifically identified as intended to do so or not.

These *Enterprise Information Security Standards* supersede all EOHHS and/or Agency documentation existing before the publication date of this Document which also covers the same subject matter as these standards or any portion thereof. No other EOHHS or Agency documentation covering the same subject matter as these *Enterprise Information Security Standards*, unless as expressly required to be developed by these *Enterprise Information Security Standards*, shall be effective without the review and approval of the EOHHS Security Office.

The consequences for violating these *Enterprise Information Security Standards* are serious. By violating this policy, you create an immediate and automatic audit finding for your Agency. These Audit findings could result in significant negative press for your Agency, additional oversight and reporting requirements, and fines. In addition, depending on the objectives violated and the method of violation, you may be subject to discipline including termination of employment, civil penalties including monetary

fines, and criminal penalties including jail time. Conformance to these policies will be actively monitored on an ongoing basis and violations will be reported to Agency and Secretariat executive staff.

III. REQUESTS FOR NON-CONFORMANCE

Any non-conformance to these standards could have dire and unintended impacts to other Information Resources or Information Systems in the EOHHS Environment. Additionally, the failure to appropriately record non-conformance to standards and any activities undertaken to minimize the impact to EOHHS's security posture could result in audit findings, fines, and other penalties. Given the nature of these controls and the interconnectedness of the EOHHS Environment, no individual Agency group is appropriately equipped to approve non-conformance to these standards. The process outlined in this section will detail how a request for non-conformance should be made and processed. For promotion of vulnerabilities from a lower to a production environment, or for risk acceptance of ongoing vulnerabilities, see the *Authorization to Operate and Operational Risk Assessment Policy and Process*.

a. All requests for non-conformance should be submitted to the EOHHS Security Office mailbox at: EOHHS-SecurityOffice@MassMail.State.MA.US. All requests must include "Request for Non-Conformance" in the title and the application/program name for which a request for non-conformance is sought.

   The body of the email should describe:
   i. the request being made,
   ii. the justification,
   iii. any compensating controls put in place to address the security gap (or a reason why there is no security gap)
   iv. timelines to address the security gap
   v. the name, title, and contact information of the individual responsible for the request

b. The request will be evaluated by the Security Office, which may seek additional information from the requester, members of EOHHS and/or impacted Agency legal teams, impacted Agency operations, and the EOHHS SCIO and/or impacted ACIOs. Response times may vary depending on the request, but all requests will be addressed within forty-eight (48) hours of receipt.

c. Once the Security Office has completed its evaluation, it will provide a memorandum to the requester outlining any research performed, recommendations, and agreed-upon timelines during which there will be a security gap.

d. Quarterly, the Security Office will meet with requesters to discuss the status of implementation of compensating controls or closing the security gap. Biennially, the Security Office will circulate the master list of requests for non-conformance to Agency and IT leadership for review and analysis.

IV. SECURITY PLANNING

a. Policy Statement

EOHHS must develop, maintain, and disseminate a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

b. Security Planning Standards

This information security plan outlines the minimum functions necessary to ensure the effective and efficient operations of the Secretariat in a way that maximizes the safety of sensitive information. While many of the organizational roles and responsibilities are outlined herein, not all specific roles and responsibilities are identified. It is the responsibility of application teams and business units to ensure that they appropriately identify critical or material positions within their respective organizations. Information security planning is a comprehensive, organization-wide effort to ensure that information in all forms is protected.

i. Roles and Responsibilities

1. Agency heads and Secretariat Chief Information Officer – these individuals are responsible for business unit and information technology planning and setting priorities for their respective organizations. These individuals are also accountable for the responsible development of programs and systems within their purview. This includes considerations of legal and policy compliance; implementation of industry standard best practices; and ensuring appropriate custodianship of constituent data that protects the confidentiality, integrity, and availability of that data.
2. Agency management teams and Assistant Chief Information Officers – these individuals are responsible for direct oversight, management and implementation of business unit and information technology planning and projects as well as for the development of programs and systems within their purview.
3. Chief Security Officer – this individual is responsible for the creation and verification of standards at EOHHS to support the responsible development of programs and systems at EOHHS.
4. EOHHS Staff – these individuals are responsible for following acceptable rules of behavior, including the *EOHHS Acceptable Use Policy.* Additionally, these individuals are responsible for ensuring the confidentiality, integrity, and availability of data maintained by EOHHS and its Agencies.

ii. Information Resource Security Plans

All Information Resources and business units must complete a security plan. This security plan must cover, at a minimum, the following topics:

1. How the information resource or business process operates consistently with enterprise architecture or planning;
2. The boundaries of the information resource or business process;
3. How the information resource or business process supports Agency operations and the Agency mission;
4. The security posture, security requirements and risk level of the information resource or business process;
5. Relationships and interconnections between the information resource or business process and other information resources or business processes;
6. Security controls in place based on the NIST 800-53 standards appropriate to that application as expressed by these *Enterprise Information Security Standards*, security controls not in place, and planned remediation or workarounds (including compensating controls);
7. How the information resource or business process architecture/design protects the confidentiality, integrity, and availability of information; and
8. Any assumptions about internal or external services and their impact to security.

These requirements will be satisfied by compliance with:

- *Section VIII, Inventory and Classification,*
- *Section IX, Assessment and Monitoring,*
- The EOHHS IT Control Plan,
- *The EOHHS Technology Office Secretariat Application Reference Manual,* and
- *The Project Integration Process & Controls Guide.*

The security plan must be reviewed and updated no less frequently than every three years.[1] While the security plan should be communicated to relevant internal and external authorized parties, it should be safeguarded from inappropriate disclosure that would compromise the security of the Information Resource.

iii. *Rules of Behavior*

The rules of behavior for use of EOHHS information resources is outlined in *Section V, Acceptable Use and Information Security Training.* Agency management teams and ACIOs are responsible for devising plans to ensure review, attestation, and compliance with the Acceptable Use Policy.

V. ACCEPTABLE USE AND INFORMATION SECURITY TRAINING

a. Purpose and Introduction

The key to ensuring a safe and secure environment is by having a staff that is competent and capable with respect to information security. No matter how secure and airtight an

[1] Pursuant to 45 CFR § 95.621, for APD-funded operations and Information Resources, this is every two years.

organization's technical environment, if its employees cannot handle information appropriately, each of those employees poses a significant vulnerability to the organization.

This *Section V, Acceptable Use and Information Security Training*, will offer the requirements for training and provide managers and staff the tools they need to ensure the EOHHS Environment is adequately protected against external and internal threats.

Agencies are encouraged to develop information security training in addition to the requirements outlined in this section. If, at the time of publication of this policy, Agencies have documentation they believe satisfies the requirements herein for acceptable use or information security training, or if the Agency develops any related documentation after the publication of this policy, the Security Office must review and approve of such documentation before implementation.

b. Policy Statement

All EOHHS employees must review and acknowledge the *EOHHS Acceptable Use Policy* within one (1) month of hire and on an annual basis thereafter, as determined by EOHHS. All EOHHS employees must take EOTSS and EOHHS training within one (1) month of hire and on an annual basis thereafter. If an EOHHS employee has not met these requirements, they shall not be provided access to Information Resources in the EOHHS Environment. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Acceptable Use Standards

The *EOHHS Acceptable Use Policy* details its purpose, requirements and scope. In summary, the Acceptable Use Policy explains the difference between appropriate and inappropriate—or permissible and impermissible—use of Information Resources across EOHHS.

In the event that any staff is found to have violated the Acceptable Use Policy, depending on factors such as the magnitude of the violation(s), the number of violation(s), and the kind of violation(s), those staff may be disciplined. Such discipline may include limitation of or removal of rights to access Information Resources, suspension or termination of employment, or civil and criminal penalties such as fines and incarceration.
The current version of record of the *EOHHS Acceptable Use Policy* is hosted on PACE and is attached to this document as Attachment 1. Older versions of the *EOHHS Acceptable Use Policy* may be stored elsewhere but should not be relied upon for compliance purposes.

Agencies may not under any circumstances create documentation to supplant or replace the *EOHHS Acceptable Use Policy.* Agencies may, however, create documentation that effectively supplements or adds to the *EOHHS Acceptable Use Policy* based on demonstrated and legitimate Agency need. Agencies are strongly encouraged to do so where the *EOHHS Acceptable Use Policy* has perceived deficiencies based on the quality or kind of data being handled by the Agency or based on legal compliance. Any supplementary materials, whether or not identified as such, must be reviewed and approved by the Security Office prior to publication and dissemination to staff. Such supplementary materials will be made effective by appending them to the *EOHHS Acceptable Use Policy* as an exhibit.

d. Information Security Training Standards

All EOHHS staff must review and acknowledge the EOHHS Information Security Training, or an approved alternative, within one (1) month of hire and prior to accessing any Information Resources in the EOHHS Environment and then on an annual basis thereafter as defined by EOHHS. The EOHHS Information Security Training shall consist of two components:

i. Any required EOTSS information security training generally made available to EOHHS staff, and
ii. Any required EOHHS information security training.

EOHHS has published the EOHHS Information Security Training on PACE. Previous versions of the EOHHS Information Security Training may be stored elsewhere but should not be relied upon for compliance purposes. At a minimum, all staff are required to take that calendar year's information security training posted to PACE. The Security Office has also developed other information security training for specific types of data that may be required based on job duties and role.

All EOHHS staff must take information security training that covers the following subject matter:

- Definition of sensitive information,
- An explanation of the need to safeguard sensitive information,
- How to protect sensitive information,
- Least access privilege,
- Password requirements,
- Kinds of data breaches and attack vectors,
- Email management,
- Incident reporting, and
- Steps that staff can take to prevent a data breach.

The current EOHHS information security training is deemed to meet the requirements of Executive Order 504 training for EOHHS employees. Additionally, the training is designed to contain information that is intended to meet the training requirements of the HIPAA Security Rule and applicable Third Party Agreements.

Agencies may create documentation that effectively supplants or replaces the EOHHS Information Security Training. Agencies may also create documentation that effectively supplements or adds to the EOHHS Information Security Training. Agencies are strongly encouraged to do so where the EOHHS Information Security Training has perceived deficiencies based on the quality or kind of data being handled by the Agency or based on legal compliance. Any supplanting or supplementary materials, whether or not identified as such, must be reviewed and approved by the Security Office prior to publication and dissemination to staff.

VI. ACCESS CONTROL

a. Purpose and Introduction

Access Control, in the broadest sense, deals with who has access to what and how. The standards outlined in this Access Control section address specific requirements about how permission to view, use, change, or update Information Resources should be granted, modified, and revoked in the EOHHS Environment. For access controls for facilities themselves, please see *Section XVII, Physical and Environmental Protections*.

Agencies may—and are encouraged to—promulgate desk level procedures and standards to implement the requirements outlined herein for their Information Resources. Agencies may already have access control documentation. This Access Control standard is not intended to supplant those documents. Care should be taken to ensure those standards conform to the requirements expressed herein. Agencies may not implement documentation, standards, or requirements that supplant these Access Control standards or modify, compromise, or circumvent the underlying controls in this document in any way.

While this document is drafted with a focus to managing access to Information Systems, the process outlined herein can—and should—be applied to all EOHHS Information Resources in whatever form and to all processes which utilize such data.

b. Policy Statement

All EOHHS Information Resources must have appropriate access controls in place to prevent unauthorized access. All access to Information Resources must be appropriate based on role, employment status, and business need. All Information Resource Owners must have the ability to control, audit, and terminate access to Information Resources. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Access Control Standards

Every Information Resource must have clearly defined and readily identifiable Owners. Owners must be capable of independently making material decisions and modifications with respect to the direction and operations of the Information Resource. In the event an Information Resource does not have a clearly defined and readily identifiable Owner upon request, the Chief Operating Officer (or equivalent position) and ACIO of the Agency to which the Information Resource is associated and/or belongs shall be assigned such roles by default. In the event an Information Resource does not belong to a specific Agency, the EOHHS Assistant Secretary for Administration and Finance and SCIO shall be assigned to such roles by default.

i. Defining Roles and Accounts

Information Resource Owners are responsible for identifying Roles and accompanying accounts in the Information Resource. To simplify the relationship

between Roles and accounts: Roles address business function and accounts address technical access based on business function. Those Owners must ensure implementation of the following requirements when defining Roles and accounts:

1. **Roles:** Each Information Resource must have clearly defined and documented Roles (including group Roles) based on responsibility, business need, staff role, or other logical association. The documentation of such Roles must include criteria for membership in that Role and an overview of the permissions granted to that role.

2. **Types of Roles:** Each identified Role must have an accompanying account, permission group, or other configuration which defines the access permissions an individual with that Role will have with respect to the Information Resources. Roles and accounts should be pared on a one-to-one basis. Multiple accounts may have the same access permissions to an Information Resource if necessitated by their accompanying Roles.

3. **Least Privilege:** Assignment of permissions and capabilities must be narrowly tailored and follow the Principle of Least Privilege. Each individual, Role, and account may have only the minimum level of access required to perform their authorized function.

   For example, a normal desktop user should not have administrator-level access on their machine and should not be able to change basic system settings or install new software; similarly, a web application should not be run with administrator rights (or root in the Linux/Unix context) to the operating systems on which it runs. At a minimum, Information Resources must have the following separate Roles and associated Accounts defined by EOTSS standard *IS.003 Access Management*:

   a. User Account
   b. System (or Application) Account
   c. Service Account
   d. Administrator (or Root) Account
   e. Firecall (or breakglass/emergency recovery) Account

4. **Ability to Review Access Controls:** All Information Resources must have a type of account (included in or in addition to the above) that is capable of reviewing lists of all individuals authorized to access an Information Resource and the accounts assigned to those individuals.

5. **Limit and Audit Privileged Accounts:** For any Accounts or Roles that have broad access to information or the ability to modify Information Resource operations ("privileged" accounts or roles), Owners must develop a mechanism to ensure that (a) account creation and use are expressly authorized based on well-defined criteria; (b) accounts are limited to the individuals whose function requires broad privilege; (c) account creation and use is tracked and auditable; and (d) appropriate mechanisms are in

place to timely offboard privileged accounts. For example, an employee providing desktop support may need to be able to elevate to administrator-level access on workstations in the group they support, but should not be able to use administrator-level access on workstations in areas of the organization they do not support, nor on servers administered by a separate group.

6. **Logical Separation:** Accounts must ensure logical separation of access to different components and data within the Information Resource based on Role. That logical separation must ensure that accounts and individuals have only the minimal amount of access necessary to fulfill their business and technical requirements. Additionally, Owners must ensure that such access constraints are uniformly enforced (across Information Resources and in each instance of access). Access must be constrained, procedurally or logically, in a way that ensures that account holders are generally prohibited from:

    a. Passing information to unauthorized individuals;
    b. Inappropriately downloading or saving information;
    c. Inappropriately passing information to other Information Resource components;
    d. Sharing account information or otherwise granting their account privileges to others;
    e. Changing security attributes to data, Information Resources, or Information Resource components;
    f. Changing security attributes for newly created data or Information Resources; or
    g. Changing how access control is governed.

    Notwithstanding the foregoing, Owners may define privileged accounts which do permit some or all of the above if business requirements warrant.

ii. Assigning Accounts

Information Resource Owners are responsible for developing, documenting, implementing, and auditing the processes for assigning Roles and accounts. These processes must meet the following requirements:

1. **Documented Process:** Owners must ensure that there is a documented process for approving, creating, modifying, monitoring, and terminating accounts and/or Roles in the Information Resource. Such process must account for:

    a. Defining who can approve the creation of new Roles and types of accounts;
    b. Defining who can approve the creation of new accounts for individuals, modifying existing accounts, and terminating accounts;

c. Defining how monitoring of accounts in and access to the Information Resource occurs; and
d. Defining the conditions under which accounts and Roles can be created, enabled, modified, disabled, and/or removed.

In addition, the process should identify the roles of one or more individuals responsible for approving, administering, monitoring, and terminating access to the Information Resource. The individual(s) must be readily identifiable upon request. If the individual(s) are not, that role will default to the applicable ACIO.

2. **Change Documentation:** With respect to account creation, modification, and termination, Owners must ensure that they receive appropriate and timely information to support a change with an account. It is the shared responsibility of Owners and the individuals best suited to know when an account should be created, changed, or decommissioned. Such individuals may include the end user, the end user's manager (if applicable), the end user's organization (if a third party), human resources, and others. Owners should determine what information sources are most appropriate to support account determinations and coordinate appropriately to receive that data. Account creation, modification, and termination cannot occur spontaneously and must be (a) supported by request documentation; and (b) recorded when such action is taken.

3. **Least Privilege with Multiple Accounts:** Some individuals may have different Roles with respect to the Information Resource and, therefore, multiple different sets of access rights. Owners should ensure that individuals accessing the Information Resource utilize the account or access rights associated with the Role being performed. For example, if an individual is both an administrator and developer for an Information Resource (where they have greater access rights as an administrator), that individual must only use the administrator access for their administrator Role and not for their developer role. Users are also responsible for ensuring that they do not misuse their more privileged accounts to perform work inappropriately in a Role for which they do not require a heightened level of access. Under no circumstances may a user access or fulfill a non-privileged Role with a privileged account. All activities undertaken with a Privileged account must be logged, and such logs either (a) shared automatically with EHS log-correlation service; or (b) maintained for at least 180 days.

4. **Identification & Authorization:** All Information Resources must require identification and authorization procedures for users to access the Information Resource. Access to Information Resources must require controls such as user credentialing and passwords meeting EOTSS and EOHHS standards. For legacy Information Resources not requiring identification and authorization procedures, a supplemental security plan must be provided which explains why user actions do not require

identification and authorization and which demonstrates compensating controls for user authentication.

5. **Central Identity Management:** Wherever possible, Information Systems shall be designed and implemented to use central identity management services (IDM) provided by EOHHS or the Commonwealth, such as Active Directory, LDAP, or web-based authentication protocol. Owners are free to use groups/roles defined in the IDM system, or to use IDM only to authenticate users, managing and assigning roles entirely within their Information System.

6. **Logging of Identification Attempts:** Every login attempt, whether successful or rejected, and whether or not using a central identity management service, must be logged. Wherever possible, these logs must be shared automatically with EOHHS log-correlation services, such as SolarWinds, and unless such log forwarding is in place, Information System Owners are responsible for maintaining the identification logs for at least 180 days. Wherever possible, these logs must include source IP address or other source-identifying information.

iii. *Access to Information and Data Management*

Information Resource Owners are responsible for ensuring appropriate access to information and management of the data in their Information Resource. Those Owners must ensure implementation of the following requirements when managing data within their Information System:

1. **Information Sharing:** Information within an Information Resource should not be shared outside of that Information Resource unless the data recipient abides by the requirements outlined and referenced in these *EOHHS Enterprise Information Security Standards*. With respect to determinations in the EOHHS Environment, the EOHHS Security Office is undertaking application risk assessments and gap analyses. Consequently, the EOHHS Security Office has determined that EOHHS is making progress toward a generally effective control environment. As such, information sharing within EOHHS and among EOHHS Information Resources is deemed appropriate based on information security considerations. Owners must still take care to ensure appropriate custody of their information. Owners must continue to ensure that sharing of data external to EOHHS is appropriately evaluated against these standards, documented, authorized, and supported by written agreement holding external parties to at least the same standards required of EOHHS, including compliance with relevant Third Party Agreements.

2. **Protect Data Transmission:** Owners must enforce appropriate control over the transmission mechanisms for data. Some data must be encrypted before being transmitted outside an Information System, outside the EOHHS Environment, or outside the MAGNet environment. When

transmitting data outside of the EOHHS Environment or interfacing with an Information Resource outside of the EOHHS Environment, Owners must establish and document rules and procedures governing data transmission, processing, and storage. See *Section XVI, System and Communications* for more information.

3. **Oversee and Manage Authorizations:** Owners must also facilitate information sharing by maintaining oversight of Information Resources. Authorized administrators of access must determine whether access to its Information Resources is appropriate, based on but not limited to, the user's roles, business justifications and other standards consistent with those outlined herein. When applicable, Owners may employ either automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

4. **Previous Logons:** Owners must ensure that the Information Resource notifies the user, upon successful logon and/or access to the system, of the date and time of the last successful logon and/or access.

5. **Concurrent Sessions:** Owners must ensure that the Information Resource limits the number of concurrent sessions for each Role and account to one concurrent session, unless required by business, programmatic, or technical need. For any account, role, or Information Resource that allows multiple concurrent sessions, Information Resource Owners must (a) document why this is allowed; and (b) ensure that auditable events (including successful logins, re-authorizations, file additions/modifications/deletions, and changes to security attributes) are traceable to a specific session.

6. **Session Time-Out:** All Information Systems must automatically terminate a user's session (timeout) and conceal or remove information displayed on-screen after no more than 15 minutes of user inactivity. Upon session termination, the user must be required to reenter credentials to reestablish access to the Information System.

7. **Protect Physical Information Resources:** Owners must develop and enforce policies governing physical copies of data, including practices for the creation and distribution of physical copies of sensitive data, consistent with the Secretary of State's Record Retention Schedule. Access to physical Information Resources must be controlled based upon requirements provided by the Business Owner. If physical copies are required, Owners must ensure that they are maintained in a locked and secure environment accessible by key, badge swipe, PIN-entry pad, guard, or other authorization mechanism. Paper documents containing sensitive information may not be left unattended in the open where they can be easily taken. If electronic sensitive information is printed or otherwise converted into paper-based sensitive information, it must be printed to a non-publicly-accessible location and must be picked up immediately. Sensitive information in

physical Information Resources may not be left unattended, especially in public spaces or shared office settings. Owners must be cognizant of more restrictive compliance requirements under various Third Party Agreements, depending on the type of data contained within an Information System.

8. **Minimize Duplication of Electronic Information:** Owners must restrict the creation of unnecessary or duplicative collections of sensitive information and ensure that non-authoritative electronic copies of Information Resources are securely deleted or destroyed as soon as they are no longer needed. Such electronic files should never be stored locally on a user's computer or on shared drives, calendars, collaborative tools, external parties' systems, or anywhere on the internet without prior authorization.

9. **Control the Release of Information:** Prior to releasing information pursuant to a public records request, litigation, or other similar request for data, Owners must engage trained EOHHS staff who are authorized to post information onto a public-facing system or application or release data to the requesting third party. These trained individuals must review the proposed content to ensure that the proposed release does not contain nonpublic information, and if it does, remove or redact such information such that it cannot be recovered from the publicly released information.

10. **Automate Key Account-Management Practices:** Within one (1) calendar year of the issuance of this Document, Owners must certify and demonstrate that the following account management functionality has been automated:

    a. Information Resource account management – this can include measures like automated emails notifying Owners when users are terminated or their roles change, necessitating a change in their account, monitoring of account usage, automated alerts around atypical account usage, etc.
    b. Automated removal of any temporary accounts, which also includes any "emergency" accounts that may be created.
    c. Automatic disabling of Information Resource accounts that are inactive for 60 days or more and that meet other criteria, defined by the Owner, for account inactivity.
    d. Automatic auditing of account creation; modification; enabling, disabling, and removal action. Additionally, Information Resource rules must be created to distinguish between appropriate and inappropriate action and which will be used to automatically notify the Owners of inappropriate actions.
    e. Automatic logging and auditing of all privileged account activity, as well as the execution of privileged functions.
    f. Automatic prevention of non-privileged users from executing privileged functions. This should include the inability to circumvent, disable, or otherwise modify systems and functionality designed to

protect an Information Resource from modification, improper access, other malicious activity, and accidental harm.

11. **Data Mining Protections:** Within one (1) calendar year of the issuance of this Document, EOHHS must gauge the feasibility of, and employ if feasible, techniques to detect and prevent unauthorized data mining within Information Resources. These techniques should be designed to protect against users' unauthorized discovery and extraction of anomalies, patterns, and correlations within large data sets. They may include, but are not limited to: limiting the types of responses provided to database queries, limiting the allowed frequency of database queries to increase the work factor needed to extract or infer information from such databases, and notifying appropriate personnel when atypical database queries, accesses, or workloads occur.

iv. Access Reviews

In order to support and enforce these standards, Owners must ensure implementation of periodic access reviews for each of their Information Resources, taking into consideration the following standards:

1. **Personnel and Procedures:** Owners must ensure that sufficient personnel, procedures, and systems are in place to effectuate the access controls they adopt. Access enforcement will be based on the decisions of these authorized systems or individuals.

2. **Review Schedule:** Information Resource access must be reviewed and updated to reflect changes to operational, business, or IT requirements, based on the following schedules:

    a. **Annual Policy Review:** All Information Resource access policies and procedures must be reviewed at least yearly.
    b. **Annual Access Log Sampling:** A random sampling of Information Resource accounts must be reviewed (audited) at least once annually to ensure that access was (i) granted; and (ii) used appropriately. Such review must be designed to verify to a high degree of certainty that appropriate processes were followed and access grants were proper.
    c. **Unused Accounts:** Information Resource accounts must be reviewed (manually or automatically) at least every 60 days to determine whether or not such accounts are still actively in use. Accounts that have not been used within the past 60 days must at least be disabled to prevent access using that account. Managers should determine a timeline and process for documenting and re-enabling such disabled accounts based on criteria such as legitimate business need, including being notified by the account holder that they still require use of the account. Managers must determine a

timeline for deletion of disabled accounts that remain unused; however, such timeline may not exceed 180 days.

d. **After an Event:** Access control policies and procedures must be reviewed and updated for any Information System or Resource identified by the SCIO or appropriate ACIO as having been involved in an Event.

e. **As Needed:** Access control policies and procedures must be reviewed and updated as needed, as systems, roles, and personnel change.

v. Wireless and Remote Access

Owners of any Information Resource or Information System that is accessible via a wireless connection, from a mobile device, or from outside MAGNet (e.g., from the internet) ("remote availability") must establish controls for all such wireless, mobile, and remote access connections, including:

1. **Documented Authorization:** Documented usage restrictions, configuration requirements, and procedural guidance must be put into place before making the system remotely available, including per-user and per-device authorization processes to be completed prior to granting remote or wireless access.

2. **Minimum Necessary Amount of Wireless, Mobile Device, and Remote Access:** Access to wireless, mobile, and remote-access connections must be limited to the minimum amount necessary required to accomplish the authorized function. Instances in which remote users are granted access to privileged data must be documented with the business justification for the level of access.

3. **Monitoring:** Manual and/or automated processes that manage, monitor and track all remote accesses through audit logs and network access control points.

VII. AUDIT AND ACCOUNTABILITY

a. Purpose and Introduction

In support of access control monitoring and ensuring the confidentiality, integrity, and availability of Information Resources, Owners must ensure that they are able to assess and verify who accessed what with respect to their Information Resources. The controls outlined herein are predominately targeted at Information Systems, but physical Information Resources should be similarly safeguarded to the extent feasible.

b. Policy Statement

All EOHHS Information Resources must have records for access to those resources managed and reviewed by Owners to ensure only appropriate and authorized access to Information

Resources occurs. Information Systems must generate logs which are capable of being absorbed by Commonwealth and EOHHS enterprise logging tools. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Audit and Accountability Standards

i. Audit Events

At a minimum, records for access to information Resources must identify:

1. Who accessed the Information Resource,
2. When the Information Resource was accessed,
3. What was accessed,
4. Whether or not data was taken (appropriately or inappropriately),
5. Whether or not any modification was made (for Information Systems), and
6. From where the access occurred (for Information Systems, if applicable).

These six pieces of information will provide a sufficient baseline for Information Resource Owners and the EOHHS Security Office to determine if improper access was made to an Information Resource and its data.

Owners must also determine what events will trigger automated alerts. Some of those events are outlined in *Section VI, Access Controls.* At a minimum, Owners must identify rules and methods for identifying the following events:

1. Disruption of Service (DOS) and Distributed Disruption of Service (DDOS) attacks;
2. Brute forcing passwords through excessive log-on attempts; and
3. Unauthorized exfiltration or access of data through indicators like file transfer size or volume of access, timing, irregular account usage, and other indicators.

Owners must also implement active monitoring for all administrative or otherwise privileged accounts which permit read access to all data in an Information System or modify access to some or all of the Information System.

Owners must develop such rules as soon as reasonably practicable, but no later than: 1) the EOHHS Security Office requests such information when implementing aggregated logging for existing Information Systems or 2) upon deployment of a new Information System to production. These events and audit rules must be reviewed and confirmed or updated annually to ensure new perceived threats are appropriately monitored.

Owners must ensure that all audit logs contain a timestamp for creation of the log of the event. All such logs must be recorded in Eastern Standard Time.

ii. *Storage Capacity and Review*

The EOHHS Security Office will only maintain audit logs in an aggregated logging system for events that generate an alert and will maintain such records for sixty (60) days. All other audit logs will be maintained on an as-needed basis and the oldest audit records which have not generated an alert will be deleted on an as-needed basis to free storage.

The EOHHS Security Office will perform an initial review of all alerts to ensure that the alert is genuine. In the event it is, the alert will be forwarded immediately to the Owners of the Information System generating the alert. The EOHHS Security Office will also mobilize its forensic and incident response units to address any potential malicious activity. If appropriate, the EOHHS Security Office will also report incidents to EOTSS pursuant to *Section XI, Incident Response and Security Incident Response Team*.

Owners are encouraged, but not required to, keep logs for longer. In the event an application has not been ingested into an aggregated logging system, within one (1) year of promulgation of these *EOHHS Enterprise Information Security Standards* Owners must produce, review, and store logs as outlined in this *Section VII, Audit and Accountability* and produce a copy of events that generate an alert to the EOHHS Security Office within twenty four (24) hours of generation of the alert for review and analysis.

iii. *Audit System Integrity and Failures*

Audit logging systems employed in the EOHHS Environment must be developed consistently with these standards to assure the integrity of data and security of that system. Access should be provided consistent with the principles of least access. Audit logging systems must also be monitored to verify the continued integrity of generated audit files and events. Such logging must be performed in a way that review of any audit log does not modify the original content or time ordering of those logs. In the event an audit logging system is compromised, an alert must be generated notifying the Owner of such event. In the event an audit logging system fails, the audit logging system should be stopped, flushed, the source of the failure identified and repaired, and then restarted.

iv. *Additional Requirements for Systems Accessing Internal Revenue Service Federal Tax Information*

Owners are responsible for developing procedures defining access requirements and protection of audit information among external organizations when audit information is transmitted across agency boundaries. This requirement applies to outsourced hosting with data centers or cloud providers.

VIII. INVENTORY AND CLASSIFICATION

a. Purpose

The purpose of this Document is to outline both the need and the method for carrying out an inventory of EOHHS's applications and information. This Document is intended to satisfy Steps 1, "Categorize Information Systems" of the National Institute of Standards and Technology ("NIST") Risk Management Framework Security Lifecycle.[2] Furthermore, the processes outlined herein was drafted to conform to the precepts outlined in Federal Information Processing Standards ("FIPS") Publication ("Pub") 199, *Standards for Security Categorization of Federal Information and Information Systems* and NIST SP 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*.

FIPS Pub 199 outlines that an information system inventory and classification is necessary to mitigate the potential impact of a loss of confidentiality, integrity, or availability. For clarification:

i. A loss of confidentiality is defined as, "the unauthorized disclosure of information."[3]
ii. A loss of integrity is defined as "the unauthorized modification or destruction of information."[4]
iii. A loss of availability is defined as "the disruption of access to or use of information or an information system."[5]

The Security Office has been tasked with preserving the confidentiality, integrity, and availability of all data used or maintained by the Secretariat. It will accomplish that goal through the implementation of administrative, physical, and technical safeguards. The exercise outlined in this Document is the critical foundational step to implementing such safeguards with respect to Information System resources. It represents the first step toward compliance with requirements imposed by law, agreement, or otherwise.

The information and system classification serves two purposes. First, it makes EOHHS aware of what data is in use, maintained or transmitted and where that occurs. Second, it is designed to direct the implementation of controls that have been determined to reduce the likelihood of a loss of confidentiality, integrity, or availability of EOHHS data. This is one of many tools that will be used to safeguard EOHHS data. It should, however, be noted that these tools will not completely prevent the loss of confidentiality, integrity, or availability of EOHHS data and that constant vigilance should be exercised to mitigate threats to EOHHS data.

---

[2] National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013), at 8.
[3] Federal Information Processing Standards ("FIPS") Publication ("Pub") 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), at 2.
[4] *Id.*
[5] *Id.*

While this *Section VIII, Inventory and Classification* is drafted with a focus to classifying and inventorying Information Systems, the process outlined herein can (and arguably should) be applied to all data the EOHHS enterprise in whatever form it exists and to all processes which utilize data.

b. Policy

All Information Systems in the EOHHS Environment shall be appropriately identified and classified.

EOHHS will accomplish this requirement by ensuring that a Form is completed for all Information Systems. Based on the contents of the Form, the Security Office will assign a classification to the Information System for the purpose of applying appropriate security controls to the Information System to help ensure the preservation of the confidentiality, integrity, and availability of the information contained therein. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Information System Inventory and Data Inventory Standards

The Information System and Data Inventory portion of this Document is designed to provide an overview of Information System functionality, interconnections between a System and other Systems, and types of data contained in a System. This process is generally started by using one of the Forms.

The following process should be followed for every Information System:

i. For all current Information Systems for which a Form has not been completed, the EOHHS Security Office should identify the appropriate Owner to fill out the Form for a specific Information System. If this is a new Information System, the Owner should fill out and update the Form, as appropriate, during system design and submit it to the Security Office.
ii. In the event an Owner identifies that the Form is inappropriate to catalogue information about the Information System, the EOHHS Security Office should work with that Owner to gather the types of information being solicited by the Form (e.g.: data in the Information System, data flows, Information System architecture, vendor access, etc.).
iii. The Owner should fill out the Form, making sure to respond to every applicable question and/or field. All Information Systems in the EOHHS Environment must have a Form completed for them, without exception. It is also critical that the Form reflect the most true and accurate version of information about an Information System.
iv. The EOHHS Security Office and program staff may later determine that a different scope of controls should apply to a system than other than as indicated in the Form due to factors not reflected in the form. However, such a determination will be impossible without the Form being filled out completely and as accurately as possible about an Information System.
v. After receipt of the Form, the EOHHS Security Office will review the Form and work with the Owner to address any outstanding questions.

vi. The EOHHS Security Office will then verify that for the interfacing system table in Question 7 of the Form that every system listed has a completed Form. If not, then the EOHHS Security Office will pursue completion of a Form for the system(s) which lack completed Forms.

vii. The EOHHS Security Office will then assign a categorization level to the system, as outlined in the Information System, Process, and Data Classification Standards immediately below.

d. Information System, Process, and Data Classification Standards

After determining the function and data contained in an Information System, the EOHHS Security Office will assign a classification to that system based on the function and data. The classification will operate as a recommendation of the level of administrative, physical, and technical security controls that the EOHHS Security Office believes applies to the system.

In order to assign a classification to specific information or an Information System, the EOHHS Security Office will use the following matrix:

Data Classification information type/system = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}

Impact, as used in the matrix, is the potential impact to a system of a loss of confidentiality, integrity, or availability, which can be one of the four following categories:

i. *No Impact* or *Not Applicable (NA)*: this would apply if one of the factors of confidentiality, integrity, or availability do not apply to the data and/or system. For example, a database of public records which is itself a public record would reflect that confidentiality is not applicable.

When applied to determining the impact of a loss of confidentiality, this impact level corresponds to "Low Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[6]

ii. *Low*: As defined by FIPS Pub 199:

The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor

[6] *Enterprise Information Security Standards: Data Classification*, EOTSS, Aug. 25, 2017, http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-information-security-standards.html.

damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.[7]

When applied to determining the impact of a loss of confidentiality, this impact level most closely corresponds to "Medium Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[8]

iii. *Moderate*: As defined by FIPS Pub 199:

The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.[9]

When applied to determining the impact of a loss of confidentiality, this impact level most closely corresponds to "High Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[10]

iv. *High*: As defined by FIPS Pub 199:

The loss of confidentiality, integrity, or availability could be expected to have a severe or **catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening

[7] *Id*. (emphasis in original).
[8] *See Supra* note 6.
[9] See Supra note 7 (emphasis in original).
[10] *See Supra* note 6.

injuries.[11]

When applied to determining the impact of a loss of confidentiality, this impact level would also constitute "High Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[12]

e. The below process will be followed to appropriately classify each Information System in the EOHHS Environment:

i. The Security Office will make an initial assessment of impact level for confidentiality, integrity, and availability based on the data provided in the Form.

ii. The Security Office will then assign an initial classification to the Information System applying the high-watermark principle: the highest impact level assigned to the system will control the overall impact level of the system. Additionally, the Security Office may assign classifications to different stages of an Information System or Process.

Example 1: EOHHS is conducting a procurement. While the procurement team is deliberating, the procurement team group score may be classified as follows:

DC_{scores} = {(**confidentiality**, *moderate*), (**integrity**, *low*), (**availability**, *low*)}
DC_{scores} = moderate

At the conclusion of deliberations, a vendor is selected and the other vendors are made aware of the selection. Any of the vendors may request a debriefing and the procurement team group score is considered a public record. At that time, the score may be classified as follows:

DC_{scores} = {(**confidentiality**, *NA*), (**integrity**, *low*), (**availability**, *moderate*)}
DC_{scores} = moderate

After the period for debriefing has expired, the score is still public records, but the urgency of maintaining such score might be determined to be lower. As such, the score may be classified as follows:

DC_{scores} = {(**confidentiality**, *NA*), (**integrity**, *low*), (**availability**, *low*)}
DC_{scores} = low

Consequently, until the predetermined criteria are met to change the classification (here, the expiration of the debriefing period) the data in the foregoing example should be considered "moderate" impact. Notably, it is considered moderate for different reasons. Prior to selection it is considered confidential, but after selection

[11] *See Supra* note 7, at 3 (emphasis in original).
[12] *See Supra* note 6.

it needs to be available for distribution to respondents. However, after the occurrence of such predetermined criteria the data in the foregoing example may be considered "low" impact because it is neither confidential, nor does it urgently need to be made available.

iii. The Security Office will then report its initial data classification to the Information System Owner. The Information System Owner may review the data classification and suggest modifications based on factors including:

1. Legal or statutory requirements,
2. Factors that may impact the assessment of confidentiality, integrity, or availability of information (e.g.: negative impacts from malicious use of data, reduction of public confidence in EOHHS if the data were inaccurate, etc.)[13]
3. Additional situational considerations (similar to those demonstrated in Example 1, above) or organizational considerations (e.g.: considerations of agency mission, etc.)[14]
4. Data sharing, and
5. Use of the data.

Such modifications will typically increase the initial classification of the Information System or data (or component impacts), but in some cases may justify lowering the initial classification.

iv. After discussion with the Information System Owner, the Security Office will assign a final data classification and categorization to the Information System. The Security Office will report such final data classification to the Information System Owner.

v. The final data classification will serve as the basis for the (1) imposition of security controls on the Information System and (2) the security controls against which the Information System will be audited.

IX. ASSESSMENT AND MONITORING

a. Purpose and Introduction

It is impossible to safeguard an environment where the issues, gaps and vdc xdeficiencies of that environment are unknown. Beginning in September, 2017, the EOHHS Security Office implemented a continuous monitoring program focusing on assessments of information systems, facilities, and operations in the EOHHS Environment.

The purpose of these assessments is to develop a baseline for the implementation of physical, technical, and administrative safeguards for Information Systems designed to

[13] *See generally*, NIST SP 800-60, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," at 20-23.
[14] *See generally, Id.* at 23-24.

protect the confidentiality, integrity, and availability of information across EOHHS. The assessments are based on the controls outlined in NIST SP 800-53, r4.

These assessments rely on the efforts of innumerable EOHHS staff, the EOHHS Security Office, and external vendors. While the EOHHS Security Office strives to completely address the needs of the EOHHS enterprise, the sheer size, magnitude and complexity of the enterprise may impact the ability to do that. Owners are encouraged to perform self-assessments using the mechanisms outlined herein. Copies of all assessments should be provided to the EOHHS Security Office as soon as reasonably practicable.

Assessments performed by the EOHHS Security Office are effectively independent. The Security Office creates standards for the EOHHS enterprise, but is not responsible for enforcement or implementation of those standards. Additionally, because members of the EOHHS Security Office do not report directly to ACIOs or Agencies, those entities will be organizationally unable to impact the impartiality of the EOHHS Security Office.

b. Policy Statement

All EOHHS Information Systems must undergo assessments based on the controls outlined in NIST SP 800-53, r4. Schedules for such assessments will be determined as further outlined in this *Section VIII, Assessment, Authorization, and Monitoring*. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Assessment, Authorization, and Monitoring Standards

i. Assessment Process

1. The EOHHS Security Office will work with Agencies, the ACIOs and CISO to determine Secretariat priority for assessments to be conducted by the EOHHS Security Office. The EOHHS Security Office shall maintain a list of assessments and indicate progress of such assessments for the purpose of reporting progress on such assessments. Information Systems identified for assessment will be chosen based on criteria outlined in the Form.

2. To initiate an assessment, the EOHHS Security Office will conduct a kickoff meeting with application support staff, facility management, or Agency management. Typically, an assessment questionnaire is provided to staff immediately prior to, at, or after this meeting.

   The assessment questionnaires are designed to provide a comprehensive view of the EOHHS, Agency, and application environments based on a review of the NIST SP 800-53, r4 standards.

3. After the kickoff meeting, the Respondents will complete the questionnaire and return it to the EOHHS Security Office for review. In the event the questionnaire is deemed incomplete based on a lack of detail in the responses or if it is missing supporting documentation, the EOHHS Security

Office will engage in an iterative process with Respondents to reasonably complete the assessment questionnaire.

4. Upon completion of the assessment questionnaire, the EOHHS Security Office will aggregate the responses and supporting documentation of the available assessment responses of: EOHHS, Agency, facility, and application. These aggregate reports can take the following representative forms:

    a. Agency and/or Facility Security Plans,
    b. HIPAA Security Risk Assessments,
    c. System Security Plans,
    d. Other forms as required or requested by the Agency

5. Upon completion of an aggregate report, the EOHHS Security Office will review the narrative and supporting documentation in the aggregate report against the NIST SP 800-53, r4 standards. Any perceived deficiencies or gaps will be recorded in a POA&M in a format that identifies, at a minimum:

    a. The kind of gap or defect;
    b. The impact of the gap or defect;
    c. The risk posed by the gap or defect, including the likelihood or magnitude of harm;
    d. Suggested remediation or mitigation of the gap or defect; and
    e. Agreed-upon timelines for remediation of the gap or defect based on the risk of the gap or defect and the priority of remediation and/or resource commitment by the Agency.

6. The EOHHS Security Office will monitor progress on the POA&M with the Respondents on at least a quarterly basis.

7. The EOHHS Security Office will revalidate its assessments on a triennial basis by default. It will revalidate assessments on a biennial basis for APD-funded systems.

ii. *Interconnection Agreements*

Prior to sharing data in any form, internal and external Agencies typically enter into Information Sharing Agreements (ISAs) or other Third Party Agreements with trading partners which outline the security and privacy requirements of any shared data. At a minimum, all ISAs entered into by EOHHS or its Agencies with an entity external to EOHHS must include a reference to compliance with applicable NIST SP 800-53 standards. Internal interconnections are deemed to be authorized based on conformance with these EOHHS Enterprise Information Security Standards. Such interconnections will be recorded based on the Form.

iii. *Monitoring*

The assessment program outlined in this *Section IX, Assessment and Monitoring* is

only one component of the EOHHS continuous monitoring program. The results of those assessments will be correlated with the information generated in *Section VIII, Inventory and Classification*; *Section VII, Audit and Accountability*; *Section X, Authorization to Operate and Operational Risk Assessment*; and any available vulnerability assessments or penetration tests generated by Information System Owners, EOHHS, and EOTSS to ensure that Information Resources are adequately protected on an ongoing basis. The specifics of this continuous monitoring program may be documented in separate desk level procedures. This information will be used by the EOHHS Security Office, including by its forensic and incident response units, to safeguard the environment and to identify and address any potential malicious activity. If appropriate, the EOHHS Security Office will also report this information to EOTSS pursuant to *Section XI, Incident Response and Security Incident Response Team*.

X. AUTHORIZATION TO OPERATE AND OPERATIONAL RISK ASSESSMENT

a. Purpose

The purpose of this section is to outline the process(es) needed to request an Authorization to Operate (ATO) or an Operational Risk Assessment which would assist with promoting a System from Development or Testing to Production where that Information System might not fully meet Commonwealth, EOHHS, and/or an Agency's information security controls. This promotion to Production with a security variance is accomplished in a safe and well-managed fashion by documenting and recording the variance, the vulnerability, the risk to proceed, and any remediation steps. This documentation will provide the relevant decision maker with facts necessary to make reasonably informed decisions about introducing security vulnerabilities into the EOHHS Environment.

Both the ATO and the Operational Risk Assessment are tools that identify the types and severity of Risks that a System as-designed poses to the data it contains and to the broader EOHHS Environment. The ATO is the tool by which business and technical stakeholders for a System can sign off on deploying a new System to production with security vulnerabilities. The Operational Risk Assessment is the tool by which business and technical stakeholders for a System can sign off on promoting changes to a currently extant system to production with security vulnerabilities, assist with tracking and updating ongoing vulnerabilities, and address newly discovered vulnerabilities.

Risk is something that could potentially result in an adverse situation for the Commonwealth. Reputational damage, loss of PHI/PII data, or data corruption are typical outcomes when Risk is taken without additional considerations on how it might be avoided, mitigated or accepted. When Risk appears and/or is identified, it should be carefully reviewed and options researched to assist with any decisions that are made.

Prior to making the determination to deploy a System into Production or implement code changes with known Risks or security faults, the Information System decision maker should perform adequate due diligence, such as obtaining an assessment for operating with Risks by contacting the Security Office for assistance with identification and cataloguing such risks. The Security Office will assist with gathering the options and discuss with Owners and

other stakeholders to help make the risks more manageable.

The Authority to Operate (ATO) permits Agency personnel to understand and accept the Risk of the status of the System at the time of deployment into Production. The sign off will need to come from the Agency's ACIO and corresponding business contact.

An Operation Risk Assessment is intended to document potential risks at the time of deployment of a System to Production or when enhancements, fixes or feature changes are made to an existing environment. The resolution or mitigation of the risks should be documented as part of sign off to ensure they will be addressed. The Operational Risk Assessment will also serve as a documentation and justification document for Auditors and other external third parties to demonstrate a high level of sophistication and thoughtfulness with respect to security vulnerabilities.

An ATO will usually be paired with the Operational Risk Assessment however the Operational Risk Assessment can be completed without an ATO for systems already in Production.

b. Policy

Any System in the EOHHS Environment that has any known Risks when deployed to Production must be appropriately documented via an ATO and/or Operational Risk Assessment. Appropriate steps to address or mitigate a Risk should be considered and done as a function of the development process. In the event that remediation or mitigation measures are not scheduled for timely deployment or change, the ATO and/or Operational Risk Assessment will be elevated for enhanced review. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Authority to Operate and Operational Risk Assessment Standards

The ATO and Operational Risk Assessment processes generally start with an Owner contacting the System and Support Desk and filling out a Project Intake Form to engage the EOHHS Security Office to review the integrity of their System. However, if the EOHHS Security Office has been engaged during the procurement and design process for the System and/or solution, then a Project Intake Form will not be required (as one should have been completed for the overall effort). Both processes follow the same general steps and have been outlined as a unified process with exceptions noted, as applicable, below.

After a Project Intake Form is completed, the ATO process continues when the EOHHS Security Office identifies from the Project Intake form or circumstances surrounding the System implementation process that the Owner will bring a new System online with vulnerabilities. Similarly, the Operational Risk Assessment process continues when the EOHHS Security Office identifies from the Project Intake form or otherwise that the Owner plans to promote System changes to Production which may include vulnerabilities. Where possible, if the Owner anticipates that one or more aspects of the System will not conform to applicable information security requirements or industry best security practices, the Owner should identify what they believe to not conform.

Upon identification that vulnerabilities exist, the EOHHS Security Office will follow the following process:

i. The EOHHS Security Office will investigate how the Owner determined that a System needs to be deployed to Production with security vulnerabilities. This investigation will include, but are not limited to:

    1. A review of potential mitigating steps that could be undertaken, such as a workaround or compensating control that will make up for the security vulnerability; and
    2. A review of the completed and/or updated Gap Analysis Questionnaire. *See* Gap Analysis Questionnaire Process (in process, please contact the EOHHS Security Office for more Information).

ii. The EOHHS Security Office will review the Gap Analysis Questionnaire with the Owner to identify and confirm the vulnerabilities sought to be introduced into Production.

iii. The EOHHS Security Office will draft a Memorandum with the appropriate information for the System at issue. The Gap Analysis will be attached to the ATO and be incorporated therein as of the date of Approval. Based on the vulnerabilities identified, the EOHHS Security Office will list the vulnerabilities and Risks, providing the following information in the Memorandum:

    1. Title of Vulnerability/Risk being captured.
    2. Overview of Vulnerability/Risk being captured.
    3. Recommendations for remediation, if any (including workarounds and compensating controls) and how they might be applied. The EOHHS Security Office may also provide detailed recommendations how they would help mitigate the risk.
    4. Summation of the rating of the Vulnerability/Risk. The Risk will be rated using the standards outlined in the EOTSS policy titled "Information Security Risk Management Standard", IS.010. Vulnerabilities will ultimately be assigned a rating of "Low", "Moderate", "High" and "Critical".
    5. An aggregate risk rating for the System based on the individual risk ratings. If the aggregate risk rating is found to be a High or Critical, the EOHHS Security Office will inform the Owner and contact the EOHHS Risk Governance Team to determine next steps with respect to ongoing management of the System's ongoing security posture.

        Note: In the event the aggregate Risks posed by the System will impact data from Secretariats or entities external to EOHHS, the Risks will be escalated to the EOTSS Risk Governance Committee.

iv. The EOHHS Security Office will review the Memorandum with the Owner to mitigate, to the extent possible, any outstanding Risks. While the EOHHS Security Office recommends that Owners attempt to mitigate all Risks, the EOHHS Security Office has determined that the following constitutes generically acceptable levels of

Risk:

Low	No more than six (6)
Moderate	No more than two (2)
High	None
Critical	None

Although the aforementioned levels of Risk are considered generally acceptable, specific instances of Risk may not be.

v. In the event the EOHHS Security Office and Owner are unable to bring the number of outstanding Risks below the levels set as acceptable, or in the event the System has one or more "High" or "Critical" Risks, the EOHHS Security Office will convene the EOHHS Risk Governance Team and escalate the Memorandum to them. The EOHHS Risk Governance Team will review the Memorandum and attempt to make recommendations for options to mitigate some of the more significant Risks to the System.

Note: In the event the Risks posed by the System will impact data from Secretariats or entities external to EOHHS, the Risks will be escalated to the EOTSS Risk Governance Committee.

vi. After reviewing the Memorandum with the Owner and/or the EOHHS Risk Governance Team (or the EOTSS Risk Governance Committee) and receiving approval from either the Owner or the EOHHS Risk Governance Team, the System or its modifications may be promoted to Production. Acceptance should be written, but may occur without written Acceptance in the following circumstances:

1. Promotion of the System to Production without signing the Memorandum, or;
2. Failure by the business and/or technical contact to sign the Memorandum thirty (30) days after: 1) the issuance of the Memorandum or 2) the conclusion of the Risk Governance Team reviewing the Memorandum, whichever is later.

vii. On an ongoing and periodic basis, the EOHHS Security Office will request updates from the Owner about progress to resolution of Risks and vulnerabilities. In the event the Owner is unable to demonstrate meaningful progress to resolution of Risks and vulnerabilities, the EOHHS Security Office will contact the EOHHS Risk Governance Team to determine next steps with respect to ongoing management of the System's ongoing security posture.

viii. By December 1, 2019, Agencies must provide a list of representative for the EOHHS Risk Governance Team that represent the following operational areas and can make decisions on behalf of the Agency with respect to deploying Systems into production with vulnerabilities:

1. Commissioner,
2. Chief Financial Officer,
3. Chief Operating Officer,
4. Agency Chief Information Officer, and
5. General Counsel

Agencies shall update such list on an annual basis, but no later than June 30 of the following year, or when an appointee no longer works for the Agency in the assigned capacity. The EOHHS Security Office will maintain such lists in order to escalate issues and seek approval for promoting vulnerabilities into Production.

XI. INCIDENT RESPONSE AND SECURITY INCIDENT RESPONSE TEAM

a. Purpose

Incident response plays a critical role in any modern enterprise: it provides a mechanism for identifying, stopping, and fixing to the best extent possible any event that could result in a loss of data at an organization. This function has become more critical than ever. Modern business technology has moved beyond its formative stages, where data was maintained and accessed only on desktops in a building. Smart phones, laptops and other portable devices have extended the electronic footprint beyond specific, well-defined physical locations, making information readily available on the go. The proliferated number of endpoints provides many points of entry into a network, which has resulted in an increase of both attempts and successful cyber-attacks from individuals, corporations and organizations looking to gain access to confidential or proprietary data. The complexity of mobile technology and modern interfaces further adds to the burden of ensuring communications and information is not compromised.

This *Section XI, Incident Response and Security Incident Response Team* ensures that an organized and repeatable response can be undertaken immediately when a Security Incident is reported. This Document provides clearly defined processes and procedures that the Security Office and its Security Incident Response Team (SIRT) will use to respond to Security Incidents and ensure that proper handling of the Security Incident and evidence thereof is maintained. The SIRT will investigate a Security Incident; attempt to determine root cause of the Security Incident; manage the Security Incident until it is mitigated, minimized, or stopped; and provide after-action assistance such as an after-action report and/or analysis and provide recommendations to increase security and training activities to mitigate risk on an ongoing basis.

This *Section XI, Incident Response and Security Incident Response Team* defines the minimum acceptable requirements at EOHHS for a Security Incident response. Agencies may have their own related documentation but may not undertake any action or documentation (explicitly identified as such or not) to supplant these standards or process. These standards and process are intended only to cover Incidents which result in impacts to the confidentiality, integrity or availability of data. These standards are not intended to cover incidents which cause physical unavailability of a site, such as because of damage to physical infrastructure, natural disaster, or other physical impacts. These standards are intended to work alongside a physical incident response plan to ensure resumption of data access as quickly as possible.

Additionally, Agencies may also have continuity of operations/business continuity plans in place. Those plans should be intended and designed to address impacts to business operations caused by unavailability of a location or resources. They should not deal with the underlying cause of the lack of access to data, which is the scope and purpose of these standards or a physical incident response plan.

Notwithstanding any statement in these *Enterprise Information Security Standards* to the contrary, while this *Section XI, Incident Response and Security Incident Response Team* activities relate to Agencies' privacy incident response activities, these standards are intended to work in conjunction with Agencies' privacy incident policies/procedures/protocol and should not be construed to replace or supersede those privacy documents. The EOHHS Security Office will make all efforts to appropriately collaborate with Agency privacy offices when a Security Incident arises.

In no event should any EOHHS staff member attempt to address a Security Incident themselves outside of the scope of this *Section XI, Incident Response and Security Incident Response Team.* Any EOHHS staff member that takes any action or inaction that exacerbates the duration, coverage, magnitude, impact or any other quality of an Incident, whether intentionally or unintentionally will be considered a malicious actor with respect to the Incident. In the event that any EOHHS staff is found to be a malicious actor with respect to an Incident, those staff may be disciplined. Such discipline may include limitation of or removal of rights to access Information Resources, suspension or termination of employment, or civil and criminal penalties such as fines and incarceration.

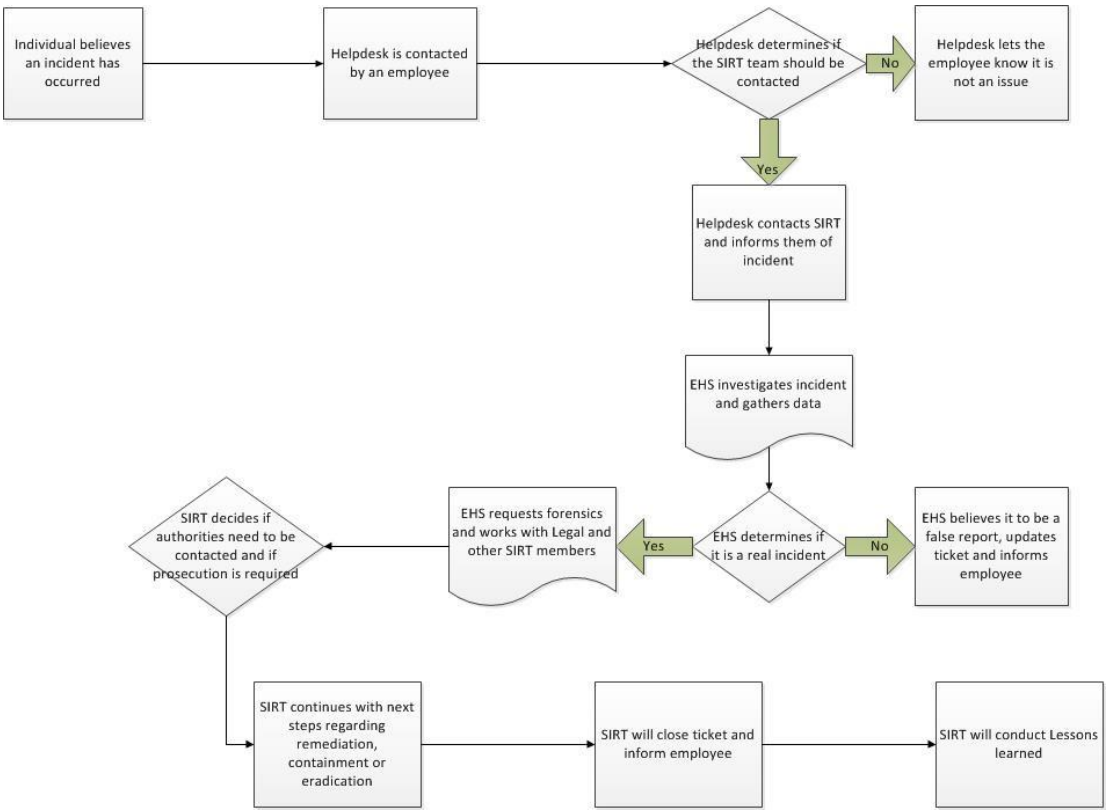
b. Policy

All Reportable Events must be reported, handled, and remediated pursuant to the terms of this *Section XI, Incident Response and Security Incident Response Team*. Agencies must designate individuals who may be contacted in the event of a Reportable Event and who are capable of serving on the SIRT until closure of the Reportable Event. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Incident Response and Security Incident Response Team Standards

i. Overview of Reportable Event Handling

The following chart outlines the workflow for how a Reportable Event will be addressed:



ii. Identification of Reportable Events

There are a number of ways that a Reportable Event may be identified. While it is impossible to list every possible situation or activity that may be or give rise to a Reportable Event, this document will strive to provide sufficient guidance to make Reportable Events readily identifiable. **As a rule, over report. When in doubt, report.** The EOHHS Security Office will help you identify a Reportable Event and will inform you if the event you reported was not, in fact, a Reportable Event.

Reportable Events fall into two different groups:

- Group 1: ongoing Security Incidents
- Group 2: events that demonstrate environmental weaknesses that could lead to a Security Incident and need to be fixed.

Group 1 is largely reactive. In a Security Incident, Information Resources have already been compromised either through confidential information being given to the wrong party thereby impacting the confidentiality of the data, being unavailable to the people who need them, or when the data is inaccurate such that people who need data are unable to get the right data. Therefore, in a Security Incident, damage has already been done to Information Resources or business processes. Addressing that damage involves stopping the spread and impact of the Security Incident (which could be a current or pending loss of data) and restoring the confidentiality, integrity, and availability of Information Resources as best as possible.

Some examples of Security Incidents are as follows:

- Loss of a mobile device(s) such as laptop, tablet or phone that is unencrypted
    - For encrypted devices, the System and Support Desk should be following their own lost device remediation plan which includes remote wiping of device
- Widespread malware/virus infection
- Confidential information disclosed, altered or destroyed
- Unauthorized changes to system hardware and/or software
- Unauthorized probing or scanning of Commonwealth systems or network
- Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks

Occurrence of nature which requires mobilization of the business continuity team Group 2, which convenes when Reportable Events might not rise to the level of a Security Incident, is largely preventative in nature. The best way to stop a Security Incident is to ensure it never happens. Therefore, the group of Reportable Events covered by this *Section XI, Incident Response and Security Incident Response Team* is broader than just Security Incidents. Reportable Events include any Event in the EOHHS Environment that highlights the potential for a Security Incident to occur. By including this group of Events in the definition of a Reportable Event, the EOHHS Security Office can work to prevent Security Incidents in the EOHHS Environment and/or minimize the potential damage from Security Incidents.

To provide a tangible example of what might constitute a Reportable Event, both of the following situations are Reportable Events:

- someone enters an EOHHS location and steals an EOHHS Information Resource (e.g.: pulling a computer off of a desk and walking out the door with it)
- someone enters an EOHHS location and steals personal property (e.g.: rummaging through peoples' personal effects to take wallets)

In the first situation described above, there is a loss of an EOHHS Information Resource and that Information Resource may also contain sensitive data. In that case, the Security Office has an important role in working with relevant parties to identify how the computer was taken, recover the computer and/ or recover or prevent the dissemination of the data, and ensure that the Security Incident does not reoccur in the future.

In the second situation described above, there is no indication that EOHHS Information Resources have been impacted. However, the situation demonstrates certain vulnerabilities in the environment that permitted the individual to enter an EOHHS location and the target of the theft could have been EOHHS Information Resources. Therefore, in an effort to safeguard EOHHS Information Resources, the latter Event, while not a Security Incident, is a Reportable Event that will be reviewed by the Security Office.

Some EOHHS operations groups use the term "incident" outside the scope of this *Section XI, Incident Response and Security Incident Response Team.* Therefore, such "incidents" are not within the scope of these standards, though they may be required to be reported under other processes. Examples of such "incidents" are:

- Network or server outages at a site unrelated to a DDOS or other attack/action from a third party
- Power outages at a site

Additionally, some Reportable Events which are required to be reported under this policy must also be reported under other policies, such as Agency Privacy Policies. Individuals reporting any Events under this *Section XI, Incident Response and Security Incident Response Team* must ensure that they appropriately report such Events to other groups as necessary.

iii. *Reporting a Reportable Event*

All Reportable Events must be reported to the EOHHS System and Support Desk immediately upon discovery. **You can contact the EOHHS System and Support Desk at (617) 994-5050 or at the email addresses available at http://eohhs-web.ehs.govt.state.ma.us/IT/agency-email-addresses.asp**. As time is of the essence during most Security Incidents, managers or Agencies shall not implement administrative processes that delay reporting of a Reportable Event and which may serve to exacerbate a Reportable Event. Examples of such administrative processes are internal programmatic, department and/or Agency reporting requirements and escalation prior to reporting the Reportable Event to the EOHHS System and Support Desk.

In some situations, a Reportable Event may constitute a Privacy Incident which is reportable to Agency legal counsel, privacy official or other designated contact under an Agency's privacy or security policy. In this case, you should report the Reportable Event to both the EOHHS System and Support Desk under this *Section XI, Incident Response and Security Incident Response Team* and to Agency legal counsel, privacy office or other appropriate official, who will cooperate with the SIRT in their response.

In some situations, a Reportable Event may also require contacting emergency services due to an immediate danger (e.g.: dialing 911 for police or fire). In the event a call to emergency services is necessary, notwithstanding the prior statement to call the EOHHS System and Support Desk first, the reporter shall first call emergency services and when the reporter is out of danger, call the EOHHS System and Support Desk.

The EOHHS System and Support Desk will then open a "Security Incident" ticket and assign it to the ENT.SEC.CSO queue.

iv. *Secretariat Incident Response Team*

Upon assignment of the "Security Incident" ticket to the ENT.SEC.CSO queue, the Security Office will review the ticket and may contact the submitter to determine whether or not the ticket describes a Reportable Event. If the ticket does not, then the Security Office will close the ticket. If the ticket does, then the Security Office will mobilize the core SIRT, composed of the following individuals from the Security Office with the following roles and responsibilities:

- Incident Response Lead / Coordinator - During resolution of the Reportable Event, the Incident Response Lead is tasked with project coordination and ensuring successful resolution and/or remediation of the Reportable Event. Activities in furtherance of those goals may include, but are not limited to: identifying the Reportable Event, triaging resolution of the Reportable Event, coordinating and liaising between relevant groups involved with resolving the Reportable Event, and engaging in appropriate closeout activities for the Reportable Event. When a Reportable Event is not underway, the Incident Response Lead will be responsible for improving EOHHS security; developing desk level procedures to ensure appropriate implementation of this *Section XI, Incident Response and Security Incident Response Team* with Agency stakeholders in order to appropriately address Reportable Events; working towards minimizing the occurrence of a Reportable Event; and working with groups throughout EOHHS to familiarize those groups with and test and operationalize the processes outlined in this *Section XI, Incident Response and Security Incident Response Team*.

In consultation with the Secretariat Security Liaisons and Forensic Analysts, the Incident Response Lead will identify the extent of the Reportable Event and make a determination if resolution of the Reportable Event requires mobilizing a broader SIRT or if the Security Office is able to resolve the Reportable Event. The conditions for mobilizing a broader SIRT will be outlined in relevant Security Office desk level procedures implementing the precepts of this *Section XI, Incident Response and Security Incident Response Team.*

In the event a broader SIRT is required:

1. Agencies must designate and provide to the EOHHS Security Office appropriate points of contact at the Agency who are able to direct on-the-ground identification, containment, and remediation efforts, if required, and secure staff participation and cooperation in identification, containment, and remediation. Agencies may designate whomever they wish, but the EOHHS Security Office recommends representatives from the following (and/or their delegates):

    - Agency Operations,
    - Finance,
    - Site and/or Office Managers,
    - Agency Legal,

- HR and Labor Relations,
- Agency Communications, and
- Agency Privacy Counsel and/or Privacy Officer (where applicable to the extent this is also a privacy incident).

2. EOHHS IT Operations must designate appropriate points of contact who are able to direct and implement on-the-ground identification, containment, and remediation efforts who should include the following:

   - IT Site Manager and/or Regional Operations Manager,
   - Server Administrators, and
   - Network Administrators.

   The SIRT has numerous purposes with respect to resolution of an incident. The SIRT can:

   a. effectively coordinate and communicate required actions for incident response and remediation,
   b. keep Agency and IT leadership updated about status of investigation and resolution of an incident,
   c. quickly course-correct management of investigation and remediation of an incident, and
   d. ensure all stakeholders are able to quickly and effectively remove any barriers to remediation of an incident.

   Within 30 days after the start of a state fiscal year, Agencies must designate the individuals who will participate in the Agency SIRT. Additionally, within 30 days after the start of a state fiscal year, EOHHS must designate the individuals who will participate in an EOHHS SIRT, should the need arise. EOHHS need not identify the IT Operations staff that will participate in a SIRT as the regional and/or office staff will assist with Incident response and remediation. The SIRT lists will be attached hereto as Attachment 9.

v. Reportable Event Handling – Overview

After the System and Support Desk opens a ticket and assigns it to the ENT.SEC.CSO queue:

1. The Incident Response Lead will review the ticket, contact the reporting employee and gather additional information to determine if a Reportable Event has, in fact, occurred. (Section XI(c)(vi)(1))
2. If it is not an incident and not a Reportable Event, the ticket is closed by the Incident Response Lead or sent back to the System and Support Desk to be addressed as not a Reportable Event, but an issue that needs to be addressed. If the ticket is closed, the requester will be notified by email.

3. If it is not an incident, but is a Reportable Event, the Incident Response Lead will perform appropriate follow-up with respect to investigation and data gathering, as described in Sections XI(c)(vi)(2) and XI(c)(vii) below.
4. If it is an incident, the Incident Response Lead will determine if it can be handled by the Security Office or if the SIRT must be assembled. The incident will then be managed as outlined further below.
5. The Security Office and/or SIRT investigates and gathers the data for the Reportable Event or incident. Forensics is performed if necessary to determine how the Reportable Event or incident started, has spread, and how best to contain the incident. There will also be a determination if the authorities need to be contacted (if not already contacted) and if additional legal action is required. (Section XI(c)(vii)(1))
    a. Because of the potential for further legal action, the utmost care must be maintained for documenting and preserving the chain of custody of materials to be used as evidence. The Security Office and SIRT should be observing and kept up to date with each transfer of custody of materials.
6. Once the path to remediation is determined, even if the start and spread of the incident has not been identified, the Security Office or SIRT will work towards remediation as expeditiously as possible while being mindful of the identification efforts. (Section XI(c)(vi)(2))
7. Once the Incident is remediated the SIRT will work towards supporting restoration of operations. (Section X.c.viii)
8. Additionally, once the incident is remediated, the SIRT will gather all supporting evidence and document its findings with respect to the incident response and management. The Security Office will maintain the document of record with respect to the incident. (Section X.c.viii)
    a. If the Incident is deemed HIGH IMPACT the report will be provided to the Risk Governance Committee.
    b. The Security Office shall use the documented findings to work towards remediating the identified vulnerabilities, improve its incident detection capabilities, and improve its response.

vi. Reportable Event Handling – Triaging, Identifying, and Investigating Attack Vector of the Reportable Event

Related Documents: *EOHHS Incident Chain of Custody Form, EOHHS Incident Evidence Form*

1. The Incident Response Lead will contact the individual who reported the Reportable Event or incident to gather additional details. Those details will be input into the EOHHS Incident Evidence Form and will include foundational information like:

    a. Affected application/website/hardware/software/business process.
    b. Is there any hardware/software affected? Servers or desktops as well as IP addresses should be recorded if this is a DDOS attack.

c. Attack vector, if known – for example, is this a phishing email that triggered the incident?
   A copy of the email should be procured and analyzed in a sandbox environment, if possible. All pertinent details about the email (sender, recipient, external link, etc.) should be recorded.
d. Necessary forensics tools should be identified (a list should be gathered of what is available for use)
e. Affected users. Who is affected by the incident? Internal and external staff? Is the public affected?
f. What environments are affected by the attack?

2. After verifying the details of the Reportable Event or incident the Incident Response Lead, in consultation with other members of the Security Office, will make a determination if the Reportable Event is an incident and if the SIRT should be assembled.

   a. In the event the incident can be managed internally by the Security Office or a slightly broader group of resources, the Incident Response Lead will continue to manage the incident as outlined herein without the SIRT.
   b. In the event the incident is HIGH IMPACT and requires significantly broader management, the Incident Response Lead will contact the SIRT to identify the incident and perform any follow-up with respect to the incident. The SIRT will meet periodically throughout the duration of the incident until resolution of the incident.
   c. The Incident Response Lead will contact the appropriate staff with access to the affected components to continue investigation of the incident:

      i. Application Subject Matter Expert (SME) - In the event the application is compromised (integrity is in question) access to it should be cutoff/read only and business continuity should be evoked
      ii. System Admin – Logs may need to be gathered for the affected system or access frozen
      iii. Network Admin – Logs may need to be gathered. Network traffic monitoring may need to be done. DDOS attack may need to involve a third party such as Akamai for assistance. The Net Admin should be able to provide some information on what protections are in place if any
      iv. Account Operations – if an account is compromised it must be disabled. The manager of the employee will be informed
      v. ITSM – if a desktop/device/server is compromised, the ITSM may need to implement on-the-ground remediation of the desktop/device/server. In the event they are directed to turn over a desktop/device/server for additional review (even in-place), the EOHHS Chain of Custody Form should be utilized. As equipment is shut down and retrieved for

handover for forensic review, the form must be completed by each person involved in moving and/or transferring control of the hardware

d. While the SMEs investigate, the Incident Response Lead will coordinate the investigation effort by ensuring and coordinating that the SMEs have the appropriate access and equipment to investigate. As time is of the essence to appropriately address and remediate an incident, any impediments to investigating the incident must be escalated through the SIRT to the Chief Security Officer and corresponding IT and programmatic management immediately to eliminate the impediment.
e. Once a path to remediation has been identified, remediation should begin. In the event the investigation of the incident and any spread is not completed, remediation should take priority to first contain the incident and minimize any damage from the incident.

vii. *Remediating an Incident*

Incident remediation will be dependent on the findings from the investigation. Below are potential scenarios for this, but each Incident may be handled differently. What is important to note is that the goal of remediation is to prevent the further compromise of the confidentiality, integrity and availability of an Information Resource or location and ensuring that future compromises should not occur due to the same cause.

Incidents and/or Reportable Events will typically fall into one of the following categories and should generally be handled as outlined:

1. Account and/or Location Compromise:

    a. This occurs when an individual(s) steal a legitimate set of credentials for access to an Information Resource or location and use that to access the Information Resource or location. Alternatively, an individual may spoof or hack an Information Resource or location using fraudulent credentials or by taking advantage of latent vulnerabilities.
    b. Any logs or other relevant records related to the access should be reviewed.
    c. Any potential violations of HIPAA or other legal compliance source should be reported to the Agency Privacy Office or equivalent immediately.
    d. Any improper access should be terminated and the source of improper access should be closed such that improper access cannot continue (e.g.: by resetting passwords). Any improper activity should be reversed, to the extent possible, and the proper state of operations should be restored to the extent feasible.

2. Suspicious employee behavior:

    a. This occurs when an employee exceeds the legitimate extent of their access or engages in behavior that will compromise the confidentiality, integrity, or availability of any EOHHS Information Resource.
    b. The Incident Response Lead should ensure that Agency Human Resources and the Legal Department are notified of the inappropriate behavior.
    c. The Incident Response Lead should work with Forensic Analysts to monitor the employee's aberrant behavior and collect evidence with respect to that behavior.
    d. In the event the employee's behavior will lead to an imminent loss of the confidentiality, integrity, or availability of Information Resources, the Incident Response Lead should act to prevent such loss.

3. Application compromise:

    a. This occurs when an individual gains access to an application (including websites) and makes material changes to the operations of that resource.
    b. Application teams may be required to place the application in read only mode in order to preserve integrity or freeze access.
    c. The intrusion vector should be identified and patched, to the extent feasible, to stop continued access.
    d. The application's backups should be reviewed to ensure the backups are verified as good. This is especially critical where, for example, there is a ransomware infection where the infection could be present in backups for days or weeks. The application should then be restored from a verified good backup. In the event a backup cannot be verified as good, then the application should be reconstructed to restore operations to the greatest extent possible.
    e. Application teams should implement business continuity plans with respect to impacted or unavailable service.

4. Information Spillage:

    a. This occurs when an Information Resource transfers information to an individual, group, or other Information Resource without authorization.
    b. The Incident Response Lead will work with Information Resource teams to identify the information involved in the information spill, the scope of the downstream spillage, and any comingling or other impact by the information spill.

c. The Incident Response Lead will work with Information Resource teams to isolate access to impacted Information Resources to prevent unauthorized access to the information spill and additional transmission to other Information Resources.
d. The Information Resource team will work to "scrub" all spilled data from the system to eliminate, to the maximum feasible extent, the presence of spilled data in any application databases (including in backups).
e. The Incident Response Lead will then work with Information Resource teams to verify that the information has been scrubbed and verify the Information Resource is "clean" prior to restoring full access to the Information Resource.

3. Virus Outbreak or Social Engineering Attack

    a. This occurs when malicious code is knowingly or unknowingly deployed in the EOHHS Environment and may range from a single instance of the malicious code to widespread dissemination of the malicious code. This may also occur where someone disseminates information as a result of a seemingly legitimate request for information which is in fact an illegitimate request or from an illegitimate source.
        i. Note that single desktop virus infections will follow the current process that EOHHS IT Site Managers ("ITSMs") have in place to initiate a virus scan and follow its recommendations for remediation unless additional assistance is needed.
    b. These are predominantly isolated incidents which can be handled internally by the Security Office with assistance by ITSMs. Occasionally, the impact will be more widespread, impacting a number of Information Resources. If that occurs, the Incident Response Lead may require the assistance of a broader group of individuals to remediate the incident.

4. Physical Disturbance/Act of God

    a. This occurs when a natural event renders inaccessible some or all of EOHHS's or an Agency's operations and Information Resources.
    b. The impacted Agency or portion of EOHHS should implement their continuity of operations plan.
    c. The Security Office will assist with coordination of the maintenance of the confidentiality, integrity, and availability of impacted Information Resources.

5. The EOHHS Security Office will maintain desk level procedures for handling each category of incident. EOHHS and its Agencies are responsible for and must individually maintain continuity of operations plans in whatever form

they deem appropriate, which outline how operations will continue in the event of the occurrence of any of the aforementioned classes of Incidents.

viii. *Restoring Operations*

EOHHS SIRT Response Form, EOHHS SIRT Incident form, EOHHS SIRT Lessons Learned form

1. Once the incident has been contained, there should be a focus on restoration of business operations

    a. Access to websites, applications, and other Information Resources should be restored from read only.
    b. Equipment should be returned as is or from a new image.
    c. A notice may need to be submitted to the public depending on the incident. A summary SIRT Response Form is attached to this Document as Attachment 6 which can provide guidance on how to respond or what information should be provided.
    d. The Incident Response Lead or their designee should complete the SIRT Incident form to close out reporting on the incident.

2. In conjunction with a restoration of business operations, the Incident Response Lead should work with Agency counsel, privacy counsel, and/or Privacy Officers to:

    a. make a determination about what privacy and security reporting is required as a result of the incident (in accordance with law and contract—outlined pursuant to *Section VIII, Inventory and Classification* and Attachment 2),
    b. complete all required privacy and security reporting, and
    c. make a determination about any remediative or corrective action necessary to satisfy legal or contractual obligations with respect to security and privacy.

3. Scheduling of Lessons Learned should be arranged with all participating and impacted Agencies and staff invited. The minutes from those Lessons Learned meeting(s) should be recorded and kept with the Incident Form for reference. Any changes to any processes, procedures, or Information Resources as a result of the Lessons Learned should be documented, tracked, and followed-up with a future meeting to ensure the change has been implemented as discussed.

d. Testing the Incident Response Plan

On an annual basis, the Incident Response Lead will coordinate with EOHHS and each Agency a tabletop exercise testing the effectiveness of this Incident Response Plan and the continuity of operations plans. Such tabletop exercise will generally include one or more scenarios designed by the Security Office to test the responsiveness of EOHHS and the

Agency with respect to an incident. The process for testing will generally adhere to the following process:

i. At the beginning of the fiscal year (July 1), the EOHHS Security Office will generate a number of incident scenarios ranging from minor to worst-case-impact. Those scenarios will be crafted to maximize testing of the incident response process and business continuity process with an eye towards intentionally stressing the processes and revealing gaps in the processes.

ii. The list of incident scenarios will be provided to the Agency SIRT by August 1. The Agency SIRT should work with other personnel at the Agency to determine an appropriate response path for the scenarios.

iii. Beginning on September 1 and ending on December 31 of that fiscal year, the Incident Response Lead will schedule times to meet with Agency SIRTs. At those meetings, the Incident Response Lead will pick a random subset of the incident scenarios and run through them with the Agency. At the Incident Response Lead's discretion, the Incident Response Lead may modify the scenario, within reason, to make it easier or more difficult. After the conclusion of the meeting, the Incident Response Lead will draft a memorandum outlining the strengths and weaknesses of the incident response and business continuity implementation and provide recommendations for improvement (if any).

iv. Beginning on January 1 of that fiscal year, the Incident Response Lead will schedule follow-up meetings with the Agency SIRTs to distribute the incident response memorandum findings and recommendations and work with the SIRTs to implement the recommendations by the end of the fiscal year.

e. Forms for Reporting on the Incident

Per EOTSS Standard IS.009, the following forms must be filled out during the investigation:

i. EOHHS SIRT Chain of Custody Form – Attachment 4
ii. EOHHS SIRT Evidence Form – Attachment 5
iii. EOHHS SIRT Response Form – Attachment 6
iv. EOHHS Lessons Learned Form – Attachment 7
v. EOHHS SIRT Incident Form – Attachment 8

XII. CONTINGENCY PLANNING

a. Purpose

Contingency Planning, in the broadest sense, deals with the planning and management of continued access to critical EOHHS Information Resources and business functions in the event of impact to the data contained within or the inability to access such data. This may result from infrastructure failure, natural disasters, or other events that compromise continued EOHHS operations.

b. Policy

All Agencies and critical EOHHS Information Resources and business functions must have a contingency plan in place. This contingency plan must consider how service provision will continue during the event giving rise to implementation of the contingency plan. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Contingency Planning Standards

All Agencies and critical EOHHS Information Resources and business functions must define and document the processes that are critical to continued service provision. Once identified, it is the responsibility of those groups to determine how operations will continue in the event of an event giving rise to deploying the contingency plan.

i. Agency leadership and Owners are responsible for ensuring the critical business functions and access to data can continue in the event of an event giving rise to deploying the contingency plan.

ii. The contingency plan must document the scenarios in which it will be activated and the mission critical assets/data/functions it will cover.

iii. The contingency plan must also include information with respect to continued operation including:

1. scenarios where access to the data is not possible such as network or power outage,
2. any manual processes that may be enacted for processes that were previously performed via an electronic means,
3. defining the roles needed and the people assigned to lead in performing those processes,
4. a list of contacts for notification of the outage and those responsible for performing any potential disaster recovery operations,
5. any connectivity to other processes or departments that would be impacted by the enactment of the contingency plan,
6. any notifications to the public of the enactment of the contingency plan,
7. timeframes of acceptable recovery as well as timeframes for enacting the various portions of the contingency plan,
8. recovery objectives should include minimizing the amount of work duplicated and data lost, and
9. details on the resumption of operations once the event has concluded.

iv. The contingency plan should further identify what failover sites exist to continue operations, even if the failover is for staff to work from home. Staff contact information should be readily accessible and available for management and other

staff to support continued operations.

d. Contingency Plan Auditing, Training and Testing

Annual testing of the plan must be conducted in order to ensure that the information in the document is correct and kept up to date. This testing should be conducted in order to maximize training of the plan with staff. When possible, a full failover test should be scheduled. The testing may also be conducted in concert with the testing outlined in *Section XI, Incident Response and Security Incident Response Team.* In addition, at least one staff member should review the efficacy of the contingency plan and make recommendations for improvement or at least identify deficiencies in the current contingency plan.

e. Contingency Planning Standards Specific to Information Systems

Owners must determine whether or not they should have a geographically distinct backup and processing site such that during an event giving rise to implementation of the contingency plan that there is no impact to service. This is deemed met if the Information System is using EOTSS's preferred or provided hosting services, which includes geographically distinct backup services. In the event an Information System is not hosted with EOTSS's preferred or provided hosting service, that Information System's Owner should determine whether or not that is appropriate based on the impact to critical Agency operations from downtime.

XIII. CONFIGURATION MANAGEMENT

a. Purpose

Configuration management, in the broadest sense, deals with changes to the configuration of Information Resources which could impact the overall security posture of the EOHHS Environment. Proper recording of the approved changes will allow environmental consistency, assist in business continuity and disaster recovery, and assist in troubleshooting problems. It also allows Owners to monitor and audit against the baseline to ensure that changes were implemented as presented and that unapproved changes were not performed.

Appropriate management of configurations allow quick and easy deployment of resources and reconstituting/rebuilding from scratch for business continuity and disaster recovery purposes. It also provides consistency across environments. In the Information System space, for example, each lower level will need to be clones of the previous (development, test, staging, and production) in order to ensure the integrity of the work being done in the Information System.

b. Policy

All EOHHS Information Resources must have a recorded Baseline. Configuration Management will include any aspect of hardware, software, settings and processes needed to enable expected and planned functionality and comply with any required regulations. Documentation shall include the architecture, any connections to other environments, and

processes captured on usage. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Configuration Management Standards

Owners must maintain a Baseline for operations, Information Systems, and other Information Resources under their purview. While the requirements outlined in this *Section XIII, Configuration Management* are focused on Information Systems, all Information Resources and processes must have prepared Baselines to support resumption of operations as expeditiously as possible.

Baselines must include, at a minimum and as applicable, the following considerations:

i. Description of the Information Resource and the intended functionality
ii. Architecture of the Information Resource
iii. Information Resource hardware components
iv. Information Resource software components
v. Configuration changes made to the installation of software and hardware aside from vendor recommendations
vi. Name, title, and contact information for Owners
vii. Location of hardware (server rack, desktop, etc.)
viii. Location of media files for installation along with any additional components that have been added
ix. Location of associated documentation for business continuity and disaster recovery
x. Configurations for creating and monitoring alerts
xi. Documentation for required configurations based on law or contract
xii. Any linkage to other Information Resources and details on how they are connected
xiii. Secure configurations for the system:

    1. Accounts with details of access to the system including groups such as system administrators and service accounts
    2. Reference to the hardened template used for the operating system
        a. Included should be any ports or services that have been enabled for the Information Resource to function and why it was necessary to deviate from the standard
    3. Audit, authentication and access controls
    4. Approved methods of accessing the system for maintenance (VPN only, SSL, physical location, etc.)
    5. Protections in place such as HIPS, endpoint protection, firewall, etc.
    6. Firewall settings
    7. Operational Risk Assessment sign off documentation, if applicable, generated pursuant to the process outlined in *Section X, Authorization to Operate and Operational Risk Assessment*

Baselines must be reviewed at least once annually and updated as appropriate. Baselines must also be reviewed upon significant and material changes to the Information Resource that render the prior Baseline obsolete.

d. Change Control Committee and Change Process

Owners should work to expeditiously implement change control committees to verify and approve a Baseline. The size and formality of these groups will vary from Information Resource to Information Resource and Agency to Agency. At a minimum, all change control committees must be structured to ensure the division of labor such that the individual or group approving of changes is competent to approve of such changes and is distinct from the person implementing changes. The change control committee should include the Information Resource Owners or report to such Owners.

Any changes to the Baseline must be submitted for approval to Owners for review. The change must be documented with detailed implementation steps, settings and software/hardware necessary to adequately implement the change in the development environment. Change documentation should also include the expected outcome(s) from the change and if there are any known security risks/vulnerabilities being introduced or remediated because of the change. If there are known security risks/vulnerabilities being introduced, the process outlined in *Section X, Authorization to Operate and Operational Risk Assessment* must be followed expeditiously to not impact deployment of changes to Production. Changes should be distributed and accessed on a need-to-know basis.

A rollback plan should also be included in the event the change does not function as expected. The rollback plan should also include the exact steps for the return to the previous Baseline. Any processes that will also change as a result should be documented and either updated in the current procedures or an addendum should be included.

Once the Owner approves of the Baseline change, it should be tested for compatibility and security impact. When testing is successfully completed and the changes are ready to be moved into the Production or business operations environment, it will need to be submitted to the change control committee for review and approval. Members of the committee will be able to ask questions to the submitter regarding the change as well as scheduling resource availability for implementation. The change control committee should review the expected time to implement the change, any rollback plans, and any authorization to operate or operational risk assessment. If approved, the change should be placed onto a change calendar managed by the change control committee. If the change is not approved, feedback should be provided to the submitter including comments for remediation for resubmission.

During implementation, the implementation team should be available to answer questions posed by the change control committee, to troubleshoot if issues arise, or to implement the rollback plan. Once the implementation is completed it will need to be verified and approved by the change control committee. Relevant stakeholders should also be notified of the completion of the change or implementation of the rollback plan. All associated documentation should be updated before the change is closed. That documentation should be maintained to support operationalization of the change. Software should be filed in a predefined and accessible media library and materials saved in a designated documentation retention area.

XIV. IDENTITY AND AUTHENTICATION

a. Purpose

The standards outlined in this *Section XIV, Identity and Authentication* address the processes, procedures, and systems used to verify the identity of individuals and accounts that may request access to Information Resources and to make authorization decisions granting or denying access.

b. Policy

All Information Systems must have appropriate administrative and technical controls in place to ensure accurate identification of individuals and accounts, and proper authorization prior to granting access to Information Systems and to functions that read, create, modify, and reporting on Information Resources. User, account, and system access shall be affirmatively managed throughout account and system lifecycles, including identification of users; disabling of known- or suspected-compromised accounts; modification of account rights and privileges when roles change, when individuals start and end service, and at otherwise appropriate times; and revocation of access when it is no longer needed to fulfill an authorized business function. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Identity and Authentication Standards

i. **Unique Identification:** Information Systems must uniquely identify and authenticate both (a) organizational users (employees, contractors, researchers, etc.); and (b) non-organizational users (vendors, external support staff); for all processes and accounts acting on their behalf, before providing access to, establishing a connection to, or executing a function on, any Information Resources.

ii. **Multi-factor authentication:** Information Systems must require multi-factor authentication for remote and network access to all user accounts, privileged and unprivileged, and for local access to privileged accounts. All authentication mechanisms must include hardening in design or implementation to resist session-replay (traffic sniffing or traffic replay) attacks. Multi-factor authentication for remote access to privileged and non-privileged accounts must include at least one factor provided by an approved smartphone app or hardware token. All Information Systems must accept and electronically verify Personal Identity Verification (PIV) credentials for identification and authentication.

iii. **Credentialing process:** The registration process to receive passwords, certificates, hardware tokens, and other authenticators must be conducted **in person** by an individual authorized to distribute such credentials. Passwords may not be sent by email or text message/SMS (except that: (i) self-serve password-reset links may be sent electronically, as long as they expire after no more than 24 hours; and (ii) one-time use PINs may be sent electronically, as long as they expire after no more than 5 minutes).

iv. **Identifiers (usernames/account names):** Owners are responsible for ensuring their Information Systems and associated processes perform all of the following requirements with respect to identifiers (usernames, account names, security badge numbers, Globally Unique Identifiers ("GUID"), etc.:

1. Receiving prior, written authorization from business process Owners before assigning an individual, group, role, or device identifier;
2. Selecting and assigning an identifier for the relevant individual, group, role, or device;
3. Preventing reuse of identifiers for at least ten years;
4. Disabling the identifier after a defined period of inactivity (60 days for user accounts; 1 year for application or system accounts; 1 year for groups with no active accounts);

v. **Authenticators (passwords, PINs, tokens):** Owners are responsible for ensuring their Information Systems and associated processes perform all of the following with respect to authenticators (passwords, PINs, biometrics, etc.):

1. Verifying the identity of the individual, group, or device receiving the authenticator before distributing it;
2. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
3. Establishing and implementing procedures for initial authenticator distribution, initial authenticator content, changing default content of authenticators prior to Information System installation, changing or revoking lost/compromised or damaged authenticators; and for revoking authenticators;
4. Changing/refreshing authenticators on a regular schedule appropriate to the authenticator type (60 days for passwords, 5 minutes for one-time PINs in apps or hardware tokens; 5 years for access cards such as PIVs and other identification cards, etc.)
5. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; protecting authenticators and authenticator content from unauthorized disclosure and modification, and requiring that individuals take steps and are trained to do the same;
6. Never using shared authenticators (e.g. password shared with multiple individuals) unless it is technically impossible to operate the Information System without doing so, and changing shared authenticators whenever there are membership changes in groups with access to a shared authenticator.
7. For hardware token-based authentication, the token and authentication system must satisfy FIPS 140-2 requirements.
8. If an Information System accepts third-party credentials, they must be FICAM-approved, and the Information System must conform to FICAM-issued profiles.

vi. **Password standards:** All password-based authentication must meet the following requirements:

1. **Complexity:** Enforce minimum password complexity of at least:
    a. Character Count:
        i. 8 characters for public user accounts,
        ii. 12 characters for all other non-administrator accounts,
        iii. 15 characters for administrator accounts,
    b. And including:
        i. 1 lower case letter,
        ii. 1 upper case letter,
        iii. 1 number,
        iv. and 1 special character.
2. **Not recently used:** Any new passwords must be different from the last 24 passwords used for that individual or account
3. **Changes must be non-trivial:** All changes must modify at least 2 characters from all stored previous passwords.
4. **Minimum and maximum age:** passwords must be changed regularly (every 60 days for user accounts; annually for service and application account), and may not be changed within 1 day of the previous change (unless a written exception justifying an earlier change is documented).
5. **Temporary/Initial Passwords:** Information Systems may allow the use of a temporary password for initial logons or password resets, as long as: (1) the initial password is randomly set; (2) it is unique to the account to which it is assigned; and (3) the system requires an immediate password change upon first login. Password resets must require re-identification of the individual whose account is being reset.
6. **Password encryption required; salt preferred:** Passwords and other authenticating credentials may not be stored or transmitted in plaintext; they must always be cryptographically protected in transit (e.g., session encryption, HTTPS) and at rest (e.g., hashed) using Acceptable Encryption Suites, and, if available, a site- or system-specific salt prior to hash.

vii. **Certificate-based authentication recommended:** Although PKI/certificate-based authentication is difficult to set up, once it has been initialized, it is more secure and arguably easier to use than passwords. For this reason, Owners are strongly encouraged to use certificate-based authentication instead of (or in addition to) password-based authentication. All cryptographic authentication mechanisms must use Acceptable Encryption Suites.

viii. **Certificate authentication requirements:** All PKI/certificate-based authentication must:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor;
2. Check certificate status information (including revocation lists via Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP), and against a Certificate Transparency chain if one exists for the relevant domain);
3. Enforce authorized access to the corresponding private key;

4. Map the authenticated identity to the account of the individual or group; and
5. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

d. Additional Design and Configuration Hardening Requirements

i. **No hardcoded credentials**: Owners must ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. Hardcoded passwords and hardcoded certificates are not permitted. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators, irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

ii. **Do not display secret authenticators:** All Information Systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals (for example, displaying asterisks (*s) at a login prompt instead of the password itself, which reduces the risk of shoulder-surfing).

iii. **Impede account enumeration attacks:** Authentication denials must behave the same whether an identifier exists and the authenticator was incorrect, or there was no matching identifier found (to prevent account-enumeration attacks). Similarly, for password reset requests by email, Information Systems must not indicate whether an account was found or not. Instead, they should indicate that if an account with that identifier (username or email address) was found, reset information was sent to its registered email address.

XV. MEDIA PROTECTION

a. Policy

All EOHHS personnel must secure media in any form in the EOHHS Environment so that Information Resources contained on those media are secured. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

b. Media Protection Standards

Staff are not restricted in the kinds of media they may use in the EOHHS Environment and all digital (e.g.: USB flash drive) and non-digital media (paper) are permitted. Staff, however, must not store Sensitive Information on unencrypted digital media or in an unencrypted format if the digital media cannot be encrypted itself. Additionally, staff may not store Sensitive Information on unsecured non-digital media. To that end:

i. All non-digital media containing Sensitive Information must be locked in a container (e.g.: filing cabinet) or secured within a locked room (e.g.: a locked office) when not in use. Non-digital media should not be left unsecured while unattended.

ii. All information resources stored on digital media must be encrypted. That encryption may be container-based (e.g.: an encrypted file) or device-based. If relying on device-level encryption, the media must meet the standards outlined in FIPS 140-2 Level 2 for secure devices.

Digital media must have an owner and devices without a specific owner must not be used in the EOHHS Environment.

All media containing Sensitive Information that leaves the EOHHS Environment must be marked on the media that it contains Sensitive Information. This may be done by marking the media as confidential, sensitive, or with some other similar marking or indication. Movements of media containing Sensitive Information outside of the EOHHS Environment should be documented such that access to the media and custody of the media can be attested to throughout transit.

When media containing Sensitive Information is at the end of its lifecycle, it must be destroyed or sanitized pursuant to the requirements of NIST 800-88. These requirements assure that information is removed from media such that the information cannot be retrieved or reconstructed.

XVI. SYSTEM AND COMMUNICATIONS

a. Policy

All Information Systems must have appropriate administrative and technical controls in place to ensure the protection of systems, components, subcomponents, and communications among them. Owners are responsible for designing and configuring their Information Systems to ensure the confidentiality, integrity, and availability of Information Systems and information resources. Generally, Information Systems shall be inventoried, affirmatively managed, configured according to industry best practices, patched with security updates, and used only so long as they are supported by the vendor or provider (or, in the case of open-source software, the project is releasing security updates, even if not formally contracted for support as with COTS or vendor-developed software). Generally, communications shall be encrypted and authenticated, and shall take place through functions that include security checks, rather than direct access to data or memory. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

b. System and Communications Standards

i. All Information Systems must:

1. Separate user functionality (including user interface services) from information system management functionality.
2. Prevent unauthorized and unintended information transfer via shared system resources.

3. Protect against or limit the effects of denial-of-service attacks, including network- and application-level flooding, DDoS, reflected DDoS, ransomware, and physical damage, by:

    a. Hardening all system configurations according to vendor recommendations and industry best practice
    b. Using protective technologies where the cost of doing so is less than the risk appropriate (which may include intrusion prevention systems, firewalls, router access control lists, proxies, reverse proxies, web application firewalls, and sinkholing/blackholing services)
    c. Allocate sufficient technical and logical resources (bandwidth, compute/CPU, memory, sessions, etc.) to handle the highest normal expected load, where appropriate partitioning such resources using priority queues and/or quotas
4. Maintain a separate execution domain for each executing process (i.e., processes may only interact through APIs, not shared memory).
5. Log system and resource loads over time, which Owners must periodically review, adjusting assigned resources to handle projected loads

ii. For each Information System, Owners must:

1. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system (e.g. between services, components, and subcomponents within the system).
2. Implement controls, where practicable, to verify the source and format of data passed between systems or between components or subcomponents within a system, ensuring that malformed requests are logged and denied.
3. Implement subnetworks for all publicly accessible system components that are physically or logically separated from internal organizational networks.
4. Design and configure their Information Systems on the assumption that interfacing systems, components, and data flows may be compromised, and develop and implement their own Information Systems with boundaries designed to stop or impede that compromise from spreading (defense-in-depth). Information Systems must avoid blindly trusting the format of data streams just because they are internal or from a known external partner; instead, their format and well-formedness must be checked at each boundary before the information is processed or passed on.

iii. For all connections to external networks or resources, Information Systems must:

1. Connect to external networks, services, or 3rd-party information systems, only through managed interfaces that include boundary-protection devices (firewalls, proxies, etc.)
2. Limit the number of external network connections
3. Implement a separate managed interface for each external service or system

4. Establish and periodically review traffic flow policies for each managed interface, with a default-deny policy (deny all, permit by exception)
5. Document any exceptions to traffic flow policies with a supporting business need, duration of such need, and approval thereof (reviewing all such exceptions at least annually, and removing any which are no longer supported by a business need)
6. Protect the confidentiality and integrity of the information being transmitted across each interface (i.e., with encryption and authentication)
7. Prevent, by policy and configuration, remote devices from simultaneously establishing non-remote connections with the Information System and communicating via some other connection to resources in external networks (i.e., split tunneling is disabled, and users are prevented from enabling it)
8. Employ authenticated proxy servers at managed interfaces for all transmissions of regulated data to any external networks, services, or 3rd-party information systems, logging metadata for all such traffic to a central logging platform

iv. Within each Information system, Owners must ensure:

1. Implementation of host-based firewalls on all servers, workstations, mobile devices, and other Information System components (or external or virtual firewalls at the immediate next network hop – e.g. a Layer 3 switch with built-in firewall)
2. Isolation of systems providing user authentication, user authorization, network management, configuration management, vulnerability scanning/management, and other high-risk services from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system
3. The Information System fails securely in the event of an operational failure of a boundary protection device (e.g., if a firewall fails, no traffic flows; if a router with ACLs cannot process the traffic load, it defaults to dropping unprocessed packets, etc.)
4. The Information System protects the confidentiality and integrity of transmitted information, within Information Systems (between components), between Information Systems, and transmissions to 3rd-party or other external systems, using Acceptable Encryption Suites during transmission to (a) prevent unauthorized disclosure of information; and (b) detect changes to information in-transit. The information system must also maintain the confidentiality and integrity of information during preparation for transmission and during reception
5. The Information System terminates the network connection associated with a communications session at the end of the session or after a policy-defined period of inactivity (not to exceed 15 minutes for applications and 4 hours for VPN/tunneling connections)

c. Key Management Standards

Owners must ensure that their Information Systems and all business processes manage the cryptographic keys for required cryptography in accordance with FIPS 140-2 Level 2; HIPAA; NIST SP-800-53r4; and other applicable laws, regulations, and directives.

All public key certificates must be issued in accordance with these same requirements, or obtained from an approved service provider that meets these requirements.

d. Mobile and Collaboration Devices Standards

Owners must ensure that collaborative computing devices (VOIP and traditional telephones, teleconference equipment, microphones, cameras (except security cameras), electronic white boards, etc.): (a) prohibit remote activation, unless (i) authorized by the relevant EOHHS Risk Governance Team, or (ii) required by law; and (b) provides an explicit indication of use to users physically present at the devices (unless (i) or (ii) above applies).

Owners must authorize, monitor, and control mobile devices that connect to Information Systems or access Information Resources, ensuring adherence to all applicable mobile device policies, and use only vetted & approved mobile devices, code, and technologies. Owners whose Information Resources contain FTI must work to prohibit access to FTI with that mobile device. Per IRS requirements, mobile devices are not authorized to be used to access FTI.

Owners must authorize, monitor, and control the use of VOIP technologies in their environments and by their employees above and beyond the EOHHS telephony system. Such Owners' authorization must be a risk-based assessment, taking into account the risk to Information Systems, Information Resources, and information itself, of potential misuse, including employee misuse (intentional or accidental) as well as malicious use (intentional eavesdropping, interference with other Information Systems, etc.).

e. Name and Address Resolution (lookup services and authoritative DNS)

Information Systems that provide name-to-address resolution (DNS, WINS, etc.), must provide additional data-origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to name or address resolution queries (e.g., DNSSEC). Where such an Information System is part of a distributed or hierarchical namespace, it must provide the means to indicate the security status of child zones and, if the child supports secure resolution services, to enable verification of a chain of trust among parent and child domains.

Information Systems that make name- or address-resolution requests must perform data-origin authentication and data-integrity verification on name and address resolution responses.

Information Systems that collectively provide authoritative name or address resolution services for an agency, organization, location, or subnetwork (e.g., authoritative DNS servers) must be fault-tolerant (i.e., at least two active systems in at least two different

physical locations, one primary and one secondary) to eliminate a single point of failure and to minimize the risk of name-resolution outages. They must also implement internal/external role separation: separate Information Systems must be used for internal-only namespaces, such that Systems with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients), while those with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Access to all internal namespace resolution services must be restricted (e.g., by address range, client lists, certificates, etc.) to internal systems, with any exceptions documented and specifically authorized.

f. Encrypting Sensitive Data in Transit

Information Systems must protect the authenticity of communications sessions (in addition to data packets) carrying Sensitive Information, using Acceptable Encryption Suites (including for confidentiality and authentication) that provides assurance of all communication parties' identities, ensures data is not modified in transit, and protects against session hijacking, session replay, XSRF, and other man-in-the-middle and session attacks. This should include data transmissions within MAGNet, as well as transmissions to and from external parties/services, and all wireless data transmissions.

Encryption and authentication should be the default choice for data transmission. In addition to required encryption, Owners are strongly encouraged to encrypt all data in transit. Wherever possible, Owners are strongly encouraged to configure their Information Systems to check certificates against the certificate revocation list, and to disallow connection if offered a revoked certificate or if the CRL cannot be reached.

g. Encrypting Sensitive Information in Email

Whenever sending sensitive information via email, Owners must ensure that their employees and Information Systems send only encrypted email, such that the authorized recipient can only receive the sensitive information over an encrypted channel. Acceptable methods include encrypting an attachment in the normal email stream, as long as the passphrase or key is shared via a separate, authenticated communications method, a plaintext email containing a link to an authentication-protected download portal, etc.

Information Systems sending or receiving email (inbound and outbound mail relays, inbox servers, etc.) must support encrypted transit using an Acceptable Encryption Suite, and must use such encryption if the other system (either sending or receiving the mail) supports it. Information Systems should log the number of emails sent to each domain, and record whether that domain supports SMTP over TLS (or other encrypted channel) or not.

h. Encrypting Sensitive Information at Rest

Information Systems must protect the confidentiality and integrity of data at rest. For all Sensitive Information, Owners must ensure either (i) physical control of access to the media storing and the Information Systems processing that information or (ii) encryption of the data with an Acceptable Encryption Suite. File, row/application, folder, and/or disk-level

encryption may be appropriate based on the system architecture and the types of risks it faces. When data is encrypted, its encryption key must be securely stored, such that the level of access required to read the encrypted data does not automatically include access to the key (e.g., encrypted .zip files may not be sent over email if the key is also shared via email); an encrypted laptop or portable hard drive does not count as "encrypted" under this Document if the passphrase or key required to decrypt it is affixed to or stored with the device.

i. Data and Process Partitioning

Where appropriate, Information Systems must be partitioned into separate physical domains or environments based on the data classification of the Information Resources and data they contain.

Highly sensitive information may only be stored in tighter-controlled environments (i.e., NIST 800-53r4 High; FedRAMP High, etc.). Highly sensitive information will be defined on an as-needed basis by each Agency maintaining the data. At a minimum, this information includes CJIS data maintained in the EOHHS Environment.

j. Sensitive Information in Fax Transmissions

For any Information Systems authorized to send or receive PHI in fax transmissions, the recipient must be authorized, the fax-capable machine located in a locked room or other secure Facility, fax preset/speed-dial numbers must be checked for accuracy at least annually and whenever cause to believe the number is inaccurate or no longer accurate arises. Outgoing fax transmissions must use a cover sheet that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone or reply to the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

XVII. PHYSICAL AND ENVIRONMENTAL PROTECTIONS

a. Purpose

Physical and environmental protections controls address physical safeguards and procedures that grant or deny access to Facilities and Supporting Infrastructure, as well as their design and operation. For access controls for Information Resources or Systems themselves, including decisions about how such permission is granted, modified, and revoked, see *Section VI, Access Control.*

b. Policy

All Facilities must have appropriate physical and environmental controls in place (considering data classification levels and operational criticality) to protect against unauthorized access, interruption of service, interception or modification of traffic, and to detect, respond to, and review incidents that arise. Compliance with these standards must

be achieved within twenty-four (24) months of publication of this Document.

c. Physical and Environmental Protections Standards

i. Restrict Access to Authorized Individuals

Managers must adopt, disseminate, provide training on, and periodically review and update (at least annually) policy and procedures to ensure implementation of the following requirements:

1. Managers must identify the Facilities for which they are responsible and any Supporting Infrastructure, determine the physical boundaries, controlled areas, and access points of each, and enforce physical access authorizations at each access point, including all of the following:
    a. Authorizing individual access according to the principle of least privilege, so that individuals only have the lowest level of access necessary to perform their (current) job
    b. Implementing technical, operational, and administrative controls to maintain separation and adhere to the principle of least privilege where authorized individuals have physical access to logically separated data, applications, databases, or virtual hosts
    c. Verifying individual access authorization before granting access to the Facility or Supporting Infrastructure
    d. Controlling ingress to and egress from the Facility using locked doors, keys, PIN entry pads, badge readers, access control vestibules (man-traps), guards, and/or other appropriate physical access controls
    e. Maintaining physical access audit logs for each access point (written and/or automated)
    f. For areas of a Facility designated as publicly accessible (e.g. lobbies, delivery areas, etc.), providing physical separation from controlled-access areas and any security safeguards necessary to support the controls applied to the controlled-access areas of the Facility (e.g., guards, cameras, motion detectors, etc.)
        i. Components of Information Systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible, as long as access to these components is effectively controlled using technical or administrative safeguards
    g. Escorting all visitors to controlled-access areas in Facilities, monitoring their activities, and logging their identity, entry and exit times, and the reason for the visit
    h. Securing all keys, key cards, identification badges, security tokens, and other physical access devices, and inventorying and accounting for them at least annually
    i. Changing combinations and keys (i) periodically (at least once every 5 years); and (ii) whenever keys are lost, combinations are compromised, or individuals are transferred or terminated (and

such individual had access to combinations, or had keys and failed to return them, or had keys and was known or suspected to have made copies)

j. Ensuring that output devices (including but not limited to printers, fax machines, and display devices that show output without requiring authentication) are appropriately located, or otherwise protected, so as to prevent unauthorized individuals from viewing or obtaining the output

k. Locating Information Systems within Facilities, and designating and designing any new Facilities, so as to minimize the opportunity for unauthorized access (considering the type of physical access controls applied, lines of sight, physical distance between Information Systems and points of access for controlled areas)

l. Designing and operating Facilities and Information Systems so as to minimize the potential for unauthorized interception, recording, and modification of wireless traffic

m. Authorizing, monitoring, and controlling the movement of all devices entering, exiting, or within a Facility (including hard drives, flash drives, CDs/DVDs, and other storage media; computers, computer parts or other components of an Information System; mobile devices, including mobile phones, tablets, and wearable devices; cameras, voice recorders, or other recording devices; in short any device which can record or store information, or connect to an Information System—including wirelessly, over WiFi, Bluetooth, Zigbee, Z-Wave, proprietary protocol, or otherwise)

n. Securely removing any sensitive data, regulated information, and licensed software from media/devices exiting a Facility, unless there is a specific business need for, and regulations and applicable Third Party Agreements allow, removal to an off-site facility

o. Ensuring any off-site facilities which handle equipment from an EOHHS Facility, where the device/equipment has not been securely erased (i.e., overwritten: standard deletion and drive formatting are not sufficient) is required to adhere to these same controls

2. Managers must maintain and approve a list of individuals with authorized access to each Facility, based on position or Role; issue authorization credentials for Facility access; periodically review their access lists; approve any visitors to the Facility; and remove individuals from access lists when access is no longer required. They must also ensure that:

    a. Physical access to Facilities is monitored to detect and respond to apparent, suspected, and reported security incidents, including break-ins, the presence of unauthorized individuals, and misplaced or stolen access credentials

    b. All individuals, including visitors, who enter access-controlled areas are included in the physical access logs

    c. Physical access logs are reviewed at least annually (sampling is permitted for periodic reviews), and reviewed in detail whenever unauthorized access is apparent, suspected, or reported

d. The results of reviews and investigations are shared with the organizational incident response capability
e. Physical intrusion alarms and other surveillance equipment are monitored
f. Staff are trained to avoid piggy-backing (using one individual's entry authorization to allow multiple people through an access point), even among colleagues
g. Staff are trained to report the presence of anyone not carrying a badge (and whom they do not recognize) to appropriate security personnel

3. Managers must ensure that contractors, vendors, and other third-parties performing work or providing goods to or services in Facilities adhere to these requirements. Managers must notify such persons or organizations that failure to do so may be grounds for termination of existing agreements and may be considered in evaluation and negotiation of future agreements.
4. Managers must ensure that procedures are in place to facilitate controlled access for emergency responders in the event of a medical, fire, or security event.

ii. Protect Facilities and Supporting Infrastructure

Managers are responsible for maintaining a stable, safe operating environment at each Facility, by:

1. Maintaining and updating Facility equipment and Supporting Infrastructure according to manufacturer recommendations, ensuring that maintenance, troubleshooting, and repair are conducted by authorized personnel, and keeping current documentation and maintenance/repair logs on all such equipment
2. Protecting from damage and destruction each Information System's power equipment, power cabling, network cabling, network devices, and other Supporting Infrastructure
3. Ensuring the ability to shut off power to each Information System (and/or individual components) in emergency situations
4. Placing emergency power shutoff switches in appropriate locations to facilitate safe and easy access for personnel
5. Protecting emergency power shutoff capability from unauthorized activation
6. Locating Information Systems within Facilities, and designating and designing any new Facilities, so as to minimize potential damage from fire, flood, wind, rain, lightning, tornado, snow, ice, falling trees/limbs, and other hazards of the weather (including at least a consideration of incoming electromagnetic radiation from EMP bursts and solar flares, even if the response is acceptance of the risk), as well as intentional sabotage (e.g., terrorism, burglary, vandalism) and foreseeable accidents (e.g., vehicular traffic on adjacent roadways, windows that may break, etc.)
7. Protecting the Information Systems from damage resulting from water leakage by:

a. Providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel
b. Using water-leak-detection devices that alert appropriate personnel

8. Providing a short-term uninterruptible power supply, to facilitate either an orderly shutdown or a transition to long-term alternate power for all Information Systems within the Facility, in the event of loss of power from the primary power-source
9. Employing and maintaining automatic emergency lighting for the Information Systems, which activates in the event of a power outage/disruption and covers emergency exits and evacuation routes within the Facility
10. Installing and maintaining fire suppression and detection devices/systems for Facilities and Information Systems that:

    a. Are supported by an independent energy source
    b. Activate detection mechanisms automatically
    c. Notify appropriate personnel in the event of a fire or activation of the device/system (including Facility personnel and emergency responders)
    d. Deploy fire-suppression capabilities automatically (for any Facility not staffed on a continuous basis)

11. Defining acceptable temperature and humidity levels based on manufacturer recommendations of Information Resource components, maintaining those levels within the Facility, and monitoring them continuously or periodically (at least hourly).

iii. Backup Facilities and Alternate Sites

1. During normal operation, all redundant, failover (whether automatic or manual), and backup Facilities must use the same controls required at the primary Facility, unless each such deviation is documented in writing and approved by the relevant EOHHS Risk Governance Team.
2. In case of emergency as designated by relevant EOHHS Risk Governance Team, alternate work sites may be used (such as other government property, or employees' homes if voluntarily provided) which do not meet all of these physical and environmental security controls, without written documentation of each deviation (although the deviation still must be, in fact, authorized by the relevant EOHHS Risk Governance Team).
3. Managers for each Facility and Information System must document and disseminate a means for employees to communicate with Managers and with information security personnel in case of security incidents, problems with the Facility, or emergency.

XVIII. PERSONNEL SECURITY

a. Purpose

Personnel Security, in the broadest sense, deals with how staff are vetted during the hiring process, monitored during employment, and appropriately offboarded when their employment ends.

b. Policy

All EOHHS staff must be appropriately vetted, provided the minimum necessary access to perform their work, be monitored on an ongoing basis, and be completely offboarded at the conclusion of employment. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Personnel Security Standards

Every Information Resource must have clearly defined and readily identifiable roles and responsibilities corresponding to the work that staff perform with respect to the Information Resource. Every Information Resource must also have an Access Coordinator. EOHHS should support Access Coordinators by providing straightforward and accessible processes for providing and revoking staff access to facilities and Information Resources.

i. Role Definition

1. All EOHHS staff positions must be classified based on their risk designation to the organization. The classifications must be consistent and supportable both within an Information Resource group and across the Agency. Some examples of how risk designation should be assigned are as follows:

- Low Risk:
  - the employee poses no or low risk to the organization for exfiltration or loss of sensitive information through mistake or intentional wrongdoing;
  - the employee's access credentials do not provide the ability for an external attacker to modify or gain access to sensitive network resources; or
  - the employee does not have decision-making authority with respect to sensitive matters or resources in the EOHHS Environment.
- Moderate Risk:
  - the employee poses some risk to the organization for exfiltration or loss of sensitive information through mistake or intentional wrongdoing;
  - the employee's access credentials provide the ability for an external attacker to modify or gain access to some sensitive network resources, but the scope and extent of that access is somehow limited; or

    - the employee has decision-making authority with respect to some sensitive matters or resources in the EOHHS Environment, but their authority or scope of authority is limited.
- High Risk:
    - the employee poses significant risk to the organization for exfiltration or loss of sensitive information through mistake or intentional wrongdoing;
    - the employee's access credentials provide the ability for an external attacker to modify or gain access to most or all sensitive network resources and there are few or no effective limitations on that access; or
    - the employee has decision-making authority with respect to sensitive matters or resources in the EOHHS Environment and there are few or no limits with respect to that authority.

Risk designations must be reviewed by the end of the calendar year and updated based on good faith assessments of staff impact to Information Resources. All new positions must be classified within thirty (30) days of creation. Positions existing at the time of drafting this policy must be classified within a year of the effective date of version 1.0 of these *EOHHS Enterprise Information Security Standards*.

ii. Working for the Organization

1. The Access Coordinator must establish screening criteria commensurate with the risk level of the position to appropriately vet and train a new staff member. Depending on the severity of risk assigned to the role, such screening may include calling references, criminal or other background checks, role or position-based training, privacy or confidentiality agreements, or other means of safeguarding Information Resources. Screening would preferably occur before staff are provided access to Information Resources, but may occur after, however must not occur more than thirty (30) days after hire.

   Low and Moderate Risk staff are only required to be screened upon hire (but must receive training annually, pursuant to *Section V, Acceptable Use and Information Security Training*). High Risk staff must be screened once annually to include, at a minimum, position-based information security training.
2. The Access Coordinator must explicitly request staff access prior to the commencement of employment, pursuant to the relevant EOHHS, Agency, and/or Information Resource requirements for access. Access must not be granted outside of the scope of those requirements. The Access Coordinator should be mindful of appropriate processes and timelines for requesting access.
3. The Access Coordinator is responsible for monitoring and appropriately updating staff access to Information Resources and the facility in which they are located.

4. When staff are transferred, the Access Coordinator for their current Information Resources and the Access Coordinator for their new Information Resources must coordinate the appropriate access and timeline for the old and new Information Resources and ensure that access is appropriately terminated and created. Both Access Coordinators are responsible for ensuring that their current and former staff have appropriate access.

   Staff access to resources in the event of a transfer should be modified effective as of the date of the transfer. Staff access to resources in the event of a transfer must not occur later than thirty (30) days after the transfer.

iii. *Termination of Access*

1. When a staff member's employment with EOHHS ends, the Access Coordinator for their Information Resources is responsible for ensuring that access to Information Resources and any facilities to which the staff had access is terminated pursuant to the relevant EOHHS, Agency, and/or Information Resource requirements for access. Access to Information Resources and facilities must be terminated as soon as reasonably practicable. Access Coordinators must ensure that access to the EOHHS network and facilities are terminated as of the last day of the staff member's employment.
2. Access Coordinators must also ensure retrieval of all Commonwealth property including, but not limited to, identification cards, laptop computers, and mobile devices.
3. Access Coordinators must take steps to preserve business continuity such that they can access files and email for the staff member and continue to fulfill the business operation conducted by that staff.

iv. External Access

1. External access to EOHHS Information Resources must be classified and categorized similarly to the standards outlined in this *Section XVIII, Personnel Security.* Access Coordinators should work with Owners and the relevant EOHHS Risk Governance Team to determine external access to those Information Resources. Vendor Access should further be assessed pursuant to *Section XIX, System and Services Acquisition.*

v. Special Provisions for Access to FTI

1. Agencies must initiate and complete a background investigation for all employees and contractors prior to permitting access to FTI. This is required not only by IRS Publication 1075, but also by MGL c. 6A § 18Z. Per the requirements of IRS-1075, background investigations for any individual granted access to FTI must include, at a minimum:

a. FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. (Contact the appropriate state identification bureau for the correct procedures to follow.) A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary-checks/state-identification-bureau-listing. This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.
b. Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last 5 years, and if applicable, of the appropriate agency for any identified arrests. The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.
c. Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization).

Any employees or contractors who fail to pass a background check or refuse to undergo a background check may not access FTI and if they are currently accessing FTI must have their access to FTI revoked immediately. All employees and contractors accessing FTI must undergo a background investigation complying with the requirements herein every five years.

vi. Sanctions for Failure to Comply

1. Relevant EOHHS Risk Governance Teams must create and enforce sanctions for:

a. Failure of staff to comply with appropriate access requirements, and
b. Failure of Access Coordinators to supervise staff access and abide by the requirements outlined herein.

XIX. SYSTEM AND SERVICES ACQUISITION

a. Policy

All externally provided Information Systems and services must be appropriately evaluated and information security standards appropriately enforced. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

b. System and Services Acquisition Standards

i. All Information Systems and services must be procured and contracted for with explicit consideration of information security requirements including criteria for:

1. Evaluation, which require an explicit description of information security functionality and at least a high-level security architecture description, and acceptance of Information Systems and services,
2. Enforcement provisions including a description of interconnection requirements (e.g.: ports, protocols, services, etc.),
3. Legal and contractual requirements for data sources that will be used in connection with the Information System or services, and
4. Detailed documentation of all information security functions and mechanisms and privileged Information System functions so that EOHHS can fully and independently implement and operate the Information System.
5. Configuration and change management to ensure that only EOHHS-approved configurations and changes are implemented.
6. Security flaw testing (including code testing using analysis tools), tracking, remediation, and resolution.

Within twelve (12) months of publication of Version 1.0 of these *EOHHS Enterprise Information Security Standards*, the EOHHS Security Office will promulgate standard language to incorporate in procurement and contract documents. That standard language will, to the extent feasible, require external entities providing Information Systems or services to abide by the requirements outlined herein. Owners must ensure that appropriate resources are allocated to ensure information security standards can be appropriately implemented. Such standards will be crafted in accordance with appropriate legal and contractual drivers, identified pursuant to *Section VIII, Inventory and Classification* and Attachment 2.

ii. Owners must adopt a system development lifecycle methodology that appropriately accounts for information security considerations and permits identification of responsible parties for information security, testing of information security measures, and integrates information security risk management principles into the development lifecycle.

iii. At EOHHS's option, all externally provided Information Systems and services must be assessed, either by EOHHS or by an external auditor. No externally provides services should be further subcontracted without EOHHS's express approval and review.

iv. All Sensitive Information must be hosted within the United States. Sensitive Information must only be accessed from within the United States or via secure VPN connections into the United States.

v. When an Information System component is no longer supported by the vendor, developer, or manufacturer, that component must:

1. Be replaced with a component that is in support, or
2. Continue in place with express written justification, approved pursuant to the process outlined in *Section X, Authorization to Operate and Operational Risk Assessment*.

XX. SYSTEM AND INFORMATION INTEGRITY

a. Purpose

System and Information Integrity addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, with respect to the integrity of Information Systems, the code running on them, and the Information Records they contain.

EHS must handle and retain information in and output from Information Resources in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, contractual obligations, and operational requirements. Generally, Information Systems must protect against malicious code running in firmware, kernel, and user-space; protect memory from unauthorized disclosure and alteration; provide facilities for vulnerability remediation and patching (and reporting); make use of logging and monitoring facilities; support security alerts, advisories, and directives; handle errors securely; and validate/sanitize information flowing into and out of the Information System and between system components. Information that is particularly important or sensitive shall be protected from unauthorized alteration and removal with the use of secure APIs (preferred over direct access), log entries for changes, cryptographic hashes, cryptographically signed modifications (e.g., PKI certificates), or through other suitable mechanism, policy, or process.

b. Policy

All Information Systems must have appropriate administrative, technical, and physical controls in place to ensure the integrity of Information Systems, code that runs on such systems, Information Records stored on such systems, guarding against improper or unauthorized modification or destruction. Owners are responsible for designing and implementing integrity controls that ensure information non-repudiation and authenticity. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. System and Information Integrity Standards

For each Information System, Owners must:

i. Identify, report on, and correct any vulnerabilities (whether publicly known or known to the Owner or any EOHHS staff) within 90 days of release of vulnerability information to the public (or release privately to EOHHS).
ii. Fully test software and firmware updates related to vulnerability remediation for effectiveness and potential side effects before installation, incorporating flaw remediation into the organizational configuration management process.
iii. Complete the installation and testing of all security-relevant software and firmware updates within 90 days of release of such update.
iv. Centrally manage the vulnerability remediation process, employing automated mechanisms (reporting, etc.), at least monthly, to determine the state of Information System component with respect to security vulnerabilities

Owners must also ensure the following physical, technical and administrative controls are in place for the following kinds of issues:

i. Malware:

Information Systems must:

1. Employ malware protection mechanisms (e.g., antivirus, executable whitelisting, etc.) at the System's entry and exit points to detect and eradicate malicious code.
2. Update malware protection mechanisms whenever new releases are available (automatically if possible, and in no case more than 30 days for signatures/definitions and 90 days for agent software) in accordance with organizational configuration management policy and procedures.
3. Run periodic scans using malware protection mechanisms (at least quarterly).
4. Perform real-time malware scans of files as they are downloaded, opened, or executed, on endpoint machines (in memory or in local storage), upon saving to or reading from shared storage (e.g., shared drives), and at network entry/exit points.
5. Block or quarantine malware where reasonably possible, alerting appropriate staff in response to detection of malware (e.g., through central logging and alerting on central log repository).

Owners must:

1. Address false positives during malicious code detection and eradication and contain and manage the potential impact on the Information System.
2. Centrally manage deployment, configuration, logging, and reporting of malware protection mechanisms/software.

ii. System and Log Monitoring:

1. Information Systems must be monitored to detect attacks, potential attacks, and indicators of compromise, identifying unauthorized, suspicious, and unusual activity. Every Information System must have designated individuals responsible for such monitoring, which group may comprise Owners, system administrators, agency staff, EOHHS staff, EOTSS staff, contractors, or other authorized parties. They must identify and analyze unauthorized and unusual activity/conditions using audits, log review, event correlation engines (e.g., SEIM), user behavior analytics, or other methodology, and initiate the incident response process when appropriate. Monitoring must cover activity on local systems, over the local network, via remote connections, and over connections to vendors/contractors/other third parties (including inbound and outbound traffic).

2. In addition to monitoring capabilities within Information Systems, Owners must ensure that independent monitoring devices (intrusion detection systems, web application firewalls, etc.) are deployed (i) strategically throughout the infrastructure (alongside Information Systems) to collect essential information such as authentication and authorization metadata; (ii) ad-hoc at appropriate locations to track transactions and information flows for highly sensitive information; and (iii) where wireless networks are deployed, to detect rogue wireless devices and attempts to eavesdrop on or inject traffic.

3. Log information, whether collected from an Information System or an independent monitoring device, must be protected from unauthorized access, modification, and deletion, including in-transit to the log collection facility and in storage once saved there. If an Information System is unable to either save its log information locally or reach a log-collection device (via a stateful, error-reporting protocol such as TCP), it must stop processing information and/or shut down.

   Owners must implement mechanisms to coordinate the access and protection of log information among external organizations when audit information is transmitted outside of EOHHS, such as with outsourced data centers or cloud providers. Those providers must be held accountable to protect and share audit information with EOHHS though mechanisms including, but not limited to, contract.

4. Owners are responsible for ensuring that Information Systems and monitoring devices send log information to a central log-management facility (centralizing at the Agency, EOHHS, or commonwealth-wide level, depending on the type of Information Resource and the application or Information System in which it resides). Owners are responsible for ensuring that their designated reviewers have access to the log, audit, correlation, and threat information necessary to perform this monitoring and analysis. Owners, Agencies, and EOHHS shall, to the extent practicable, ensure automated methods and tools are used to support near real-time analysis of events.

5. Users and services must have unique accounts, account metadata, or other identifying information, enabling those monitoring to identify the individual, service, account, or other party on whose behalf the Information System is acting, and the location or system where the activity is taking place.

6. Monitoring activity must be heightened whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, the Commonwealth, or the United States, based on information from law enforcement, intelligence, industry threat exchanges, or other credible sources of information. Owners, agency CIOs, and EOHHS are responsible for coordinating and implementing appropriate monitoring

activities and for configuring Information Systems to provide notice sufficient to allow such monitoring.

iii. *Receiving and Processing Security Alerts from External Entities*:

EOHHS shall (working with EOTSS as appropriate) designate appropriate personnel to receive information security alerts on an ongoing basis from reliable external partners to be identified by the EOHHS Security Office as regards specific information security threats and known indicators of compromise. EOHHS shall coordinate responses to these alerts, engaging the incident response process and notifying Owners and other agency staff as appropriate. Patch management will be managed separately: Owners shall designate appropriate personnel from among their system administrators to receive routine patching alerts for their Information Systems (usually from vendors). Incident response and patch management shall be tracked and measured against established SLA targets for each process, and the reason for and POAM for resolving any SLA overages shall be documented.

iv. *Security Function Testing*:

Information Systems must verify that security functions (such as access control, authentication/authorization, etc.) are operating correctly. This verification must be performed: (i) at system startup (or resume/wake from suspend); (ii) upon command by user with the appropriate privilege; and (iii) routinely at least monthly. The Information System must generate an alert for appropriate personnel, and then shut down or restart, when anomalies in security functions are detected. Failed tests or anomalous results must be treated as potential incidents and proceed through the incident response process.

v. *Integrity Checks for Core Components*:

Information Systems must use integrity verification tools (whitelists, tripwires, file hash comparisons, etc.) to detect unauthorized changes to core system components, such as operating system software, security functions, and any applications or programs running with root/administrator/full control permissions. These checks must occur: (i) at system startup; (ii) when new versions of core system components are installed; (iii) when new instances of core systems components are spawned or run; (iv) periodically (at least monthly, and at least weekly for systems containing highly sensitive information). Failed integrity checks or anomalous results must be treated as potential incidents and proceed through the incident response process.

vi. *Spam and Anti-Phishing Protection*:

Every Information System that sends or receives email must use anti-spam and anti-phishing protection mechanisms at entry and exit points, enabling detection of and incident response to unsolicited messages, spoofed or fraudulent email messages, and especially email soliciting usernames, passwords, or other authenticating information (e.g., account numbers, authorization codes, etc.). These protection

mechanisms must be (i) centrally managed by agency, EOHHS, or EOTSS, and connected to log-collection facilities and incident management processes; and (ii) automatically updated when new releases are available in accordance with organizational configuration management policy and procedures.

The EOHHS incident response process shall include responses to known or suspected phishing attacks, and EOHHS shall provide a facility for users to report suspected phishing. EOHHS may "phish" users at any time to determine risk posture and may require users who submit information in such a phishing audit to complete additional information security training.

vii. *Data/Input Validation*:

Information Systems must implement controls to verify the source and format of data passed from users to Information Systems, from third-party systems to Information Systems, or between Information Systems, ensuring that malformed requests (including user inputs) are logged and denied. Where practicable, such controls should also be applied to transmissions or between components or subcomponents within a System.

viii. *Prevent Data Leakage in Error Messages*:

Information Systems must generate error messages that provide no more information than necessary for corrective actions, and must not reveal information that could be exploited by adversaries. This includes such measures as ensuring that the system response is the same for situations with valid usernames with invalid passwords and for situations with invalid usernames (i.e., "invalid username or password" rather than "username recognized, but invalid password").

Error messages should not reveal instance-configuration information. For example a web application that cannot connect to its database server should report "unable to connect to database" instead of "database at IP address 1.2.3.4 could not be reached," and a caching proxy or web application firewall should not reveal the name or address of the system it sits in front of. If this kind of information is required for troubleshooting, it may be written to the application/system log, but not shown directly to the user or interfacing system. The information in the system log should be tagged with a unique error identifier, and then the user presented with that error identifier, so that issues can still be traced and resolved, but only by personnel authorized to do so.

ix. *Memory Protection*:

Every Information System must implement protections for its memory, to prevent unauthorized code execution (or minimize the chances of successful exploitation). These protections can range from administratively choosing programming languages (or choosing products based on programming language/platform) that do not allow direct memory access or enforce strict bounds checking, to buffer overflow protection (e.g., Data Execution Prevention or DEP), stack canaries, the NX (No-

Execute) bit, and/or Address Space Layout Randomization (ASLR).

XXI. DEFINITIONS

TERM	DEFINITION
Acceptable Encryption Suites	means encryption that meets all of the following requirements: (a) complies with applicable federal, state, and local laws, federal and state Executive Orders, directives, policies, regulations, and standards of industry best-practice; (b) is approved under FIPS 140-2 for use in government; (c) capable of providing authentication assurance according to a certificate trust chain; and (d) is not currently known to be vulnerable to feasible attacks. The category of Acceptable Encryption Suites specifically excludes proprietary (non-public or non-peer-reviewed) encryption, as well as any cipher suite or key length that has been deprecated according to industry best practice or current web browser standards (i.e., Firefox, Chrome, Internet Explorer/Edge). Note that support for Acceptable Encryption Suites is not by itself sufficient: fallback to unacceptable encryption suites must also be explicitly disabled. In particular, as of the drafting of this document, the following algorithms/ciphers are **deprecated and not permitted**: SHA-1, DES, 3DES, RC4, MD5, SSLv2, SSLv3, and TLS-1.0. Acceptable Encryption Suites as of this drafting **include** TLS 1.2 (as long as any weak ciphers are disabled) and TLS 1.3.
Acceptable Use	means a set of rules applied by the owner of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.
Access Coordinator	means the individual identified as being responsible for managing staff access to Information Resources
Access Log	means a list of all requests for individual files that people or bots have requested from a Web site.
ACIO	means Assistant Chief Information Officer.
ACLs	Means Access Control List. It is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges.
Active Directory	means the directory used by the Commonwealth to maintain the identities of users within its network
Active Monitoring	means injecting test traffic into a network and then measuring its performance. These tests can either be one-way or round trip
Agency	means one of the constituent offices, departments, hospitals and Soldiers' Homes defined as being within EOHHS and included in Attachment 9.
Aggregated Logging System	means a system that gathers up disparate log files for the purposes of organizing the data in them and making them searchable.

TERM	DEFINITION
Aggregate Report	means a report that collects data within a selected criteria and aggregates it into totals.
APD	means Advanced Planning Document.
ATO	Means Authorization to Operate. This is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations, including mission, functions, image, organizational assets, etc.
Attack Vector	means the method or type of attack used against a computer system or network.
Audit Finding	means the items identified and reported resulting from a process that evaluates audit evidence and compares it against audit criteria.
Audit Log	means a digital record that is created to document when a change is made to a system.
Baseline	means the secure settings and configuration necessary for the protection of the Information Resource. These settings will be modified as updates, patches, code changes, or process changes are incorporated into the Information Resource.
BCP	means Business Continuity Plan. This is a plan to help ensure that business processes can continue during a time of emergency, disaster or any other case where business is not able to occur under normal conditions.
CIO	means Chief Information Officer.
Collaborative Tools	means software tools or applications that support groups of individuals to accomplish a common goal or objective.
Commonwealth	means the Commonwealth of Massachusetts.
Commonwealth Data	means the information created, maintained, or stored by or on behalf of the Commonwealth in whatever form such data is created, maintained, or stored. For purposes of clarification, Commonwealth Data includes Sensitive Information, but may also include information freely available to the public.
Commonwealth Enterprise	means the interconnected system infrastructure, networks, and information systems used within EOHHS.
Compensating Controls	means mechanisms put in place to satisfy a security requirement that are not explicitly as stated, due to legitimate technical or documented business constraints, but still sufficiently mitigate the risk associated with the requirement.

TERM	DEFINITION
Compliance	means evidence of having met a specific set of policies, standards, laws, frameworks regulations, etc.
Concurrent sessions	means when there is more than one user accessing the same computer resource at the same time or in the same predefined period of time
Configuration	means any arrangements to code, updates, patches and processes to an Information Resource.
COOP	means Continuity of Operations Plan. This is a federally-established policy to ensure that critical functions continue and that personnel and resources are relocated to an alternate facility in case of emergencies.
COTS	means commercial off-the-shelf. These are the products packaged solutions which are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.
CRLs	means Certificate Revocation Lists. It is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.
CSRF	also known as CSRF, Cross-site request forgery. It is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts.
Data Flows	means the movement of data through a system comprised of software, hardware or a combination of both.
Data Mining	means The process of finding anomalies, patterns and correlations within large data sets for the purpose of discovering connections and predicting outcomes.
Development	means a System is in an environment where the structure or operation of that System is being developed or modified in such a way to not impact Production and/or the data contained therein.
Document	means this EOHHS Enterprise Information Security Standards
EMP	means Electromagnetic Pulse. It is considered a short burst of electromagnetic radiation. This kind of burst can come from a variety of sources, including our own sun, but in this case refers to a concentrated pulse from an event like a nuclear detonation that occurs at an extremely high altitude.
Encrypted	means data that has been translated into another form or code to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks.
Endpoints	means remote computing devices such as laptops, desktops, tablets or phones that communicate back and forth with a network

TERM	DEFINITION
EOHHS or the **Secretariat**	means the Commonwealth of Massachusetts Executive Office of Health and Human Services as defined by MGL c. 6A §16 and composed of the Agencies.
EOHHS Environment	means the facilities and information systems under EOHHS control that store, process, or use EOHHS data in any format and for any purpose.
EOHHS Information Resource or **Information Resource**	Information Resources include both technical and non-technical methods of storing, accessing, and processing information. Technical Information Resources include, without limitation: computers (including laptops), servers, printers and other peripherals, smartphones and other mobile devices (including tablets), storage media, network locations or information systems, that are either: 1) developed and/or provided by EOHHS; 2) connected to the EOHHS network, programs, applications, databases, or network shares managed by the Commonwealth or EOHHS; or 3) used to process Commonwealth Data or other Sensitive Information. Non-Technical Information Resources include, without limitation: any printed, handwritten, or other physical forms of Commonwealth Data or other Sensitive Information, such as paper documents and files, microfilm, physical photographs, as well as methods of storing them, such as filing cabinets, desk drawers, and storage rooms.
EOHHS Risk Governance Team	means a group composed of Agency leadership and EOHHS subject matter experts who are able to make determinations and recommendations with respect to risk acceptance for systems with an excessive amount of Risk. Where a System is escalated to the EOHHS Risk Governance Team, the team shall be composed of 1) key leadership from the impacted agencies whose data and environments may be impacted by the Risks which should include the following individuals or their assigns: Commissioner, Chief Financial Officer, Chief Operating Officer, Agency Chief Information Officer, and General Counsel and 2) key subject matter experts from EOHHS IT including the Security Office, IT Operations, and the EOHHS architecture team.
EOTSS	means the Executive Office of Technology Services and Security.
Event	means anything that occurs that impacts operations at EOHHS. Events that are within the scope of *Section X, Incident Response and Security Incident Response Team*, are Reportable Events.
Facility	means any facilities housing EOHHS Information Resources or Information Systems, whether or not owned by an Agency or a third-party, and whether or not operated or staffed by Agency or third-party personnel.
FICAM	means the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative, which is run by the GSA and certifies products and services as FIPS-compliant.

TERM	DEFINITION
Forensic Analyst	is a member of the Security Office generally tasked with assisting with collection of electronic information for forensic matters at EOHHS. With respect to operationalization of this Document, Forensic Analysts are responsible for providing support to the Security Office and to assist with identification of the cause of a Reportable Event and management of tools throughout the Reportable Event to ensure remediation of a Reportable Event.
Form	means the Agency-appropriate identification and classification form an Information System. An example identification and classification form is attached here as Attachment 2.
FTI	means Federal Tax Information. It is a Public Key Certification - A digital certificate containing a public key for an entity and a name for that entity, together with some other information that is rendered un-forgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.
Gap Analysis	means the comparison of a system or organization's current performance with desired performance or future state.
HIPAA	means the Health Insurance Portability and Accountability Act of 1996. This rule created by The U.S. Department of Health and Human Services established set of national standards for the protection of certain health information. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.
IDM	means Integrated Data Management. This is the process of bringing many data sources together to aid the daily functions of a business.
Incident Response Lead	is the member of the Security Office tasked with managing implementation and operationalization of *Section X, Incident Response and Security Incident Response Team*.
Information Resources	means the data and information used by an organization.

TERM	DEFINITION
Information Resource Owner or **Owner**	means the individual or group who has the authority to make decisions about an Information Resource. Typically Information Resources will have at least one "owner" who manages or is responsible for the data contained in the Information Resource. Information Systems have two owners: the IT manager for that Information System and the business or programmatic manager who manages the program or data that the Information System supports or uses, respectively.
Information Security Incident or **Incident**	means any situation due to any action or inaction, internally or externally, that does or could lead to an situation including, but not limited to, compromising the confidentiality, availability, or integrity of: 1) the Commonwealth or EOHHS network and/or environment, 2) Commonwealth Data, 3) EOHHS Information Resources, or 4) an EOHHS location.
Information System or **System**	means any application, system, process, database, or other mechanism for using, processing, manipulating, accessing, and/or storing data. Additionally, while the focus of Information System is for electronic data, Information System need not be limited to electronic data and may include non-technical versions of technical processes (e.g.: a paper database of files stored in a filing cabinet).
Information System Classification	means a process in which organizations assess the data that they hold and the level of protection it should be given. A typical system will include four levels of confidentiality: • Confidential (only senior management have access) • Restricted (most employees have access) • Internal (all employees have access) • Public (everyone has access)
ISA	means Information Sharing Agreement. This is a common set of documented principles that organizations have agreed to follow when sharing information with each other.
ITSM	means It Service Management all the activities involved in designing, creating, delivering, supporting and managing the lifecycle of IT services.

TERM	DEFINITION
Key Account Management practices	means a process of tracking and managing accounts critical to an organization
LDAP	means Lightweight Directory Access. This is a client/server protocol used to access and manage directory information.
Linux	means a type of open source operating system. Linux is software that sits underneath all of the other software on a computer, receiving requests from those programs and relaying these requests to the computer's hardware.
Log Correlation Services	means tools that take data from either application logs or host logs and then analyzes the data to identify relationships.
Logical Separation	means maintaining local and virtual connections separately within a network computing environment in order to optimize information security
MAGnet	means Massachusetts Access to Government network. This is the Commonwealth's WAN, or wide area network.
Malware	means malicious code, such as viruses, trojans, worms, spyware, adware, ransomware, scareware, logic bombs, and the like, regardless of how packaged, delivered, or executed (macros, scripts, executables, in-memory exploitation, etc.).
Manager	a designated point of contact responsible for controlling access to a Facility, identifying the individuals authorized to access a Facility, granting physical access to those individuals, and denying access to all others.

TERM	DEFINITION
Memorandum	means an Authority to Operate memorandum or an Operational Risk Assessment memorandum, as applicable, following the form attached here as Attachment 3.
Non-conformance	means instances in which information assets do not meet specifications, standards or requirements in some manner
OCSP	means Online Certificate Status Protocol. It is the Internet protocol used by web browsers to determine the revocation status of SSL/TLS certificates supplied by HTTPS websites.
PACE	the Commonwealth of Massachusetts Human Resources training application and repository.
Personal Identity Verification credential or **PIV credential**	refers to a US Federal government-wide credential used to access government facilities and systems, and has the meaning and requirements given to it under NIST publication FIPS 201-2 (commonly referred to as the "Common Access Card" or "CAC").
PHI	Means Protected Health Information. This is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services.
Phishing	means a fraudulent attempt to obtain sensitive information such as usernames, passwords, financial information, or other sensitive information by disguising the communication as one from a trusted entity such as a bank, helpdesk, or software/hardware vendor. Phishing is often, though not always, conducted over email.
PII	Means Personally Identifiable Information. This is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples of PII may include name, date of birth, place of residence, credit card information, phone number, race, gender, criminal record, age, and medical records
POA&M	means Plan of Actions and Milestones.
Privacy Incident	means any situation due to any action or inaction, internally or externally, that leads to an exfiltration of Sensitive Information as further defined in Agency privacy policy and procedures.
Production	means a System is in an environment that is in use for business operations that typically contains live and not test data.
Project Intake Form	means the document utilized by EOHHS to initiate or request a project within the Enterprise

TERM	DEFINITION
Public-facing	means any free or paid application or system that the public can access. Public-facing systems often comprise a public-facing component as well as a private side that is available only to internal staff.
Reportable Event	means any Event that impacts EOHHS Information Resources and which is reportable under *Section XI, Incident Response and Security Incident Response Team* as described further in Section XI.a.ii. All Incidents are Reportable Events and are a subset of Reportable Events.
Respondent	the group of application staff, facility staff, and Agency operations staff that respond to an assessment questionnaire.
Risk	A Risk is comprised of the following equation: Threat x Vulnerability = Risk. There is no Risk if a Threat or Vulnerability does not exist. Likewise, a minor Threat or Vulnerability might accompany a high level of Risk depending on the corresponding factor in the equation. NIST 800-30 defines Risk as, "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."
Risk Assessment	means an assessment identifies the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets.
Risk Governance Team	means cybersecurity governance team whose activities involve the development, institutionalization, assessment and improvement of an organization's enterprise risk management and security policies
Role	means the standard business function performed by the individual with respect to the Information Resource.
SCIO	means the Secretariat Chief Information Officer.
Secretariat Security Liaison	is a member of the Security Office generally responsible for interfacing with Agencies to respond to information security questions and issues. With respect to operationalization of *Section X, Incident Response and Security Incident Response Team*, Secretariat Security Liaisons are responsible for providing support to the Security Office and to work with Agencies to ensure remediation of a Reportable Event.
Security Office	means the EOHHS Security Office.
SEIM	means Security Event & Incident Monitoring system, a database-driven event correlation tool.

TERM	DEFINITION
Sensitive Information	means any Commonwealth Data not made freely available for public consumption whether written, electronic, or otherwise stored, which may include: Protected Health Information, as that term is defined under HIPAA (45 CFR Parts 160 to 164); "personal data," as defined in M.G.L. c. 66A; "personal information," as defined in M.G.L. c. 93H; "personally identifiable information," as used in 45 CFR §155.260; "patient identifying information," as defined in 42 CFR Part 2; and any other individually identifiable information that is treated as confidential under applicable law regulation or other legal obligation to which EOHHS or an Agency is subject (including, for example, any state and federal tax return information or Social Security Administration information) in whatever form such data is created, maintained, or stored.
Sensitive Information, High or **Highly Sensitive Information**	includes, but is not limited to, federal "secret" clearance level materials (and above), personally identifiably AIDS and other infectious disease data, nuclear materials databases, and CJIS data.
Service and Support Desk	means the EOHHS Service and Support Desk, available at (617) 994-5050 or at the email addresses available at http://eohhs-web.EOHHS.govt.state.ma.us/IT/agency-email-addresses.asp.
Session Hijacking	also known as cookie hijacking and it is the exploitation of a valid computer session. It is to gain unauthorized access to information or services in a computer system.
Session replay	it is the ability to replay a visitor's journey on a web site or within a mobile application or web application. Replay can include the user's view (browser or screen output), user input (keyboard and mouse inputs), and logs of network events or console logs.
Shared Drives	means drives that let users quickly share files from computer-to-computer, allowing all users on the network drive to access stored files and share files with one another.
SIRT	Means Security Incident Response Team. This is a group within EOHHS tasked with responding to an Incident.
SLA	means service-level agreement. It is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.

TERM	DEFINITION
SMTP	means Simple Mail Transfer Protocol. It is a TCP/IP protocol used in sending and receiving e-mail. is a communication protocol for electronic mail transmission.
Social Engineering Attack	means an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain
Supporting Infrastructure	means electricity, data/voice transmission lines (such as fiber, coaxial, twisted-pair, POTS, or otherwise), wireless (including WiFi, GSM, CDMA, LTE, LMDS, WiMax, point-to-point radio, etc.), and any other telecommunications infrastructure providing service to or otherwise supporting a Facility or Information System. Supporting Infrastructure includes redundant infrastructure, if that redundancy is relied upon to satisfy any controls or requirements outlined in this Document.
Test	means a System is in an environment where the structure and operation of the System may be tested in such a way to not impact Production and/or the data contained therein.
Third Party	means a party external to EOHHS who provides or received data from EOHHS. This could include vendors who receive, process, or use EOHHS information. It could also include federal and state teaming partners who provide us information, such as the Centers for Medicare & Medicaid Services, the Social Security Administration, the Internal Revenue Service, the Department of Revenue, and others.
Third Party Agreement	means an agreement with a third party for the transfer of our data and/or the provision of services. Depending on context, this may mean an agreement with a vendor who is receiving, processing, or using our data or an agreement with a trading partner providing us data. As required by these Standards, we may have imposed on us or will need to impose specific privacy and security obligations.
Threat	A Threat is defined as any natural or man-made circumstance that could have an adverse impact on an organizational asset. This includes Threats like building a data center in an earthquake prone area to allowing data entry into a form field without validating, sanitizing or filtering that entry first. NIST 800-30 defines Threat as “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.”

TERM	DEFINITION
TLS	means Transport Layer Security. It is a protocol that provides authentication, privacy, and data integrity between two communicating computer applications. It's the most widely-deployed security protocol used today and is used for web browsers and other applications that require data to be securely exchanged over a network, such as web browsing sessions, file transfers, VPN connections, remote desktop sessions, and voice over IP (VoIP).
Unix	means an open source, portable, multiuser operating system originally developed in 1969
Virus	A Virus is defined as a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.
VoIP	Means Voice Over Internet protocol. It is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
Vulnerability	A Vulnerability is defined as the absence or weakness of a safeguard in an asset that makes a Threat potentially more likely to occur, or likely to occur more frequently. Common Vulnerabilities are poor coding practices or not changing the default admin password in a System once acquired. NIST 800-30 defines Vulnerability as “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.”

Changelog			
Date	**Version**	**Author**	**Change Summary**
12/9/2019	1.0	EOHHS Security Office	Effective Date – Approved by Secretary Sudders

ATTACHMENT 1: EOHHS ACCEPTABLE USE POLICY

Commonwealth of Massachusetts Executive Office of Health and Human Services

INTRODUCTION

This Policy applies to all Users of EOHHS Information Resources. In furtherance of your job duties, you may be required or requested to access EOHHS Information Resources and only for the purpose of completing such duties. Your use of EOHHS Information Resources may be monitored, recorded, and audited. EOHHS has the right to review your files and emails at any time and for any reason without your prior consent. **Especially when using Technical EOHHS Information Resources (as defined below), you should have no expectation of privacy.** Unauthorized or improper use of EOHHS Information Resources may result in disciplinary action, as well as civil and criminal penalties.

You are responsible for using EOHHS Information Resources responsibly, in accordance with your job duties, and for protecting these resources against unauthorized or unpermitted use.

This Policy updates and supersedes the EOHHS Acceptable Use Policy, Version 1.0, dated 11/17/2015.

This Policy covers the following subjects:

1. Acceptable Use
2. Passwords
3. Equipment
4. Data Handling
5. Communications
6. Incident Reporting

By using an EOHHS Information Resource, you agree to the terms of this Policy.

DEFINITIONS

"Agency" means one of the offices, departments, hospitals and Soldiers' Homes defined as being within EOHHS pursuant to MGL c. 6A §16.

"Commonwealth" means the Commonwealth of Massachusetts.

"Commonwealth Data" means the information created, maintained, or stored by or on behalf of the Commonwealth in whatever form such data is created, maintained, or stored. For purposes of clarification, Commonwealth Data includes Sensitive Information, but may also include information freely available to the public.

"Devices" means a subset of EOHHS Information Resources which includes, without limitation: computers (including laptops), peripherals such as printers and monitors, desk phones, headsets, smartphones, cell phones, portable storage media and other equipment capable of utilizing, accessing, or storing Commonwealth Data or EOHHS Information Resources.

"EOHHS" means the Commonwealth of Massachusetts Executive Office of Health and Human Services as defined by MGL c. 6A §16.

"EOHHS Information Resource" EOHHS Information Resources include both technical and non-technical methods of access to, processing, and storing information. Technical EOHHS Information Resources

include, without limitation: computers (including laptops), servers, printers and other peripherals, smartphones and other mobile devices (including tablets), storage media, network locations or information systems 1) developed and/or provided by EOHHS; 2) connected to the EOHHS network, programs, applications, databases, and network shares managed by the Commonwealth or EOHHS; or 3) used to process Commonwealth Data or other Sensitive Information. Non-Technical EOHHS Information Resources include, without limitation: any printed forms of Commonwealth Data or other Sensitive Information, such as paper documents and files and methods of storing them, such as filing cabinets.

"Policy" means this Acceptable Use Policy.

"Portable Device" means laptops, smartphones, cell phones, tablets, flash drives and other portable devices.

"Sensitive Information". Any Commonwealth Data not made freely available for public consumption which may include Protected Health Information, as that term is defined under HIPAA (45 CFR Parts 160 to 164); "personal data," as defined in M.G.L. c. 66A; "personal information," as defined in M.G.L. c. 93H; "personally identifiable information," as used in 45 CFR §155.260; "patient identifying information," as defined in 42 CFR Part 2; and any other individually identifiable information that is treated as confidential under Applicable Law (including, for example, any state and federal tax return information) in whatever form such data is created, maintained, or stored.

"System and Support Desk" means the EOHHS System and Support Desk, available at (617) 994-5050 or at the email addresses available at http://eohhs-web.EOHHS.govt.state.ma.us/IT/agency-email-addresses.asp.

"User" means any individual who, in the course of doing business, accesses EOHHS Information Resources. Users include all EOHHS employees, workforce contractors, and third party contractors or vendors performing work with or on behalf of EOHHS. Where a member of the public access an EOHHS Information Resource under the direction of or while being attended by a User (even if not permitted to access such EOHHS Information Resource) then that User is responsible for the member of the public's actions.

ACCEPTABLE USE

This section describes the general "do's" and "don'ts" with respect to EOHHS Information Resources and what constitutes generally acceptable and unacceptable use of EOHHS Information Resources.

You should use the EOHHS Information Resources provided to you in furtherance of performing your job duties. In using EOHHS Information Resources, you must comply with all related federal and state laws, policies, and processes for use of EOHHS Information Resources including, but not limited to, compliance with Privacy Act of 1974. In order to do so, you should understand and comply with EOHHS annual training and education requirements and complete Security Awareness, Privacy, and other necessary training modules upon hire and annually thereafter, or on a schedule otherwise required by EOHHS. Those trainings will provide the background and information necessary to abide by precepts of acceptable use. You are required to comply with the guidelines provided in those trainings regarding use of EOHHS Information Resources. If in doubt about a specific activity, you are advised to consult with your manager and/or contact the System and Support Desk to be put in contact with the EOHHS Security Office.

Access to EOHHS Information Resources may only be granted to you if you have a job-related need. Additionally, access may only be granted to you to the extent necessary to complete the scope of your job duties. Accounts to access EOHHS Information Resources are provided to you only for your use of the information system. **Under no circumstances may you share your account information, including passwords, or allow another individual to access EOHHS IT Resources with your account. You are responsible for all actions taken using your accounts.** Additionally, you should not independently grant access to EOHHS Information Systems, unless within the scope of your job duties. In the event you are required to grant access to someone else for EOHHS Information Resources, you should ensure that you are doing so as required by law or based on programmatic need and only to the extent necessary for legal compliance or to fulfill that programmatic need.

Unless expressly part of your job duties, regardless of the type of access you have, you must never attempt to bypass access control measures or view, modify, or delete or destroy parts of any EOHHS Information Resource. If your job duties or responsibilities change, your need to access EOHHS Information Resources may change. Your manager is responsible for communicating those access changes to the System and Support Desk ***immediately.*** To that effect, any new employee access or terminated employee access must also be communicated to the System and Support Desk ***immediately***. If you discover that you have access beyond what is allowed, you must notify your manager and the System and Support Desk ***immediately*** so that your access may be adjusted appropriately.

EOHHS Information Resources are the property of EOHHS and the Commonwealth. EOHHS owns the data created or stored on these systems, including all email messages and the information they contain. **You do not own Information Resources on the EOHHS Network and should have no expectation of privacy in those Information Resources—including your MassMail emails.** If any data must be accessed or reviewed by the EOHHS Security Office during the course of a vulnerability assessment, investigation, or otherwise, the EOHHS Security Office will access such data as needed. Accessing that data will be coordinated—if feasible—through the respective EOHHS ACIO and program or project manager.

Any activity that you take on the network or with respect to EOHHS Information Resources that violates State and Federal law is prohibited. Those activities include using EOHHS Information Resources to copy, distribute, utilize, or install unauthorized copyrighted materials or any activity that might violate law and policy related to information protection (e.g., hacking, spamming, etc.). Furthermore, any activity such as viewing, creating, storing, and/or processing pornographic or other offensive or graphic content on EOHHS Information Resources is prohibited.

In addition, you may be disciplined for undertaking certain activities both within and outside of the workplace that relate to your employment at EOHHS. Activities that will adversely impact the workplace by causing the agency to not operate efficiently or effectively and/or create a hostile work environment include, but are not limited to:

- Sending harassing, threatening or offensive communications to other Users or members of the public; or
- Sending communications, including social media posts, that are disparaging towards or reflect poorly on other Users, the populations served by EOHHS, your Agency, EOHHS, or the Commonwealth.

You may not use EOHHS Information Resources for the purpose of utilizing, creating, storing, and/or processing your personal data, such as music, videos, family photographs, and personal documentation. This includes accessing your personal email accounts and connecting to social media (unless a function of your job duty). Streaming music and videos over Commonwealth networks, unless explicitly required as a function of your work for EOHHS, is also prohibited.

When not using EOHHS Information Resources, you must log off, lock, or terminate your session with those EOHHS Information Resources. You must also ensure that your computer or Portable Device automatically logs off or locks when not in use such that a password is needed to log in to the device. You may not install on any Device an automated sign-on system, password, or access phone numbers; a password must be required to be input by you each time an EOHHS Information Resource is accessed. Failure to abide by these log-on requirements could permit unauthorized access with your credentials.

You are accountable and responsible for all actions you take or which are undertaken with your account credentials while using EOHHS Information Resources. Failure to comply with the requirements set forth in this Policy may result in suspension of your access and/or disciplinary action, up to and including termination of employment or removal from a contract for contractor personnel. In some cases, violations may be grounds for civil action or criminal prosecution, **including fines and/or jail time**. Sanctions for non- compliance will be handled in accordance with applicable laws and regulations, collective bargaining agreements, civil service rules, and/or contractual agreements relating to third-party workforce.

You may seek exceptions to specific requirements in this Policy if absolutely necessary to fulfil your job duties. In order to do so, you must make a request in writing to your Agency's ACIO and corresponding business contact explaining in detail: 1) the acceptable use provision sought for exception, 2) the form of the exception, 3) the business justification for the exception, and 4) why the User cannot perform their job duties without the exception. The exception will be treated as a "Critical" level Risk pursuant to the Authorization to Operate and Operational Risk Assessment Policy and Process. If you are denied an exception, you may not attempt to implement the exception through a workaround or "self-help."

PASSWORDS

All Device passwords (provided by EOHHS or used to access EOHHS Information Resources) must meet the following minimum requirements:

- Be twelve (12) characters in length at minimum; and
- Contain one of the following characteristics:
  - One (1) upper-case letter,
  - One (1) lower-case letter,
  - One (1) number, and
  - One (1) special character (! @ # $ % ^ & * ( ) _ + = [ ] \ | ' " : ;< > ? / .).

The security office recommends that Users try to make longer passphrases. The more seemingly random the passphrase (to others), the better. For example, "P4ssword!" is much less secure than "Mytruckbatterydied!" which is much less secure than "Badtrucknopower!".

Passwords must be changed a minimum of every sixty (60) days and may not be repeated for twenty five (25) iterations. If you have multiple accounts to access EOHHS Information Resources, you must not

use the same password for those accounts. Compromised passwords must be changed immediately. If you believe that one of your Information System accounts has been compromised, even if you are unsure of that, err on the side of caution and change your password, even if not directed to do so.

Passwords or any other authentication mechanism must never be stored in printed or written form in any easily accessible place. If passwords are stored digitally, they must not be stored in a clear-text or human-readable format. The Security Office recommends that you never store passwords in an unsecured fashion. Ideally, you should memorize your passwords. If you cannot memorize your passwords, write them down in a place where they will not be easily found (e.g.: store them in a locked drawer, cabinet, or your wallet) or store them digitally in an encrypted format.

Passwords must not be shared or disclosed with anyone, including other EOHHS employees. System and Support Desk staff will never ask you for your password and you should not share your password with System and Support Desk staff. Do not allow web browsers or applications to store passwords and login information. If possible, you should shield keyboards from view when passwords are being entered.

EQUIPMENT

You may use EOHHS-provided Devices to access and store Commonwealth Data and other EOHHS Information Resources. You may sometimes use personally-owned Devices to access Commonwealth Data and other EOHHS Information Resources. The conditions under which you may use a personally-owned Device are described further in this Section. Some Commonwealth Data and EOHHS Information Resources may require special configurations or may be limited in how or where they may be accessed. You must consult with the "owners" or managers of those EOHHS Information Resources to ensure that access is being conducted appropriately.

You must abide by all policies and procedures related to the use of Devices and other office equipment. The most current versions of any policies and procedures will be posted on the Security Office Intranet site, at http://eohhs-web.EOHHS.govt.state.ma.us/wp/informationsecurity.aspx. Devices and other office equipment are provided by EOHHS for official use only and in furtherance of your job duties. EOHHS does not condone personal use of EOHHS-provided Devices. Any Device that uses, accesses, or stores Commonwealth Data, including personal Devices, may be monitored, recorded, and audited. EOHHS has the right to review any information accessed, stored, printed, copied, or otherwise utilized on Devices at any time and for any reason.

Any Device used to access or process EOHHS Information Resources must be password protected. You must also ensure any Device used to access or process EOHHS Information Resources automatically locks after a time period consistent with EOHHS requirements and that a password is required to unlock the Device. Consistent with this, you must not program any Devices with automated sign-on sequences, automated password completion, or remote access phone numbers; you must enter a password each time you access a Device.

Downloading and installation of software applications onto EOHHS-provided Devices is prohibited without prior approval. You must not circumvent administrative lockouts or permissions in an attempt to install such software applications. Altering code, introducing malicious content, tampering with another person's account, denying service, port mapping, or engaging a network sniffer outside of the scope of your explicit job duties is prohibited. Even if you have a legitimate job-related reason to engage in these activities, you must seek approval as required by EOHHS.

In order to use a personally-owned Device to access EOHHS Information Resources, you must: 1) receive permission from your supervisor to use personally-owned equipment and 2) present the personally-owned equipment to the EOHHS Security Office for inspection and certification to use the personally-owned equipment. The Security Office or your supervisor may determine that access to EOHHS Information Resources may need to be conducted through VPN. Additionally:

a) EOHHS may monitor, record, and audit use of personally-owned Devices when accessing EOHHS Information Resources. You should not have an expectation of privacy when using the personally-owned Device to access EOHHS Information Resources.
b) EOHHS may require specific encryption, virus protection, anti-spyware, firewall/intrusion detection, and other software or settings to be installed on the personally-owned Device prior to that Device accessing EOHHS Information Resources. EOHHS may also require that such software is configured to meet EOHHS configuration requirements prior to connection to EOHHS networks. EOHHS may further require that certain software or certain kinds of software not be installed on a personally-owned Device due to the security vulnerabilities that may be introduced. You must implement those requirements and may not modify or deviate from requirements.

You may not use personally-owned Devices to store Commonwealth Data or EOHHS Information Resources. You should only store Commonwealth Data or EOHHS Information Resources on the appropriate network drive (individual or shared) to which you have access or EOHHS-provided portable media which has been provided for the purpose of storing specific Commonwealth Data or EOHHS Information Resources. Any removable or portable media used to store such information must be encrypted and password protected. When not in use, portable media must be secured in a desk or filing cabinet which can lock or be carried with you securely at all times.

The foregoing requirements related to Devices also apply Portable Devices. However, there are a number of additional requirements specific to Portable Devices.

Portable Devices, to the extent technically possible, must have disk-level encryption installed and enabled. Portable Devices should never be used to store sensitive Commonwealth Data, including PII or PHI. You are ultimately responsible for the Portable Devices and will be responsible for the loss of stored data on a Portable Device if the Portable Device is lost or stolen. The Security Office recommends that you keep devices under your physical control at all times and take all necessary precautions to protect Portable Devices against loss, theft, damage, abuse, or unauthorized use.

When traveling, you must keep Portable Devices under your physical control at all times. Consequently, you must not place any Devices in checked luggage. Additionally, you must not store any Devices in a publically accessible locker or storage space (such as at an airport, a train or bus station). At security checkpoints, such as airport security, you must place any Devices on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If delayed, you must visually monitor the Devices to the extent possible until you can retrieve the Devices.

You must avoid leaving any Devices in in a hotel room. If you must leave a Device in a hotel room, you must lock it inside a safe provided by the hotel. If a safe is not available, you must keep the Device with you. You must never leave a Device unattended in an automobile, even if the vehicle is locked. Public or

shared computers (e.g. hotel business computers, library computers, etc.) should not be used to access EOHHS Information Resources or Webmail access.

Portable Devices must not be simultaneously connected to the EOHHS network and any kind of non-EOHHS network connection (including physical, wireless, or other connection). The exception to this is where a Portable Device is a smartphone and is required to connect to both a cellular network to function and an EOHHS wireless network.

You may be asked to return or hand-over Portable Devices to EOHHS for security-related repairs and inspections. Users must comply with these requests promptly and make the device completely available to EOHHS. Failure to do so may result in the loss of privileges to keep the Device (if an EOHHS provided Device) or access the EOHHS network with it (if a personally-owned Device). In the course of an inspection or update, EOHHS may need to make modifications to the Device, including software updates, which may delete all data on the Device. EOHHS has no responsibility for data improperly stored on a Device. If, during the course of an inspection, the Security Office finds software EOHHS determines should not be on a device, that software is subject to deletion without notice. This includes screen savers, games, software downloaded from the Internet, software brought from home, and software provided by other state agencies.

Unsecured wireless communication protocols (like Bluetooth and Infrared transmission) must not be used at an EOHHS location or when accessing EOHHS Information Resources. Wireless communication protocols, including the EOHHS Public Access Wi-Fi, must not be used to transmit PII, PHI, SSA and FTI data, or similarly sensitive data.

DATA HANDLING

You must ensure the proper handling of Sensitive Information according to applicable requirements, including but not limited to federal and state law, third party agreements, Commonwealth Executive Orders, and EOHHS policy and process. Your Agency may also have additional specific data privacy requirements with respect to Sensitive Information you may access. You must abide by those requirements at all times.

You must not divulge any Sensitive Information obtained through or in connection with your employment with the Commonwealth to any unauthorized person or organization or in violation of applicable requirements including, but not limited to federal and state law, third party agreements, Commonwealth Executive Orders, and EOHHS policy and process.

You may only use Sensitive Information in furtherance of and consistent with your job duties. You must not use, or permit others to use, any Sensitive Information that is not available to the general public for private purposes or personal use. You may only modify Sensitive Information in furtherance of and consistent with your job duties. You must not remove official documents or records from files or otherwise alter Sensitive Information for personal or inappropriate reasons. Falsification, concealment, mutilation, or unauthorized modification of Sensitive Information is prohibited and, in many cases, may subject you to criminal and civil penalties.

If you must dispose of Sensitive Information, you must do so properly. EOHHS requires that information be disposed of pursuant to the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88. This means that:

(a) Non-technical EOHHS Information Resources (e.g.: paper documents) must be appropriately shredded such that the information they contain cannot be reconstructed. If your location has EOHHS-provided shredder bins, you must dispose of Sensitive Information there.
(b) Technical EOHHS Information resources must be completely wiped prior to disposal such that the data once stored on them is practically unrecoverable. You must contact your local IT Site Owner or the EOHHS Security Office to assist you with such destruction.

Prior to any data deletion or destruction, ensure you are in compliance with records retention guidelines pursuant to the Massachusetts Statewide Records Retention Schedule.

COMMUNICATIONS

Internet activities that may impact the confidentiality, integrity or availability of EOHHS information and information systems, or cause degradation of network services, are prohibited unless otherwise expressly permitted for official duties. You should not use EOHHS Information Resources to browse the internet for personal use. In no event may you host, set up, administer, or operate any type of public-facing server on any EOHHS network. Additionally, the use peer-to-peer (P2P) file sharing over the EOHHS network or on EOHHS Information Resources is prohibited. This includes any storage platforms such as Dropbox and Google Drive.

You may only use your MassMail email address in furtherance of your job duties and must not use it for personal matters. Most emails transmitted over MassMail are considered public records and may be disclosed if requested. Except for limited personal use, you must not transmit or distribute via EOHHS email any non-work related information about another employee. Improper use includes, but is not limited to broadcasting inappropriate messages (e.g., unsolicited personal views on social, political, religious, or other non-business matters; email chain letters; etc.) to Commonwealth mailing lists or other Users.

You may not transmit or store Commonwealth Data to or from personal email accounts (e.g. Yahoo, Gmail, Comcast, etc.). You must also not transmit Commonwealth Data to third parties via email outside of the scope of your job duties. You should not forward e-mail messages received through MassMail to addresses outside of MassMail unless required by your job duties.

MassMail email addresses are never to be sold or otherwise shared, disseminated, or used in any unofficial manner. You are encouraged to use your MassMail addresses to sign up for third-party work-related electronically distributed newsletters or magazines. You are, however, prohibited from using your MassMail address to sign up for third-party non-work-related electronically distributed newsletter or magazine.

If you receive an email message from any source requesting personal or organizational information or asking to verify accounts or security settings (a phishing email), you must treat the receipt of the email as a “Security Incident.” Similarly, you should treat emails that you receive from an unknown third party that implore you to click a third party link or download an attachment as “Security Incidents.” Do not click the link, download the attachment, or open the attachment. You should follow the incident reporting process outlined in the “Incident Reporting” section below in all of those cases. Additionally, you should also delete the message after forwarding it.

All official Commonwealth email communications must be conducted through a MassMail email account. Personal or private email addresses should not be used for business purposes. Use of personal or private email addresses may make the contents of those email accounts subject to disclosure and review by the Commonwealth and/or adverse third parties in a claim or cause of action against the Commonwealth.

EOHHS reserves the right to log and monitor all traffic that enters or leaves Commonwealth managed networks. Access and use of email via a technical EOHHS Information Resource should not be considered private.

Users who are identified as being a source of unauthorized intrusion or otherwise conducting prohibited activities on the network may be disconnected from the network. Re-establishing connection will be at the discretion of the EOHHS Security Office in consultation with the User's senior management.

All electronic messages created or received by state employees using the Commonwealth's information technology resources are public record under the Commonwealth's Public Records Law, M.G.L. c. 66, § 10, and most are therefore subject to public scrutiny. All such electronic messages are also records subject to the Commonwealth's Records Conservation Law, M.G.L. c. 30, § 42, and must be disposed of, or retained according to the agency's disposition schedule and the records retention guidelines pursuant to the Massachusetts Statewide Records Retention Schedule. The majority of such messages are also potentially discoverable communications for purposes of litigation. Agency heads and organization authorities must ensure that all electronic communications, are retained, disposed of, and disclosed, in compliance with the Public Records Law, the Massachusetts Statewide Records Retention Schedule, and the relevant discovery rules.

The Commonwealth VPN Solution provides remote access to a wide variety of technical EOHHS Information Resources for authorized users from any personal computer with a web browser that supports 128 bit encryption. The Commonwealth VPN Solution also provides the ability to telework remotely in emergency, contingency, or COOP situations.

When working at an alternate workplace (including from home), you must follow security practices that are at least as restrictive as those required at your primary workplace. Users who use VPN must protect the privacy and security of all EOHHS data and equipment in the same manner as required when working at an EOHHS location.

INCIDENT REPORTING

All incidents must be reported to the System and Support Desk immediately. An incident may include, but is not limited to, one of the following events:

- Loss or theft of a Device,
- Compromise of your account credentials,
- Loss of Commonwealth Data,
- Inappropriate or misdirected transmission of Sensitive Information,
- Presence of a virus on a Device,
- Suspicious email; and

- Anomalous System performance.

If in doubt, err on the side of caution and report an event as an incident. Failure to report an incident may lead to the impact, extent, or effect of the incident being exacerbated. If you fail to report an incident and it gets worse, you are responsible for the expanded scope of the incident and may be held accountable for such expanded scope.

If you report an incident, you may be contacted by the Security Office to provide additional information or be directed to take steps to resolve the incident. You must comply with such Security Office requests and direction to resolve an incident.

ATTACHMENT 2: INFORMATION RESOURCE INVENTORY FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Application Name: _____
Date: _____

Application Inventory Instructions

This questionnaire is being sent to all application managers in order to inventory all applications within the EOHHS Environment. For purposes of this review "application" is a generic term intended to cover systems, applications, databases, or other mechanisms that hold, transmit, or otherwise process data. The term should be interpreted as broadly and liberally as possible.

The following clarifications and explanations have been included to assist with completing the questionnaire. If you have additional questions, please contact Aaron Weismann at (617) 689-2844 or Aaron.Weismann@State.MA.US.

- Question 1: please provide the name of the application, spelling out any acronyms.
- Question 2: please provide a high-level explanation of your application functionality. We recommend keeping this to a paragraph in length, but more text could be appropriate based on the complexity and functionality of your application.
- Question 3: additional details and explanation have been provided for MassHealth functions/activities
    - Member/consumer assistance – does your application support or is your application involved in activities related to providing assistance to MassHealth applicants or members?
    - Eligibility determinations – does your application support determinations of eligibility for benefits offered by MassHealth?
    - Eligibility appeals – does your application support or is your application involved in appeals for denials of eligibility?
    - Premium billing/co-payment – does your application support or is your application involved in premium billing or co-payments?
    - Managed care/plan enrollment – does your application support or is your application involved in enrollment activities for managed care or healthcare plans supported by MassHealth or otherwise?
    - CAC program – does your application support or is your application involved in activities related to the Certified Application Coordinator program, which is to assist individuals with applying for MassHealth membership?
    - Estate recovery – does your application support or is your application involved in activities related to the MassHealth estate recovery program, which is to reimburse MassHealth from a decedent's estate under certain circumstances for care provided to them by MassHealth?
    - Casualty recovery –does your application support or is your application involved in activities related to the MassHealth casualty recovery program, which is to recover the cost of medical services provided to MassHealth members with respect to an accident or injury, to the extent such costs are reimbursed or otherwise covered by a third party (such as the person or organization that caused the accident or injury, workers' compensation or other insurance)?
    - Premium assistance – does your application support or is your application involved in activities related to the MassHealth premium assistance program, which helps individuals pay for healthcare when they are not eligible for MassHealth coverage, but are eligible for a credit towards private healthcare premiums?
    - Other third party liability (TPL) – does your application support or is your application involved in activities related to the determination of third party healthcare coverage?

Application Name: _____
Date: _____

- Oversight/financial integrity – does your application support or is your application involved in activities related to the MassHealth oversight and financial integrity group for activities like fraud prevention?
- Quality improvement – does your application support or is your application involved in activities related to improvement of benefits and care delivery?
- Reporting to CMS – to your knowledge, is your application directly or involved with any data reporting to CMS?

- Question 4: please provide a narrative explanation of the architecture/operation of your application.
- Question 5: what kinds of data does your application interact with? The data in the chart is organized as follows:

First Name/Initial	☐	Last Name	☐
Home Address	☐	Home Zip Code	☐
Work Address	☐	Work Zip Code	☐
Provider Number	☐	Employee ID	☐
Drivers License/State ID No.	☐	Financial Account #	☐
Tax ID	☐	SSN	☐
Credit/Debit Card #	☐	FTI	☐
Commonwealth Data	☐	MassHealth Number	☐
Hub Data	☐	MassHealth claims/encounter data	☐
MassHealth eligibility information	☐	MassHealth enrollment information	☐
Other Confidential Information (please specify):_____	☐	Health information (please specify):_____	

Key

Personal Information
Financial Information
Health / Claims Information
Federal Tax Information
Federal Hub (HIX) Data – also considered health information
Data generated by the Commonwealth
Other misc. confidential data

Additional details and explanation for each data point have been provided below:

- First Name/Initial – does your application interact with first names or initials (MassHealth Members, Providers, etc.)
- Last Name – does your application interact with last names (MassHealth Members, Providers, etc.)
- Home Address – does your application interact with home addresses (MassHealth Members, Providers, etc.)
- Home Zip Code – does your application interact with home zip codes (MassHealth Members, Providers, etc.)
- Work Address – does your application interact with work addresses (MassHealth Members, Providers, etc.)
- Work Zip Code – does your application interact with work zip codes (MassHealth Members, Providers, etc.)

- Provider Number – does your application interact with provider numbers (NPIs, etc.)
- Employee ID – does your application interact with employee IDs (EOHHS employee ID numbers, EINs, etc.)
- Driver's License/State ID No. – does your application interact with driver's license or other legal state identification numbers?
- Financial Account # - does your application interact with financial account numbers (bank account, etc.) other than credit and debit card numbers?
- Tax ID – does your application interact with state or federal tax identification numbers?
- SSN – does your application interact with social security numbers?
- Credit/Debit Card # - does your application interact with credit or debit card numbers?
- FTI – does your application interact with federal tax information, which is a specific kind of information provided by the IRS which contains information obtained from tax returns
- Commonwealth Data – does your application interact with data generated by the Commonwealth?
- MassHealth Number – does your application interact with MassHealth Member numbers?
- Hub Data – does your application interact with data from the federal Hub (part of HIX)?
- MassHealth claims/encounter data – does your application interact with claims or encounter data for treatment or other healthcare services provided to MassHealth Members?
- MassHealth eligibility information – does your application interact with information about eligibility for MassHealth benefits?
- MassHealth enrollment information – does your application interact with information about enrollment for MassHealth Membership?
- Other Confidential Information – does your application interact with any other information that might be considered "confidential" which is not otherwise included in the above list? Please specify generally what that information is.
- Health Information – does your application interact with other "health information" which is not otherwise included in the above list? Please specify generally what that information is.

- Question 6: please list the total number of users for your application broken down by internal and external user numbers.
- Question 7: please use the chart to explain what external connections your system has. This should be a comprehensive list of all external access to the system or transmission from the system. For non-EOHHS external connections, please feel free to use a high level of abstraction for the connection (e.g.: DOR, Providers, etc.). For internal systems, please list all systems and sub-systems to which you know your application connects. Please also include an explanation of any acronyms or system function (e.g.: AIMS is the "Account Information Management System" or is a system used for user account access management).
- Question 8: please list the vendors who access the application, whether that application is for development or ongoing access to or management of data. Please list the kinds of data accessible by each vendor. Also, please indicate whether or not (by answering "yes" or "no") there is data not accessible by your vendors.
- Question 9: please indicate whether or not your application is publicly accessible, the kinds of data that are publicly accessible, and whether or not there is data not accessible by the public.
- Question 10: please indicate whether or not your application is accessible by other third parties (including auditors, other agencies, and vendors not performing development or management activities of your application), who they are, what kinds of data is accessible by them, and whether or not there is data not accessible to those third parties.

Application Name: _____
Date: _____

- Question 11: please indicate all auditing that your application performs (manual or automatic).

Application Name: _____
Date: _____

1. What is the name of your application?
2. Please explain generally what your application does.
3. Please indicate if your application is involved with/supports any of the following MassHealth functions/activities:

Member/consumer assistance	☐	Estate recovery	☐
Eligibility determinations	☐	Casualty recovery	☐
Eligibility appeals	☐	Premium assistance	☐
Premium billing/co-payment	☐	Other third party liability (TPL)	☐
Managed care/plan enrollment	☐	Oversight/financial integrity	☐
CAC Program	☐	Quality improvement	☐
		Reporting to CMS	☐

4. Please describe, at a high level, the architecture of your application.
5. What kinds of data are transmitted, processed, manipulated, stored, collected, or otherwise pass through your application?

First Name/Initial	☐	Last Name	☐
Home Address	☐	Home Zip Code	☐
Work Address	☐	Work Zip Code	☐
Provider Number	☐	Employee ID	☐
Drivers License/State ID No.	☐	Financial Account #	☐
Tax ID	☐	SSN	☐
Credit/Debit Card #	☐	FTI	☐
Commonwealth Data	☐	MassHealth Number	☐
Hub Data	☐	MassHealth claims/encounter data	☐
MassHealth eligibility information	☐	MassHealth enrollment information	☐
Other Confidential Information (please specify):_____	☐	Health information (please specify):_____	

Other data (please specify) _____

6. Approximately how many other users (internal and external) have access to your application?
7. Does your Application interface with other systems? Y ☐ N ☐ (If you respond "Y", please fill out the remaining questions in this section; a chart has been provided for your convenience)

    a. What systems does your Application interface with?
    b. Does your application send or receive data?
    c. For each system with which your application interfaces, please describe how your application interfaces with them (e.g.: one or two-way connections, type of connection, persistence of connection, etc.).
    d. For each system with which your application interfaces, please describe what kind of data is transmitted to and from your Application into the other system. *Please use data types referenced in section 5 of this form*.

Application Name: _____
Date: _____

Interfacing System Name	Program Contact for Interfacing System	Send or Receive Data (or both)	Type of connection (e.g.: interchange, SFTP, etc.)	What data transmitted (Please indicate, where possible, if specially protected data like Federal Hub or data received from the SSA is transmitted)

8. Is your application directly accessible by a third party vendor (e.g.: does a non-EOHHS entity do work in your application)? Y ☐ N ☐

    a. Which vendor(s)?
    b. What data is accessible by the vendor(s)?
    c. Is there data that is not accessible by the vendor(s)?

9. Is your Application publicly accessible? Y ☐ N ☐

    a. What data is accessible by the public?
    b. Is there data that is not accessible by the public?

10. Is your application accessible by other third parties (e.g.: auditors, MCOs, EHS constituent agencies, other agencies, etc.)? Y ☐ N ☐
    a. Accessible by whom?
    b. What data is accessible?
    c. Is there data inaccessible to these parties?

11. How does auditing of your application take place, including what logs are maintained, what information is captured in those logs, how long those logs are maintained and how/how often logs are reviewed or analyzed for abnormalities? (A chart has been provided for your convenience)]

Log	Information captured	Length of time log is maintained	Review/analysis method and frequency

Application Name: _____
Date: _____

12. What legal and contractual compliance does your application require? (A chart has been provided for your convenience)

Information Resource:	**BSAS DataMart**
Applicable laws	• MGL c. 66A
Applicable contracts	•
Data Types	• Application logs • Metadata •
Requirements	•

Application Name: _____
Date: _____

Based on the foregoing information, the Security Office has made the following assessment with respect to impact level:

Impact Area	Impact Level	Justification
Confidentiality		
Integrity		
Availability		

Using the high watermark principle, the aggregate impact level for this Application is:
_____.

ATTACHMENT 3: AUTHORITY TO OPERATE/ OPERATIONAL RISK ASSESSMENT MEMORANDUM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

[Authority to Operate/Operational Risk Assessment] Memorandum
for the
Executive Office of Health and Human Services
[Agency]
[Program]
[System]

TO: [Agency ACIO and corresponding business contact]

CC: [EOHHS Risk Governance Team]

FROM: EOHHS Security Office

RE: [System Name] (System)

DATE: [DATE]

I. Introduction

This Memorandum is being transmitted on behalf of the Executive Office of Health and Human Services' (EOHHS) Security Office to identify issues with the named information system and raise awareness of the issues its vulnerabilities pose to the data it contains and the broader EOHHS Environment. The ultimate goal of this Memorandum is to request signoff by the recipients for continued operation of the System. The Security Office recommends that the vulnerabilities not be accepted in their current state and that the issues be remediated within [timeline]. The Security Office further recommends [further recommendations].

[Populate System and program background, including any other considerations for the System]

II. Overview of the Vulnerability/Risks

A. How Risk is Rated

Table 1: Risk Rating in Aggregate

Residual Risk		Likelihood			
		Highly Likely (4)	Likely (3)	Possible (2)	Unlikely (1)
Impact	Critical (4)	Critical (16)	Critical (12)	High (8)	Moderate (4)
	High (3)	Critical (12)	High (9)	Moderate (6)	Low (3)
	Moderate (2)	High (8)	Moderate (6)	Moderate (4)	Low (2)
	Low (1)	Moderate (4)	Low (3)	Low (2)	Low (1)

In order to calculate the risk rating, as outlined in Table 1, above, multiple considerations are taken into account to provide an aggregate rating of the impact of a vulnerability and the likelihood of the vulnerability occurring. The impact is determined by looking at the different kinds of results of a vulnerability being exploited, as outlined in Table 2, below. Once an Impact is identified, it is provided a two numerical ratings. First, it is provided a rating based on the severity of the impact on low to critical scale numerically measured between one and four, respectively. Second, it is provided a rating based on the ease or likelihood of an impact occurring. Again, this is based on the likelihood from low to critical numerically measured between one and four, respectively. By multiplying the two numbers together, the Security Office is able to determine the overall risk rating of a vulnerability.

Table 2: Impact Categories

Impact Categories	Definition
Financial	Financial impact to the Commonwealth based upon a risk being realized.
Reputational	Impact of a loss of confidence from its personnel, constituents, business partners and regulators, which would degrade the Commonwealth's reputation.
Legal and regulatory	Impact could result in observations, recommendations and/or comments from other state entities and/or federal oversight agencies and/or regulators
Operational	The operational impact to processes, people and technology in which Commonwealth employs to achieve its strategy and normal business operations.

Impact Rating	Impact Measurement
Critical	4
High	3
Moderate	2
Low	1

B. System Risks

The following vulnerabilities have been identified for the System:

Finding Group	NIST Control/Policy Impacted	Key Observation	Suggested Remedies from Architecture and Security Teams	Review comment Project	Estimated Fix Date	Risk Rating
Application						

1						
Database						
Quality Assurance						

III. Identification of Risk

A. Breakdown of Vulnerabilities by Risk Level:

Critical		
High		
Moderate		
Low		
		Total Vulnerabilities

Aggregate Risk Level:

B. Next Steps

[Identify recommendations for System, including escalating to the EOHHS Risk Management Team]

IV. Security Office Comments

[Observations, recommendations, other relevant information, etc.]

To Be Executed After Meeting with the EOHHS Risk Governance Team:

After the conclusion of the EOHHS Risk Governance Team Meeting(s) for the System, we have determined:

	To resolve the vulnerabilities in full prior to promoting the System to production

	To accept that the System has potentially significant vulnerabilities that may result in a loss of confidentiality, integrity, or availability of data in the System; to permit the System to operate "as-is" and resolve the vulnerabilities within the next [(1-12) months/(1-3) years]; and develop a remediation plan to be submitted to the EOHHS Security Office within the next 60 days for review and recommendation.

By signing below, we will ensure appropriate remediation of the System. We understand that the Security Office may be required to take additional action based on the contents of the Memorandum, including providing a copy of this Memorandum to EOTSS and other oversight agencies as required by law or policy.

Signed:

[Name, Title ACIO]	Date
[Name, Title Business Contact]	Date

ATTACHMENT 4: CHAIN OF CUSTODY FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Name Of Affected	
Name of Submitter	
Date/Time	
Location	
Incident #	

Description of Evidence	
Item # (mark evidence)	**Description (Model, Serial, Condition)**

Chain of Custody				
Item #	**Date/Time**	**Released By (Signature)**	**Received By (Signature)**	**Comments/Location**

Authorization for Disposal

Evidence recorded and stored for incident # ____ may be destroyed or released to the released to the rightful owners

☐ Evidence will be destroyed

- Items to be destroyed
- Signature of person releasing evidence _____
- Signature of person destroying evidence _____
- Signature of person witnessing destruction _____

☐ Evidence will be released to owner

- Items to be released
- Signature of person releasing evidence _____
- Signature of person receiving evidence _____

ATTACHMENT 5: SIRT EVIDENCE FORM

Commonwealth of Massachusetts Executive Office of Health and Human Services

Incident Response Lead

Summary of Details		
Date/Time		
Name of affected application(s)	•	
Servers, Desktops, hardware affected (include IPs)	•	
External IPs (if applicable)	•	
Attack Vectors (if known)		
Forensic tools being used	•	
Affected Users		
Environment(s) Affected	☐ Development ☐ QA	☐ Test ☐ Production

Checklist items

Logs gathered and secured?	☐ Yes	☐ No
Was the attack occurring prior to being reported?	☐ Yes	☐ No
• If so, is there evidence available?	☐ Yes	☐ No
Does evidence need to be preserved for prosecution?	☐ Yes	☐ No

Analysis

Recommendations for Containment and/or Eradication

Recommendations for Remediation	
Staff Needed for Remediation	
Name	**Role**
Resources needed for Remediation (software patch, tool purchase, etc.)	

Next Steps

Priority	
Business Impact	
Information Impact	
Recovery Impact	
Contact Information for Response Team	
Name and phone number	**Role**

Are external organizations required to assist? ☐Yes ☐No

Contact Information for External Organizations	
Name and phone number	**Role**

Policies and Procedures for Response (if available)
•

Response (internal, external)

Additional SIRT members needed

Name	Role

Information Security Rating

Impact	Characteristics
High	• Threat to human safety. • Adverse impact on a "Critical" or "High" risk rated information asset, including infrastructure, applications and services (see Asset Management Standard). • Financial or legal liability equal to $1m and above to the Commonwealth. • Potential compromise of information classified as confidential information, including PII and other regulated information.
Medium	• Adverse impact on a "Medium" risk rated information asset, including infrastructure, applications and services (see Asset Management Standard). • Financial or legal liability between $1m and $100,000. • Potential compromise of information not intended for public disclosure.
Low	• Adverse impact on a "Low" risk rated information asset, including infrastructure, applications and services (see Asset Management Standard). • Financial or legal liability of less than $100,000.

ATTACHMENT 6: SIRT RESPONSE FORM

Commonwealth of Massachusetts Executive Office of Health and Human Services

The following form should be filled out by the designated team member(s) who will be providing a response to the public or internally to the organization

Name of Responders	Contact Information

Impact

Business Impact	
Information Impact	
Recovery Impact	
Summary of Details	
Audience to be Notified	Public, Colleges, Hospitals, Internal Users
Method of Communication	Email, Telephone, Television, Letter
Time and Date of Incident	
Affected Clients/Business	Internal Users, Website visitors, Payroll
Details on Information Impact	Proprietary information, PHI, Website defacement
Current Status of Incident	Ongoing investigation, Contained, Stopped
What is Being Done	Vendor contacted for patch, Police looking to make arrest, Anti-virus updates being made
Who is Involved	Police, CISO, CIO, FBI

Information Security Impact Rating

Impact	Characteristics
High	• Threat to human safety. • Adverse impact on a "Critical" or "High" risk rated information asset, including infrastructure, applications and services *(see Asset Management Standard).* • Financial or legal liability equal to $1m and above to the Commonwealth. • Potential compromise of information classified as ***confidential information,*** including PII and other regulated information.
Medium	• Adverse impact on a "Medium" risk rated information asset, including infrastructure, applications and services *(see Asset Management Standard).* • Financial or legal liability between $1m and $100,000. • Potential compromise of information not intended for public disclosure.
Low	• Adverse impact on a "Low" risk rated information asset, including infrastructure, applications and services *(see Asset Management Standard).* • Financial or legal liability of less than $100,000.

ATTACHMENT 7: SIRT LESSONS LEARNED FORM

Commonwealth of Massachusetts Executive Office of Health and Human Services

Lessons Learned	
Date	
Time	
Location	
Coordinator	
Incident #	
Attendees	

Summary of Incident
What was done right?
What could be done better?
Recommendations for improvement
Create/Update Policies, Procedures or Training?

Action Items	Person Responsible	Deadline

ATTACHMENT 8: SIRT INCIDENT FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Incident Response Lead

Name	
Date	
Department and Role	
Email Address	
Location	
Phone	

Incident Reporter

Name	
Date	
Department and Role	
Email Address	
Location	
Phone	

Incident Details

Time and Date of Incident	Location

Incident #	

Description of Incident and Type

Current Status of Incident

List of Affected Resources (include applications, servers, users, groups, etc)

Does this appear to require forensics? Explain why

Does this appear to have legal, criminal or litigation ramifications? Explain why

Recovery Time Expectations
Stakeholders that need to be notified
Associated forms filled out for investigation and data collections
Containment Measures
Evidence Collected
Next Steps

ATTACHMENT 9: SIRT TEAM COMPOSITION BY AENCY

Commonwealth of Massachusetts
Executive Office of Health and Human Services

EOHHS (including IT, HR, Finance, the Secretary's Office)	•
MassHealth (including HSN)	•
Department of Transitional Assistance	•
Department of Public Health	• Eileen Sullivan, Elizabeth Scurria Morgan, Lakeisha Applegate, Kelly Driscoll, Al Williams (DPH non-hospital), Jeanne Cannata (DPH hospitals)
BORIM	•
Department of Mental Health	•
Department of Developmental Services	•
Department of Children and Families	•
Department of Youth Services	•
Massachusetts Rehabilitation Commission	•
Massachusetts Commission for the Blind	•
Massachusetts Commission for the Deaf and Hard of Hearing	•
Executive Office of Elder Affairs	•
Veterans Affairs	•
Holyoke Soldiers' Home	•
Chelsea Soldiers' Home	•
Office of Refugees and Immigrants	•

Privacy Officers and/or Designated Legal Contact by Agency

EOHHS	• Sarah Ricardi
MassHealth	• Sarah Ricardi
Department of Transitional Assistance	•
Department of Public Health	• Lakeisha Applegate
BORIM	•
Department of Mental Health	•
Department of Developmental Services	•
Department of Children and Families	•
Department of Youth Services	•
Massachusetts Rehabilitation Commission	•
Massachusetts Commission for the Blind	•
Massachusetts Commission for the Deaf and Hard of Hearing	•
Executive Office of Elder Affairs	•
Veterans Affairs	•
Holyoke Soldiers' Home	•
Chelsea Soldiers' Home	•
Office of Refugees and Immigrants	•

INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE MASSACHUSETTS EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES (STATE AGENCY)

A. PURPOSE: The purpose of this Information Exchange Agreement ("IEA") is to establish the terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein "data") to assist the State Agency in administering certain federally funded, state-administered benefit programs (including state-funded, state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:

- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement ("CMPPA Agreement") attached as **Attachment 1**, governing the State Agency's use of the data disclosed from SSA's Privacy Act System of Records; and
- all other terms and conditions set forth in this IEA and Attachments 2 through 6.

B. PROGRAMS AND DATA EXCHANGE SYSTEMS: (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA's data exchange systems is attached as **Attachment 2**. **Attachment 2** provides a brief explanation of each system, as well as use parameters, as necessary.

TABLE 1

FEDERALLY FUNDED BENEFIT PROGRAMS	
Program	**SSA Data Exchange System(s)**
☒ Medicaid	SDX, BENDEX, SVES IV, QC, PUPS
☒ Temporary Assistance to Needy Families (TANF)	SDX, BENDEX, SVES IV, QC, PUPS
☒ Supplemental Nutrition Assistance Program (SNAP- formally Food Stamps)	SDX, BENDEX, SVES IV, QC, PUPS
☐ Unemployment Compensation	
☐ State Child Support Agency	
☐ Low-Income Home Energy Assistance Program (LI-HEAP)	
☐ Workers Compensation	
☒ Vocational Rehabilitation Services	SDX, BENDEX, SVES IV

☒ Foster Care (IV-E)	**SDX, BENDEX, SVES IV**
☒ State Children's Health Insurance Program (CHIP)	**SDX, BENDEX, SVES IV, SVES I/Citizenship, PUPS**
☐ Women, Infants and Children (W.I.C.)	
☒ Medicare Savings Programs (MSP)	**LIS**
☐ Medicare 1144 (Outreach)	
☒ *Other Federally Funded, State-Administered Programs (List Below)*	
Program	SSA Data Exchange System(s)
Optional and Mandatory State Supplement to the Supplemental Security Income Program (State-funded income maintenance payment under Title XVI of the Social Security Act)	**SDX, BENDEX, SVES IV**
Social Services Block Grant (Under Title XX of the Social Services Act to Pay for In Home Support and Stabilization Services and Domestic Violence Services)	**SDX, BENDEX, SVES IV, QC**
Vocational Rehabilitation Services for the Blind (Cash Reimbursement under SSA Cost Reimbursement Program)	**SDX, BENDEX, SVES IV, QC, PUPS**

(2) The State Agency will use each identified data exchange system ***only*** for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and Federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will:

a) use the **Federal tax information** disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a program listed in 26 U.S.C. § 6103(1)(7) and (8).

b) use **citizenship status data** disclosed by SSA only to determine entitlement of *new applicants* to: (a) the Medicaid program and CHIP pursuant to the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA to receive the *SSA Data Set* through the Centers for Medicare & Medicaid Services' (CMS) Federal Data Services Hub (Hub).

Applicants for Social Security numbers (SSN) report their citizenship data at the time they apply for their SSNs; there is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

C. **DATA EXCHANGE REQUEST FORM (DXRF), FORM SSA-157:** Prior to signing this IEA, the State Agency will complete and submit to SSA a Form SSA-157 DXRF for each of the federally funded, state-administered programs checked in **Table 1** above. SSA will not disclose any data under this IEA until it has received and approved the completed DXRF for each of the programs identified in **Table 1** above.

D. **TRANSFER OF DATA:** SSA will transmit the data to the State Agency under this IEA using the data transmission method identified in **Table 2** below:

TABLE 2

TRANSFER OF DATA
☐ Data will be transmitted directly between SSA and the State Agency.
☒ Data will be transmitted directly between SSA and the Massachusetts Executive Office of Technology Services and Security (State Transmission/Transfer Component ("STC")) by File Transfer Management System (FTMS), a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.
☐ Data will be transmitted directly between SSA and CMS' Hub by a secure method of transfer approved by SSA. CMS will transmit the *SSA Data Set* between SSA and the State Agency pursuant to an agreement between SSA and CMS regarding the use of the Hub.
☐ Data will be transmitted [*select one:* directly between SSA and the Interstate Connection Network ("ICON") *or* through the [name of STC Agency/Vendor] as the conduit between SSA and the Interstate Connection Network ("ICON")]. ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the "Systems Security Requirements for SSA Web Access to SSA Information Through the ICON," attached as **Attachment 3**.

E. **SECURITY PROCEDURES:** The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3551, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the State Agency will comply with SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," attached as **Attachment 4**, as well as the Security Certification Requirements for use of the *SSA Data Set* transmitted via CMS' Hub, attached as **Attachment 5**. The SSA security controls identified under **Attachment 4** of this IEA prevail for all SSA data received by the State Agency, as identified in Table 1 of this IEA. For any tax return data, the State Agency will also comply with the "Tax Information Security Guidelines for Federal, State and Local Agencies," Publication 1075, published by the Secretary of the Treasury and available at the following Internal

Revenue Service (IRS) website: http://www.irs.gov/pub/irs-pdf/p1075.pdf. This IRS Publication 1075 is incorporated by reference into this IEA.

F. **CONTROLLED UNCLASSIFIED INFORMATION (CUI) REQUIREMENTS:** Pursuant to 32 C.F.R. § 2002.16(a)(6), the State Agency must handle any CUI in accordance with Executive Order 13556, 32 C.F.R. Part 2002, and the CUI Registry. The State Agency acknowledges that misuse of CUI is subject to penalties established in applicable law, regulations, or Government-wide policies. The State Agency will report any non-compliance with handling requirements to SSA using methods approved by SSA.

G. **STATE AGENCY'S RESPONSIBILITIES:** The State Agency will not direct individuals to SSA field offices to obtain data that the State Agency is authorized to receive under this IEA in accordance with Table 1. Where disparities exist between individual-supplied data and SSA's data, the State Agency will take the following steps before referring the individual to an SSA field office:

- Check its records to be sure that the data of the original submission has not changed (e.g., last name recently changed);
- Contact the individual to verify the data submitted is accurate; and,
- Consult with the SSA Regional Office Contact to discuss options before advising individuals to contact SSA for resolution. The Regional Office Contact will inform the State Agency of the current protocol through which the individual should contact SSA, i.e., visiting the field office, calling the national network service number, or creating an online account via *my* Social Security.

H. **CONTRACTOR/AGENT RESPONSIBILITIES:** The State Agency will restrict access to the data obtained from SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this IEA. At SSA's request, the State Agency will obtain from each of its contractors and agents a current list of the employees of its contractors and agents who have access to SSA data disclosed under this IEA. The State Agency will require its contractors, agents, and all employees of such contractors or agents with authorized access to the SSA data disclosed under this IEA, to comply with the terms and conditions set forth in this IEA, and not to duplicate, disseminate, or disclose such data without obtaining SSA's prior written approval. In addition, the State Agency will comply with the limitations on use, duplication, and redisclosure of SSA data set forth in the CMPPA Agreement, especially with respect to its contractors and agents.

I. **SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):**

1. The State Agency will ensure that its employees, contractors, and agents:
   a. properly safeguard PII furnished by SSA under this IEA from loss, theft, or inadvertent disclosure;
   b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;

c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.

2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center at 1-877-697-4889. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 6**, to quickly gather and organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.

4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost or breached and bear any costs associated with the notice or any mitigation.

J. POINTS OF CONTACT:

FOR SSA

Boston Regional Office:
Susan Fay
Data Exchange Coordinator
Center for Disability and Programs Support
JFK Federal Building, Room 1925
Boston, MA 02203
Phone: (617) 565-2855
Fax: (617)565-9359
Email: Susan.Fay@ssa.gov and
BO.MA.RO.CPS.Data.Exchange@ssa.gov

Data Exchange Issues:
Donald Scott
Government Information Specialist
Office of the General Counsel
Office of Privacy and Disclosure
G-401 West High Rise
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-8850
Email: Donald.Scott@ssa.gov

Program and Policy Issues:
Michael Wilkins
State Liaison Program Manager

Systems Security Issues:
Jennifer Rutz
Director

Office of Retirement and Disability Policy
Office of Data Exchange, Policy Publications, and International Agreements
Office of Data Exchange
3609 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-4965
Fax: (410) 966-4054
Email: Michael.Wilkins@ssa.gov

Office of Information Security
Division of Compliance and Oversight
Suite 3383 Perimeter East Building
6201 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-0266
Email: Jennifer.Rutz@ssa.gov

Systems Issues:
Jennifer Cullinane, Branch Chief
DBIA/Data Exchange and Verification Branch
of IT Programmatic Business Support
Office of Systems
3-F-3 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-8044
Fax: (410) 966-3147
Email: Jennifer.Cullinane@ssa.gov

FOR STATE AGENCY

Agreement Issues:
Mimi Brown
Assistant General Counsel
Executive Office of Health and Human Services
One Ashburton Place, 11th Floor
Boston, MA 02108
Phone Number: (617) 573-1718
Fax Number: (617) 573-1895
Email Address: Mimi.Brown@state.ma.us

Technical Issues:
Aaron Weismann
Chief Security Officer
Executive Office of Health and Human Services
100 Hancock Street, Room 4020
Quincy, Massachusetts 02171
Phone Number: (617) 689-2844
Fax Number: (617) 573-1895
Email Address: Aaron.Weismann@mass.gov

K. **DURATION:** The effective date of this IEA is July 1, 2020. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section L. below at least 30 days before the expiration and renewal of such CMPPA Agreement.

L. **CERTIFICATION AND PROGRAM CHANGES:** At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of

the programs or data exchange processes listed in this IEA, the parties will modify the IEA in accordance with Section M. below and the State Agency will submit for SSA's approval new Form SSA-157 DXRFs under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

M. MODIFICATION: Modifications to this IEA must be in writing and agreed to by the parties.

N. TERMINATION: The parties may terminate this IEA at any time upon mutual written consent. In addition, either party may unilaterally terminate this IEA upon 90 days advance written notice to the other party. Such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow under this IEA, or terminate this IEA, if SSA, in its sole discretion, determines that the State Agency (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this IEA or the CMPPA Agreement.

O. INTEGRATION: This IEA, including all attachments, constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties, or promises made outside of this IEA. This IEA shall take precedence over any other document that may be in conflict with it.

ATTACHMENTS

1 – CMPPA Agreement
2 – SSA Data Exchange Systems
3 – Systems Security Requirements for SSA Web Access to SSA Information Through ICON
4 – Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration
5 – Security Certification Requirements for use of the *SSA Data Set* Transmitted via CMS' Hub
6 – PII Loss Reporting Worksheet

P. AUTHORIZED SIGNATURES: The signatories below warrant and represent that they have competent authority on behalf of their respective agency to enter into the obligations set forth in this IEA.

The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

SOCIAL SECURITY ADMINISTRATION
REGION I

Linda M Dorn

Linda M. Dorn
Regional Commissioner

6-29-2020

Date

MASSACHUSETTS EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

Marylou Sudders

Marylou Sudders
Secretary

6.29.20

Date

RENEWAL OF THE COMPUTER MATCHING AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES
OF MASSACHUSETTS

SSA Match #6003

Under the applicable provisions of the Privacy Act of 1974, amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o)(2), a computer matching agreement (CMA) will remain in effect for a period not to exceed 18 months. Within 3 months prior to the expiration of such CMA, however, the Data Integrity Board (DIB) may, without additional review, renew the CMA for a current, ongoing matching program for a period not to exceed 12 additional months if:

1. such program will be conducted without any changes; and

2. each party to the CMA certifies to the DIB in writing that the program has been conducted in compliance with the CMA.

A copy of the CMA to be renewed is attached hereto.

The following match meets the conditions for renewal upon signature of the officials authorized in sections VII and VIII of this renewal:

I. TITLE OF MATCH

Computer Matching and Privacy Protection Act (CMPPA) Agreement Between the Social Security Administration and the Executive Office of Health and Human Services of Massachusetts (Match #6003)

II. PARTIES TO THE MATCH

Recipient Agency:	Executive Office of Health and Human Services of Massachusetts (State Agency)
Source Agency:	Social Security Administration (SSA)

III. PURPOSE OF THE AGREEMENT

This CMA between SSA and the State Agency sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 of the Act (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions

of this CMA ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA verifies the Social Security number and discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state-administered benefits from SSA Privacy Act Systems of Records.

IV. ORIGINAL EFFECTIVE AND EXPIRATION DATES OF THE MATCH

Effective Date:	January 1, 2020
Expiration Date:	June 30, 2021

V. RENEWAL AND NEW EXPIRATION DATES

Renewal Date:	July 1, 2021
New Expiration Date:	June 30, 2022

VI. CHANGES

By this renewal, SSA and the State Agency make the following non-substantive changes to the CMA:

In Article XV, "**Points of Contact**," information under subsection B. "State Point of Contact" should be deleted in its entirety and replaced with the following:

B. State Point of Contact

Mimi Brown, Assistant General Counsel
Executive Office of Health and Human Services
One Ashburton Place, 11th Floor
Boston, MA 02108
Phone: 617-573-1718/Fax: 617-573-1895
Email: Mimi.Brown@mass.gov

VII. SOCIAL SECURITY ADMINISTRATION SIGNATURES

Source Agency Certification

As the authorized representative of the source agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any changes for an additional 12 months, subject to the approval of the respective Data Integrity Boards of the parties.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

_____

Anatoly Shnaider
Regional Commissioner
Boston

Date_____

Data Integrity Board Certification

As Chair of the Data Integrity Board of the source agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any changes for an additional 12 months.

Matthew Ramsey — Digitally signed by Matthew Ramsey Date: 2021.01.13 15:01:22 -05'00'

Matthew D. Ramsey, Chair
Data Integrity Board

EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES of MASSACHUSETTS SIGNATURES

Recipient Agency Certification

As the authorized representative of the recipient agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any changes for an additional 12 months, subject to the approval of the respective Data Integrity Boards of the parties.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

MLSudders

Marylou Sudders
Secretary
Massachusetts Executive Office of Health and Human Services

Date 4.06.21

Attachment: Computer Matching Agreement

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES
OF MASSACHUSETTS

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) between the Social Security Administration (SSA) and Executive Office of Health and Human Services of Massachusetts (State Agency) sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 of the Act (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions of this Agreement ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA verifies the Social Security number (SSN) and discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state-administered benefits from SSA Privacy Act Systems of Records (SOR).

B. Legal Authority

SSA's authority to disclose data and the State Agency's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 453, 1106(b), and 1137 of the Act (42 U.S.C. §§ 653, 1306(b), and 1320b-7) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (Federal tax information);
- Sections 202(x)(3)(B)(iv) and 1611(e)(1)(I)(iii) of the Act (42 U.S.C. §§ 402(x)(3)(B)(iv) and 1382(e)(1)(I)(iii)) (prisoner data);

- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Section 1902(ee) of the Act (42 U.S.C. § 1396a(ee)); Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3551, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State Agency must follow with regard to use, treatment, and safeguarding of data.

II. Scope

A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.

B. The State Agency will execute an Information Exchange Agreement (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.

C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs, which are specifically identified in the IEA:

1. Temporary Assistance to Needy Families (TANF) program under Part A of Title IV of the Act;
2. Medicaid provided under an approved State plan or an approved waiver under Title XIX of the Act;
3. State Children's Health Insurance Program (CHIP) under Title XXI of the Act;
4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);

5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
10. Programs under a plan approved under Titles I, X, XIV, or XVI of the Act;
11. Foster Care and Adoption Assistance under Title IV of the Act;
12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
13. Other applicable federally funded programs administered by the State Agency under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.

D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

This Agreement and related data exchanges with the State Agency are necessary for SSA to assist the State Agency in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

B. Expected Results

The State Agency will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State Agency's program criteria. A cost-benefit analysis for the exchange made under this Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

IV. Record Description

A. Systems of Records (SOR)

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications;
- 60-0059 -- Earnings Recording and Self-Employment Income System;
- 60-0090 -- Master Beneficiary Record;
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB);
- 60-0269 -- Prisoner Update Processing System (PUPS); and
- 60-0321 -- Medicare Part D and Part D Subsidy File.

The State Agency will only use the Federal tax information (FTI) contained in **SOR 60-0059** (Earnings Recording and Self-Employment Income System) in accordance with 26 U.S.C. § 6103.

B. Data Elements

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information. Specific listings of data elements are available at:

http://www.ssa.gov/dataexchange/

C. Number of Records Involved

The maximum number of records involved in this matching activity is the number of records maintained in SSA's SORs listed above in Section IV.A.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

The State Agency will notify all individuals who apply for federally funded, state-administered benefits that any data they provide are subject to verification through computer matching with SSA. The State Agency and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

The State Agency will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing

computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

C. Opportunity to Contest

The State Agency will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;

2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and

3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the planned action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

Pursuant to 5 U.S.C. § 552a(p)(1)(A)(ii), SSA's DIB has determined that the State Agency may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when the benefit record is created.

The SSA Enumeration System used for SSN matching is 100 percent accurate based on SSA's Office of Quality Review (FY 2015 Enumeration Accuracy Report, April, 2016).

SSA does not have an accuracy assessment specific to SOR 60-0059 (Earnings Recording and Self-Employment Income System). The correctness of the FTI provided to SSA, as an agent for the Internal Revenue Service (IRS), is generally contingent upon the correctness of the information provided by the payer of the income.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, the State Agency must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. The State Agency must independently verify citizenship data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

VII. Disposition and Records Retention of Matched Items

A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.

B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.

C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.

D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.

E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

SSA and the State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related NIST guidelines, and the current revision of IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, available at http://www.irs.gov. In addition, SSA and the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical

security requirements governing all data SSA provides electronically to the State Agency, including SSA's *Electronic Information Exchange Security Requirements and Procedures for State and local Agencies Exchanging Electronic Information with SSA*, as well as specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

SSA has the right to monitor the State Agency's compliance with FISMA, the terms of this Agreement, and the IEA and to make onsite inspections of the State Agency for purposes of auditing compliance, if necessary, during the lifetime of this Agreement or of any extension of this Agreement. This right includes onsite inspection of any entity that receives SSA information from the State Agency under the terms of this Agreement, if SSA determines it is necessary.

IX. Controlled Unclassified Information (CUI) Requirements

Pursuant to 32 C.F.R. § 2002.16(a)(6), the State Agency must handle any CUI in accordance with Executive Order 13556, 32 C.F.R. Part 2002, and the CUI Registry. The State Agency acknowledges that misuse of CUI is subject to penalties established in applicable law, regulations, or Government-wide policies. The State Agency will report any non-compliance with handling requirements to SSA using methods approved by SSA.

X. Records Usage, Duplication, and Redisclosure Restrictions

A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.

B. The State Agency will comply with the following limitations on use, duplication, and redisclosure of SSA data:

1. The State Agency will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in the IEA.

2. The State Agency will not extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement. In limited circumstances that are approved by SSA, the State Agency may extract information about an individual other than the applicant/recipient when the applicant/recipient has provided identifying information about the individual and the individual's income or resources affect the applicant's/recipient's eligibility for such program.

3. The State Agency will not disclose to an applicant/recipient information about another individual (i.e., an applicant's household member) without the written consent from the individual to whom the information pertains.

4. The State Agency will use the FTI disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement programs in accordance with 26 U.S.C. § 6103(l)(7) and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision IRS Publication 1075.

5. The State Agency will use the citizenship status data disclosed by SSA only to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to CHIPRA, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA. The State Agency will further comply with additional terms and conditions regarding use of citizenship data, as set forth in the State Agency's IEA.

6. The State Agency will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.

7. The State Agency will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. The State Agency will provide its contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, the State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

8. If the State Agency is authorized or required – pursuant to an applicable law, regulation, or intra-governmental documentation – to provide SSA data to another State or local government entity for the administration of the federally funded, state-administered programs covered by this Agreement, the State Agency must ensure that the State or local government entity, including its employees, abides by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement and the IEA. At SSA's request, the State Agency will provide copies of any applicable law, regulation, or intra-governmental documentation that authorizes the intra-governmental relationship with the State or local government entity.

Upon request from SSA, the State Agency will also establish how it ensures that State or local government entity complies with the terms of this Agreement and the IEA.

9. The State Agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

10. The State Agency will conduct triennial compliance reviews of its contractor(s) and agent(s) no later than three years after the initial approval of the security certification to SSA. The State Agency will share documentation of its recurring compliance reviews with its contractor(s) and agent(s) with SSA. The State Agency will provide documentation to SSA during its scheduled compliance and certification reviews or upon request.

C. The State Agency will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. The State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use. To the extent SSA approves the requested redisclosure, the State Agency will ensure that any entity receiving the redisclosed data will comply with the procedures and limitations on use, duplication, and redisclosure of SSA data, as well as all administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency including specific guidance on safeguarding and reporting responsibilities for PII, as set forth in this Agreement and the accompanying IEAs.

XI. Comptroller General Access

The Government Accountability Office (Comptroller General) may have access to all records of the State and its State Agencies that the Comptroller General deems necessary to monitor or verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(l)(K).

XII. Duration, Modification, and Termination of the Agreement

A. Duration

1. This Agreement is effective from January 1, 2020 (Effective Date) through June 31, 2021 (Expiration Date).

2. In accordance with the CMPPA, SSA will: report the proposal to re-establish this matching program to the Congressional committees of jurisdiction and OMB in accordance with 5 U.S.C. § 552a(o)(2)(A) and OMB Circular A-108 (December 23, 2016), and publish notice of the matching program in the Federal Register in accordance with 5 U.S.C. § 552a(e)(12).

3. Within 3 months before the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:

   - the applicable data exchange will continue without any change; and
   - SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.

4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State Agency has violated or failed to comply with this Agreement.

XIII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State Agency the costs of furnishing the electronic data from the SSA SORs under this Agreement.

XIV. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to the State Agency under any IEAs governed by this Agreement. Furthermore, SSA is not liable for any damages or loss resulting from the destruction of any materials or data provided by the State Agency.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of SSA and the relative importance of this request to others. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

XV. Points of Contact

A. SSA Point of Contact

Regional Office
Susan Fay, Data Exchange Coordinator (DEC)
Center for Programs Support
JFK Federal Building, Room 1925
Boston, MA 02203
Phone: 617-565-2855/Fax: 617-565-9359
Email: Susan.Fay@ssa.gov and
BO.MA.RO.CPS.DATA.EXCHANGE@ssa.gov

B. State Agency Point of Contact

Mimi Brown, Assistant General Counsel
Executive Office of Health and Human Services
One Ashburton Place, 11th Floor
Boston, MA 02108
Phone: 617-573-1718/Fax: 617-573-1895
Email: Mimi.Brown@state.ma.us

XVI. SSA and Data Integrity Board Approval of Model CMPPA Agreement

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

SOCIAL SECURITY ADMINISTRATION

Monica Chyn
Acting Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

2-13-19
Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.

Mary Ann Zimmerman
Acting Chair
SSA Data Integrity Board

4/3/2019
Date

XVII. Authorized Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective agency to enter into the obligations set forth in this Agreement.

The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

SOCIAL SECURITY ADMINISTRATION

Linda M. Dorn

Linda M. Dorn
Regional Commissioner
Boston

11-19-2019

Date

MASSACHUSETTS EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

M L Sudders

Marylou Sudders
Secretary

11.07.19

Date

Authorized Data Exchange System(s)

BEER (Beneficiary Earnings Exchange Record): Employer data, including Federal tax return information, for the last calendar year.

BENDEX (Beneficiary and Earnings Data Exchange): Primary source for Title II eligibility, benefit, and demographic data.

LIS (Low-Income Subsidy): Data from the Low-Income Subsidy Application for Medicare Part D beneficiaries -- used for Medicare Savings Programs (MSP).

Medicare 1144 (Outreach): Lists of individuals on SSA roles, who may be eligible for medical assistance for: payment of the cost of Medicare cost-sharing under the Medicaid program pursuant to Sections 1902(a)(10)(E) and 1933 of the Social Security Act (Act); transitional assistance under Section 1860D-31(f) of the Act; or premiums and cost-sharing subsidies for low-income individuals under Section 1860D-14 of the Act.

PUPS (Prisoner Update Processing System): Confinement data received from over 2000 state and local institutions (such as jails, prisons, or other penal institutions or correctional facilities).

QUARTERS OF COVERAGE (QC): Quarters of Coverage data as assigned and described under Title II of the Act -- The term "quarters of coverage" is also referred to as "credits" or “Social Security credits” in various SSA public information documents. This application provides various QC data, including the maximum and minimum number of QCs credited for earned wages or self-employed income within a range of years.

SDX (SSI State Data Exchange): Primary source of Title XVI eligibility, benefit, and demographic data, as well as data for Title VIII Special Veterans Benefits (SVB).

SVES (State Verification and Exchange System): A batch system that provides SSN verification, Title II benefit information, and Title XVI information through a uniform data response based on authorized user-initiated queries. The SVES types are divided into five different responses as follows:

SVES I:	This batch provides strictly SSN verification.
SVES I/Citizenship*	This batch provides strictly SSN verification and citizenship data.
SVES II:	This batch provides strictly SSN verification and Title II benefit information
SVES III:	This batch provides strictly SSN verification and Title XVI benefit information.
SVES IV:	This batch provides SSN verification, Title II benefit information, and Title XVI benefit information, which represents all available SVES data.

SOLQ/SOLQ-I (State On-line Query/State On-line Query-Internet): A real-time online system that provides SSN verification and MBR and SSR benefit data similar to data provided via a SVES IV response.

SOLQ/Citizenship* or SOLQ-I/Citizenship* transmissions provide strictly SSN verification and citizenship data.

UIQ (Unemployment Insurance Query): A real-time online system that provides SSN verification to State Unemployment Agencies. Title II benefit information may also be disclosed to State Unemployment Agencies; however, the disclosure of Title II benefit data is generally restricted to only those State Agencies that administer unemployment insurance that are offset by the receipt of Title II benefits. UIQ transactions are transmitted to State Unemployment Agencies through the Department of Labor (DOL) Interstate Connection Network (ICON) Hub. The two UIQ response types are as follows:

UIQ I:	This transaction provides strictly SSN verification
UIQ II:	This transaction provides strictly SSN verification and Title II benefit information.

SSA Data Set: A data set consisting of the following data elements: SSN verification, monthly and annual Title II benefit information, Title II disability indicator, death indicator, quarters of coverage, prisoner data, and citizenship* data. The *SSA Data Set* is transmitted to approved State Agencies through the Centers for Medicare & Medicaid Services' (CMS) Federal Data Services Hub (Hub). Subject to technical, fiscal, and administrative limitations that may need to be resolved, SSA may approve a State Agency's request to receive the *SSA Data Set* when:

1. the State Agency uses the *SSA Data Set* for eligibility determinations in conjunction with Insurance Affordability Programs eligibility determinations;
2. the State Agency operates an integrated eligibility verification system (IEVS) and the IEVS initiates the call through CMS' Hub;
3. the State Agency uses a streamlined multi-benefit application; and
4. the State Agency submits an attestation capturing the authorization from CMS to utilize CMS' Hub.

** Confirmation of consistency of citizenship status data, as recorded in SSA's records, is disclosed by SSA to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA to receive the SSA Data Set through CMS' Hub.*

Attachment 3

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

12/9/2016

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

A. General Systems Security Standards

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

B. System Security Requirements for SWA's

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

1. General System Security Design and Operating Environment

The SWA must provide a written description of its' system configuration and security features. This should include the following:

a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and

c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

Meeting this Requirement

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

2. Automated Audit Trail

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored

in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL will approve the SWA's request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

Meeting this Requirement

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA's requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system's audit trail and retrieval capability. The SWA must be able to identify employee's who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system's audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

3. System Access Control

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The SWA must have

management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

Meeting this Requirement

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

4. **Monitoring and Anomaly Detection**

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

  This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

  This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

  This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

  This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA

information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)

- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

5. **Management Oversight and Quality Assurance**

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to

determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

6. **Security Awareness and Employee Sanctions**

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and

understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

7. Data and Communications Security

The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

D. Onsite Systems Security Certification Review

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of

reviewing and updating the SWA compliance with the systems security requirements described above.

Social Security Administration (SSA)

Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration

Technical System Security Requirements (TSSR)

Security Categorization: Moderate

Version 10.4

November 22, 2021

Prepared by

Office of Information Security

Document Revision History

Date	Description	Version	Author
12/05/2019	Converted TSSR requirements to NIST SP 800-53 rev 4 controls	10.0	OIS
02/12/2020	Added Controlled Unclassified Information (CUI) language in section 1.3	10.1	OIS
01/08/2021	Added: CA-3, CA-8, SA-11 Removed: AU-3(1), PE-5, PS-5, SC-17, SI-12 Updated: DM-2 to include SSA retention specific language, MP-2 to accurately reflect NIST language	10.2	OIS
2/19/2021	Added: VAN and Data Transmission Requirements Updated assessment language throughout document Updated assessment timeframe Updated SEQ submission requirements	10.3	OIS
11/22/2021	Added Third Party Assessment guidance (section 1.6.4) Added SRTM reference with SEQ (section 1.6)	10.4	OIS

Table of Contents

1 INTRODUCTION 5
1.1 Applicable Laws and Regulations 6
1.2 Applicable Standards and Guidance 6
1.3 Controlled Unclassified Information (CUI) 7
1.4 Electronic Information Exchange (EIE) Definition 7
1.5 Roles and Responsibilities 7
1.5.1 SSA Office of Information Security (OIS) 7
1.5.2 SSA Regional Data Exchange Coordinator (DEC) 8
1.5.3 Electronic Information Exchange Partner (EIEP) 8
1.5.4 State Transmission/Transfer Component (STC) 8
1.6 SSA Security Assessments 8
1.6.1 Documenting Security Controls in the SEQ 9
1.6.2 EIEP Security Assessment Participation 10
1.6.3 Scheduling of Onsite Assessment 10
2 SYSTEMS SECURITY STANDARDS AND REQUIREMENTS 11
2.1 Access Control 15
2.2 Accountability, Audit, and Risk Management 20
2.3 Audit and Accountability 21
2.4 Awareness and Training 24
2.5 Contingency Planning 25
2.6 Data Minimization and Retention 26
2.7 Identification and Authentication 27
2.8 Incident Response 29
2.9 Media Protection 31
2.10 Personnel Security 32
2.11 Physical and Environmental Protection 34
2.12 Planning 35
2.13 Risk Assessment 37
2.14 Security Assessment and Authorization 38
2.15 System and Communications Protection 41
2.16 System and Information Integrity 42
2.17 System and Services Acquisition 45
APPENDIX A. ACRONYMS 47
APPENDIX B. ADDITIONAL DEFINITIONS 49

List of Tables

Table 1: Acronyms and Terms 47
Table 2: Additional Definitions 49

1 Introduction

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its Electronic Information Exchange Partners (EIEPs). EIEPs must protect the information with efficient and effective security controls.

This document consistently references the concept of EIEPs; however, the SSA Security Evaluation Questionnaire (SEQ) document will use the terms "State Agency" or "State Agency, contractor(s), and agent(s)" or "organization" for clarity. Most state officials and agreement signatories are not familiar with the acronym EIEP; therefore, SSA will continue to use the terms "State Agency", "Tribal Entity", "Territory", similar but different synonyms, or "State Agency, contractor(s), and agent(s)" or "organization" in the same manner as the Computer Matching and Privacy Protection Act (CMPPA) and Information Exchange Agreements (IEA). This allows for easier alignment and mapping back to the information exchange agreements between state agencies and SSA. It will also provide a more "user-friendly" experience for the officials who complete these forms on behalf of their agencies.

The objective of this document is to ensure that SSA can properly determine EIEPs as compliant with SSA security standards, requirements, and procedures.

This document helps EIEPs understand the criteria that SSA uses when assessing and certifying the system design and security features used for electronic or physical access to SSA data. Finally, this document provides the framework and general procedures for SSA's Security Assessment Program.

The primary statutory authority that supports the information contained in this document is the Federal Information Security Management Act , as amended by the Federal Information Security Modernization Act (FISMA) of 2014 (Pub. L. 113-283). FISMA became law as part of the Electronic Government Act of 2002. FISMA is the United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manufactured threats. FISMA assigned the National Institute of Standards and Technology (NIST), a branch of the U.S. Department of Commerce, the responsibility to outline and define compliance with FISMA. Unless otherwise stated, all of SSA's requirements mirror the NIST- defined management, operational, and technical controls listed in the various NIST Special Publications (SP) libraries of technical guidance documents.

Following Federal Information Processing Standards (FIPS) documents: FIPS-199, FIPS-200, and NIST 800-60 volume II, SSA has determined that its data is considered Personally Identifiable Information (PII). NIST, in solidarity with OMB, defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information". As a result of this classification of data, SSA has determined that there is a consistently moderate level of risk associated with the storing, processing, and transmitting of its data. NIST 800-53 Revision 4 defines the minimum security controls to be applied to Low, Moderate, and High risk data and the information systems associated with the data. SSA has determined that a selection of these controls are applicable to any organization storing, processing, or transmitting SSA data outside of a federal facility.

To gain electronic access to SSA data, under the auspices of a data exchange agreement, EIEP's must comply with SSA's current Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration. This document is synonymous with the term Technical System Security Requirements (TSSR). The TSSR specifies minimally acceptable levels of security safeguards to protect SSA data. SSA maintains the TSSR as a living document (subject to change) that addresses emerging threats, new vulnerabilities, and the development of new technology that potentially places SSA data at risk. SSA will work with EIEPs to resolve deficiencies, which result from updates to the TSSRs. EIEPs may proactively ensure their ongoing compliance with the TSSRs by periodically requesting the most current TSSR package from their SSA Point of Contact (POC) from the data exchange agreement. Additions, deletions, or modification of security controls directly affect the level of security and due diligence SSA requires EIEPs use to mitigate risks. The emergence of new threats, attack methods, and the development of new technology warrants frequent reviews and

revisions to our TSSR. Consequently, EIEPs should expect SSA's TSSR to evolve in harmony with the industry standards.

1.1 Applicable Laws and Regulations

- Computer Fraud and Abuse Act [Public Law (PL) 99-474, 18 U.S. Code (USC) 1030]
- E-Authentication Guidance for Federal Agencies [Office of Management and Budget (OMB) M-04-04]
- Federal Information Security Modernization Act (FISMA) of 2014 [PL 113-283]
- Freedom of Information Act (FOIA) As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Preparing for and Responding to a Breach of Personally Identifiable Information [OMB M-17-12]
- Privacy Act and Trade Secrets Act [18 USC 1905]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Unauthorized Access Act [18 USC 2701 and 2710]

1.2 Applicable Standards and Guidance

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Assessing Security and Privacy Controls in Federal Information Systems and Organizations [NIST SP 800-53A, Revision 4]
- Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems [NIST SP 800-37 Revision 2]
- Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60 volumes 1 & 2, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Managing Information Security Risk [NIST SP 800-39]

- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30]
- Security and Privacy Controls for Federal Information Systems and Organizations [NIST SP 800-53, Revision 4]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Social Security Administration, Office of Information Security, Information Security Policy (ISP)
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

1.3 Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Pursuant to 32 C.F.R. § 2002.16(a) (6), the State Agency must handle any CUI in accordance with Executive Order 13556, 32 C.F.R. Part 2002, and the CUI Registry. The State Agency acknowledges that misuse of CUI is subject to penalties established in applicable law, regulations, or Government-wide policies. The State Agency will report any non-compliance with handling requirements to SSA using methods approved by SSA.

1.4 Electronic Information Exchange (EIE) Definition

EIE is any electronic process in which SSA discloses information under its control to any third party for program or non-program purposes, without the specific consent of the subject individual or any agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the programmatic systems of parties to electronic information sharing agreements with SSA. This includes access to SSA systems, batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

1.5 Roles and Responsibilities

1.5.1 SSA Office of Information Security (OIS)

OIS has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's program integrity monitoring and reporting activities, developing and disseminating security training and awareness materials, and providing consultation and support for a variety of agency initiatives. OIS conducts SSA's security assessments to ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic data exchange agreements executed by SSA with external partners. Within the context of SSA's security policies and the terms of the electronic data exchange agreements with SSA's EIEPs, SSA exclusively conducts and brings to closure security assessments. This includes (but not limited to) any EIEP that processes, maintains, transmits, stores, or destroys SSA data in accordance with pertinent Federal requirements.

1.5.2 SSA Regional Data Exchange Coordinator (DEC)

Regional DECs serve as a bridge between SSA and EIEPs. DECs assist in coordinating data exchange security assessment activities with EIEPs; (e.g., providing points of contact with state agencies, drafting and updating information exchange agreements, etc.) DECs are also the first points of contact for states if an employee of a State Agency or an employee of a State Agency's contractor or agent becomes aware of suspected or actual loss of SSA data.

1.5.3 Electronic Information Exchange Partner (EIEP)

Electronic Information Exchange Partner is an organization that has an IEA with SSA and receives SSA data. SSA requires EIEPs to adhere to the standards, requirements, and procedures, published in this TSSR document. Both SSA and EIEPs must exercise due diligence in the responsibility for establishing appropriate management, operational, and technical safeguards to ensure the confidentiality, integrity, and availability of its records and to protect against any anticipated threats or hazards to their security.

1.5.4 State Transmission/Transfer Component (STC)

A STC is an organization that performs as a transmission and/or collection point for one or more other entities. An STC must also adhere to the same management, operational, and technical controls as the EIEP.

1.6 SSA Security Assessments

Security assessments involve the examination, interview, and testing of information system personnel, network, software, and hardware. All organizational units and personnel responsible for the answers given in the Security Evaluation Questionnaire (SEQ) and Security Requirements Traceability Matrix (SRTM), will be expected to attend the security assessment in its entirety. A significant part of the review process, and the validation of many safeguards, involves the demonstration, by the organization, of their information system(s). It is expected that organizations are capable and prepared to support a full demonstration of the system(s) as well as an ad hoc analysis from SSA assessment personnel.

The security assessment is performed every 3-5 years after an initial assessment and authorization has been completed. Deviations from the triennial review cycle are managed on a case by case basis.

The security assessment process applies to organizations that seek electronic and physical access to SSA data and consists of five phases:

Phase 1. Pre-Assessment:

a. In the pre-assessment phase, SSA assessment personnel will:
    i. Contact Data Exchange Coordinators for an updated list of points of contact,
    ii. Verify points of contact with the subject organization(s),
    iii. Send engagement letters and copies of the most recently updated TSSR and SEQ
    iv. Work with organizations to answer questions regarding the assessment process.
b. Organizations that have established a new agreement with SSA will not receive engagement letters, instead they will be contacted by the SSA OIS External Compliance Branch to onboard them into the security assessment program. This will effectively begin the pre-assessment phase.

Phase 2. SEQ and SRTM Review:

a. All organizations must complete the SEQ. The SEQ is an assessment document that allows organizations to clearly articulate how they have implemented SSA security controls and met the security objectives.
b. The assigned SSA security assessor must receive the completed SEQ no less than 60 days prior to a security assessment.

c. Organizations entering into an initial interconnection, or implementing a significant change, will need to notify SSA 8-12 months prior to the production deployment date and will need to provide the completed SEQ no less than 120 days prior to the assessment.

Phase 3. Assessment:

a. The SSA security assessment is conducted by SSA, or on its behalf, to examine the full suite of management, operational, and technical security controls implemented by the organization to safeguard data obtained from SSA.
b. As stated above, a significant part of the review process, and the validation of many safeguards, involves the demonstration, by the organization, of their information system(s). It is expected that organizations are capable and prepared to support a full demonstration of the system(s) and applicable supporting components as well as an ad hoc analysis from SSA assessment personnel.

Phase 4. Post-Assessment:

a. Notify organization of findings
b. Remediation period
    i. SSA will allow for a fixed period of time for some findings, depending on severity, to be remediated. This time cannot be extended and any finding still open after the remediation period will be elevated to a Plan of Action and Milestone (POA&M).
c. Final Report
    i. The final report will detail the findings that will need to be remediated by the EIEP, and findings closed during the remediation period.
d. POA&M Creation
    i. Any findings that remain open after the remediation period will result in the need for the organization to create a POA&M to address the finding.

Phase 5. POA&M Monitoring:

a. POA&Ms are monitored quarterly.
    i. Severity of the finding and age of the POA&Ms will constitute additional activities from SSA.
b. The organization is required to track POA&Ms and report the progress quarterly or as milestones are achieved.

NOTE: SSA will never request documentation for security assessments unless necessary to assess the EIEP's security posture. The information is only accessible to authorized individuals who have a need for the information as it relates to the EIEP's compliance with its information exchange agreement.

1.6.1 Documenting Security Controls in the SEQ

EIEPs must submit an SEQ when one or more of the following circumstances apply:

- To obtain approval for requested access to SSA data for an initial connection,
- To obtain approval to reestablish previously suspended or terminated access to SSA data,
- To obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, or security implementations planned or made since approval of their most recent security assessment,
- To document descriptions and explanations of measures implemented as the result of a data breach or security incident and to confirm compliance when one or more security breaches or incidents involving SSA data occurred since their most recent successfully completed security assessment,

SSA may require a new SEQ if changes occurred (other than those listed above) that may affect the terms of the EIEP's information exchange agreement with SSA.

SSA will not approve the initiation of transactions and/or access to SSA data before the EIEP fully complies with the TSSR.

NOTE: Organizations that function only as an STC, transferring SSA data to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's TSSR and exercise their responsibilities regarding protection of SSA data.

1.6.2 EIEP Security Assessment Participation

SSA requires that any individual responsible for, or consulted in, completing the SEQ attend the security assessment~~s~~ for their respective organization in its entirety.

SSA may request to meet with the following stakeholders during the security assessment:

- Sample of managers, supervisors, information security officers, system administrators, etc. responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA data, and for reviewing reports and taking necessary action,
- Individuals responsible for performing security awareness and employee sanction functions to learn how EIEPs fulfill this requirement,
- Sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA data
- Individual(s) responsible for management oversight and quality assurance functions to confirm how the EIEP accomplishes this requirement, and/or
- Any additional individuals as deemed appropriate by SSA (i.e. Analysts, Project/Program Manager, Claims Representatives, etc.)

1.6.3 Scheduling of Onsite Assessment

SSA will schedule the assessment based on the SSA requirements. For newly established agreements, SSA will not schedule the onsite assessment until SSA has administratively approved the EIEP's SEQ.

SSA is required to conduct an onsite security assessment no later than 60 days prior to production date for any significant changes or initial access involving SSA data.

The scheduling of the onsite review may depend on additional factors including:

- SSA's workload and resource considerations,
- The reason for submission of the SEQ,
- The severity of security issues, if any,
- Circumstances of the previous review.

1.6.4 Third Party Assessments

Based on guidance in NIST SP 800-37, SSA's Authorizing Official may leverage the official assessment results produced by a third party provided to the information system's authorizing official to authorize the use of an information system, service, or application to meet SSA assessment objectives. SSA requires the third-party assessment to be at a minimum equivalent to the scope, depth, and breadth of an SSA assessment, and organizations must and make available sufficient evidence regarding the security state of an information system so that SSA's authorizing official can use that evidence to make credible, risk-based decisions regarding

the operation and use of that system or the information it processes, stores, or transmits. SSA will leverage an active federally authorized information system (IRS, CMS, CJIS, etc.…), industry recognized independent assessments (SOC 1, SOC 2), and independent third- party assessments using the individually agency's requirements.

What are the requirements?

- A completed ATO by the organization for the cloud system, service, or application (FedRAMP Authorization or Agency Authorization to Operate).
- OIS review of the authorization package and documentation (SSP, SAP, SAR, POAMs, additional documentation as necessary)
- Assessment of SSA tailored controls will be required. Security controls assessments may be required for other controls in scope
- Leveraged ATO from the other organization must remain in good standing and following the continuous monitoring requirements
- Immediate notification by CIO, CISO, or System Owner if the leveraged ATO is revoked

Since the required assessment and authorization documentation is owned by the organization, it is the sole responsibility of the organization to provide the required documentation to SSA for review. SSA's goal is to provide an efficient security assessment process with organizational partners that aligns with other Federal standards and alleviates redundancy for our partners.

2 Systems Security Standards and Requirements

SSA's TSSR represents the current industry standard for security controls, safeguards, and countermeasures required for federal information systems by federal regulations, statutes, standards, and guidelines. Additionally, SSA's TSSR includes organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

SSA must assess and certify that the EIEP has implemented security controls that meet the requirements and work as intended, before the authorization to initiate transactions to and from SSA.

The TSSR addresses management, operational, and technical aspects of safeguards to ensure only authorized disclosure and usage of SSA data stored, processed, or transmitted by SSA's EIEPs.

SSA requires EIEPs to document and seek formal approval from SSA's Office of Privacy and Disclosure (OPD) if they plan to share SSA data with another organization or to allow them direct access to their system. This includes, but is not limited to, law enforcement, other state agencies, tribal entities, and state or federal organizations that perform audit, quality, or integrity functions.

EIEPs that store, process, or transmit SSA data must comply with the following systems security controls.

The following subsections define the security requirements for 17 control families derived from NIST 800-53 Revision 4. This subset of security controls will help SSA establish a sense of risk associated with the storing, processing, and transmitting of SSA data by the subject organization. SSA does not make any recommendations as to how security controls are implemented.

1. Intent: EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA data neither prevents nor impedes the EIEP's ability to:

- Safeguard the information to comply with SSA and NIST requirements.
- Effectively and efficiently investigate fraud, data breaches, or security events that involve SSA data.
- Detect instances of misuse or abuse of SSA data.

For example, utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or associated systems security requirements and procedures.

NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA to administer programs governed by the presiding CMPPA and/or service level agreement, i.e. IEA.

2. Oversight: The EIEP must process SSA data under the immediate supervision and control of authorized personnel. Any changes to the processing of SSA data must be approved through a documented change management process, any significant changes must be approved by SSA prior to implementation.

3. Schedule: A preliminary schedule for all activities involved in planning, establishing, and maintaining the interconnection will be developed and coordinated through the Office of Data Exchange (ODX). In addition, both parties agree to the schedule and conditions for terminating or reauthorizing the interconnection.

4. Data Transmission:

a. The EIEP must use the electronic connection established between the EIEP and SSA and any software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA.

b. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.

c. EIEPs must ensure that SSA data is not accessed, processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.

d. SSA data must traverse an appliance with State administrative authority prior to being sent to a third-party provider (cloud service provider or managed service provider).

e. SSA requires that EIEPs maintain a verification account number (VAN) for SSA data exchanges.

5. Data Protection:

a. Access: EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA data are held to the same security requirements as employees of the EIEP.

b. Storage: EIEPs must store information received from SSA in a manner that, at all times, is physically and electronically secure using FIPS 140-2 approved methods from access by unauthorized persons.

c. Safeguards: EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA data via computer, remote terminal, or other means.

d. Confidentiality: EIEPs must advise employees with access to SSA data of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.

6. Live Data Testing: The use of live SSA data in test environments should generally be avoided and is not authorized unless specifically approved by the Office of Information Security through the submission of a formal request. At least 60 day in advance, agencies must formally request SSA approval to use live SSA data in a testing environment.

SSA defines live data as primarily unmodified, non-sanitized data extracted from SSA files that identifies a specific individual SSA provided information. The use of live data in testing environments is limited to the terms of the Information Exchange Agreement or other authorized SSA purposes and may be disclosed only to those individuals with a need-to-know.

Any systems within pre-production testing environments ideally will be configured according to requirements in this publication. However, the Office of Information Security understands most agencies may not be able to fully implement all TSSR requirements in a test environment.

Agencies wishing to use live SSA data in pre-production must submit a formal request to SSA's Office of Information Security for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing.

Need and Use Justification statements should be revised to cover this use of SSA data, if not already addressed. State agencies should check their Information Exchange Agreements to verify if "testing purposes" is covered.

Testing efforts that use live SSA data primarily fall into two categories: one-time testing and ongoing testing.

An example of a one-time testing use of live SSA data would be for system testing that is done prior to a new system implementation and, once testing has validated that the data will work properly, the live SSA data is not required to continue to remain in the test environment. For one-time testing efforts, the Office of Safeguards requires the SSA data to be deleted from systems and databases upon completion of testing efforts, and that the hard drive of the test systems be sanitized electronically prior to repurposing the system for other state agency testing efforts.

Duration for ongoing test activities will be agreed upon as part of the live data request process. Some examples of ongoing testing efforts include:

a. Testing of extract, transform, and load (ETL) process to validate federal data loading into a database.

b. Application testing of eligibility modeling that requires data match between the entire population of state and federal information, where building a set of dummy data is not feasible.

7. Incident Response: EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA data affected by the incident.

8. Security Awareness: EIEPs must have an active and robust security awareness program.

9. Contingency Planning:

a. In accordance with the NIST Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency Plan (CP) that includes a Disaster Recovery Plan (DRP) that addresses both natural disaster and cyber-attack situations.

b. SSA additionally requires the Contingency Plan to include details regarding the organizational Business Continuity Plan (BCP) and a Business Impact Analyses (BIA) that address the security of SSA data if a disaster occurs.

c. Organizations should coordinate contingency planning training, testing, and exercises to minimize the impact of disasters and other contingencies that could damage the connected systems or jeopardize the confidentiality and integrity of shared data. Considerations include emergency alerts and notification; damage assessment; response and recovery, and data retrieval. The organizations are to notify each other about changes to emergency POC information (primary and alternate), including changes in staffing, addresses, telephone and fax numbers, and e-mail addresses.

10. Interconnection Security Agreement (ISA): The ISA describes the process of data communication and the impact of the data interchange. An interconnection is defined, as the direct connection between two or more Information Technology Systems for the purpose of sharing/exchanging the information. The interconnection must be in compliance with NIST Special publication 800-47 titled "Interconnecting Information Technology Systems", and to satisfy CA-3 control of the NIST Special publication 800-53 titled "Security & Privacy Controls for Federal Information Systems and Organizations". Current agreements between SSA and EIEPs satisfy the requirements of 800-47.

11. Planned Disconnect: Any planned disconnect should be coordinated with the SSA internal business liaison who will notify the appropriate SSA components and the EIEP point of contact concerning the planned disconnection at least 90 business days before the disconnection takes place. Before terminating the interconnection, the initiating party should notify the other party in writing, and it should receive an acknowledgment in return. The notification should describe the reason(s) for the disconnection, provide the proposed timeline for the disconnection, and identify technical and management staff who will conduct the disconnection.

12. Emergency Disconnect: If one or both organizations detect an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it might be necessary to abruptly terminate the interconnection without providing written notice to the other party. This extraordinary measure should be taken only in extreme circumstances and only after consultation with appropriate technical staff and senior management.

The system owner or designee should immediately notify the other party's emergency contact by telephone or other verbal method, and receive confirmation of the notification. Both parties should work together to isolate and investigate the incident, including conducting a damage assessment and reviewing audit logs and security controls, in accordance with incident response procedures. If the incident was an attack or an intrusion attempt, law enforcement authorities should be notified, and all attempts should be made to preserve evidence.

The initiating party should provide a written notification to the other party in a timely manner (e.g., within five days). The notification should describe the nature of the incident, explain why the interconnection was terminated, describe how the interconnection was terminated, and identify actions taken to isolate and investigate the incident. In addition, the notification may specify when and under what conditions the interconnection may be restored, if appropriate.

13. Change Management: In the event that EIEP or SSA make changes which trigger the need for re-authorization it would require the ISA to be updated and reauthorized by both parties. Please refer to "Documenting Security Controls in the SEQ" for further details.

14. System Configuration: If a party intends to make technical changes to the system architecture that party will report those changes to the other party's designated technical staff counterparts before the changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign a new Interconnection Security Agreement within one (1) month of implementation.

15. Topological Drawing: The EIEP should include a topological drawing illustrating the interconnectivity from SSA to the EIEP. The drawing should include all communications paths, circuits, and other components used for the interconnection, from "Organization A's" system to "Organization B's" system. The drawing should depict the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations) and the physical location of the connection point.

16. Security Assessment: At its discretion, SSA or a third party (i.e. contractor) must have the option to conduct onsite security assessments or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

2.1 Access Control

Control Number	AC-1
Title	Access Control Policy and Procedures
SSA Requirement	The organization must: a. Develop, document, and disseminate to designated organization officials: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the access control policy and associated access control controls; b. Review and update the current access control procedures with the organization-defined frequency.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AC-2
Title	Account Management
SSA Requirement	The organization must: a. Identify and select the accounts with access to SSA data to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts; h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes. i. Authorizes access to the information systems that receive, process, store or transmit SSA data based on valid access authorization, need-to-know permission or under the authority to re-disclose SSA data. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance (from NIST 800-53)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.
Control Number	AC-3
Title	Access Enforcement
SSA Requirement	The organization must: Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
Supplemental Guidance	Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-
Control Number	AC-3(7)
Title	Access Enforcement | Role-Based Access Control
SSA Requirement	The organization information system must: enforce a role-based access control policy over defined subjects and objects and controls access based upon the need to utilize SSA data.
Supplemental Guidance (from NIST 800-53)	Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of

	access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.
Control Number	AC-3(8)
Title	Access Enforcement | Revocation Of Access Authorization
SSA Requirement	The organization must: Enforce a role-based access control over users and information resources that have access to SSA data, and control access based upon organization defined roles and users authorized to assume such roles.
Supplemental Guidance (from NIST 800-53)	Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.
Control Number	AC-4
Title	Information Flow Enforcement
SSA Requirement	The organization information system must: enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the need for interconnected systems to share SSA data to conduct business.
Supplemental Guidance (from NIST 800-53)	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.
Control Number	AC-5
Title	Separation of Duties

SSA Requirement	The organization must: a. Separate organization-defined duties of individuals; b. Document separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. *SSA also requires that the state organization prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.* *Federal requirements and SSA policy exclude any employee who uses SSA data to process programmatic workloads to make benefit or entitlement determinations from participation in management or quality assurance functions.*
Supplemental Guidance (from NIST 800-53)	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.
Control Number	AC-6
Title	Least Privilege
SSA Requirement	The organization must: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Supplemental Guidance (from NIST 800-53)	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.
Control Number	AC-6(1)
Title	Least Privilege | Authorize Access to Security Functions
SSA Requirement	The organization must explicitly authorize access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.
Supplemental Guidance (from NIST 800-53)	Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system
Control Number	AC-6(7)
Title	Least Privilege | Review Of User Privileges
SSA Requirement	The organization must: a. Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and b. Reassign or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance (from NIST 800-53)	The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.
Control Number	AC-7
Title	Unsuccessful Logon Attempts
SSA Requirement	The organization must: a. Enforce a limit of no fewer than three (3) and no greater than five (5) consecutive invalid logon attempts by a user during an organization-defined time period; and b. Automatically lock the account/node for: an organization-defined time period; or locks the account/node until released by an administrator; or delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
Supplemental Guidance (from NIST 800-53)	This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.
Control Number	AC-8
Title	System Use Notification
SSA Requirement	The organization must: a. Displays to users system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information organization-defined conditions, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.
Supplemental Guidance (from NIST 800-53)	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.
Control Number	AC-11
Title	Session Lock

SSA Requirement	The organization's information system: a. Prevents further access to the system by initiating a session lock after organization-defined time period of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.
Supplemental Guidance (from NIST 800-53)	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.
Control Number	AC-17
Title	Remote Access
SSA Requirement	The organization must: a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize remote access to the information system prior to allowing such connections.
Supplemental Guidance (from NIST 800-53)	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

2.2 Accountability, Audit, and Risk Management

Control Number	AR-3
Title	Privacy Requirements for Contractors and Service Providers
SSA Requirement	The organization must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.
Supplemental Guidance (from NIST 800-53)	Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

2.3 Audit and Accountability

Control Number	AU-1
Title	Audit and Accountability Policy and Procedures
SSA Requirement	The organization must: a. Develop, document, and disseminate to individuals and organizations that store, process, or transmit SSA data: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. If an STC is utilized, specifically address the purpose, scope, roles, responsibilities, management commitment, coordination among STC and organizational entities, and 3. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Review and update the current: 1. Audit and accountability policy at least triennially; and 2. Audit and accountability procedures at least triennially.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AU-2
Title	Audit Events
SSA Requirement	The organization must: a. Audit the following events: 1) Viewing SSA data stored within the organization's system; 2) Viewing of screens that contain SSA data; 3) All system and data interactions concerning SSA data. b. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Determines that the following events are to be audited within the information system: 1) Viewing SSA data stored within the organization's system; 2) Viewing of screens that contain SSA Data; 3) All system and data interactions concerning SSA Data.
Supplemental Guidance (from NIST 800-53)	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may

	determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.
Control Number	AU-3
Title	Content of Audit Records
SSA Requirement	The organization information system must generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
Supplemental Guidance (from NIST 800-53)	Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.
Control Number	AU-6
Title	Audit Review, Analysis, and Reporting
SSA Requirement	The organization must: a. Review and analyze information system audit records periodically for indications of inappropriate or unusual activity involving SSA data]; and b. Report findings according to the organization incident response policy.
Supplemental Guidance (from NIST 800-53)	Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.
Control Number	AU-6(1)
Title	Audit Review, Analysis, and Reporting | Process Integration
SSA Requirement	The organization must employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
Supplemental Guidance (from NIST 800-53)	Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.
Control Number	AU-7

Title	Audit Reduction and Report Generation
SSA Requirement	The organization information system must provide an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.
Supplemental Guidance (from NIST 800-53)	Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.
Control Number	AU-9
Title	Protection of Audit Information
SSA Requirement	The organization information system must protect audit information and audit tools from unauthorized access, modification, and deletion.
Supplemental Guidance (from NIST 800-53)	Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.
Control Number	AU-11
Title	Audit Record Retention
SSA Requirement	The organization must retain audit records for three (3) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Supplemental Guidance (from NIST 800-53)	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.
Control Number	AU-12
Title	Audit Generation
SSA Requirement	The organization information system must: a. Provide audit record generation capability for the auditable events defined in AU-2 a. at the audit reporting mechanism; b. Allow security personnel to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3
Supplemental Guidance (from NIST 800-53)	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

2.4 Awareness and Training

Control Number	AT-1
Title	Security Awareness and Training Policy and Procedures
SSA Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to SSA data: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy and; 2. Security awareness and training procedures. The training and awareness programs must include: The sensitivity of SSA data, The rules of behavior concerning use and security in systems and/or applications processing SSA data, The Privacy Act and other Federal and state laws governing collection, maintenance, use, and dissemination of information about individuals, The possible criminal and civil sanctions and penalties for misuse of SSA data, The responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA data, The restrictions on viewing and/or copying SSA data, The proper disposal of SSA data, The security breach and data loss incident reporting procedures, The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code, Social engineering (phishing, vishing and pharming) and network fraud prevention.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AT-2
Title	Security Awareness Training
SSA Requirement	The organization must provide basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter.

Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.
Control Number	AT-3
Title	Role-Based Security Training
SSA Requirement	The organization must provide role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.
Control Number	AT-4
Title	Security Training Records
SSA Requirement	The organization must: a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and b. Retain individual training records for at least five years. *SSA also requires the organization to certify that each employee, contractor, and agent who views SSA data certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure*.
Supplemental Guidance (from NIST 800-53)	Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

2.5 Contingency Planning

Control Number	CP-2

Title	Contingency Plan
SSA Requirement	The organization must: a. Develop a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by a senior manager; b. Distribute copies of the contingency plan to personnel and organizations supporting the contingency plan actions; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the information system at least annually; e. Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to personnel and organizations supporting the contingency plan actions;
Supplemental Guidance (from NIST 800-53)	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

2.6 Data Minimization and Retention

Control Number	DM-2
Title	Data Retention and Disposal
SSA Requirement	The organization must: a. Retain each collection of SSA Data no longer than required for the organization's business process or evidentiary purposes; b. Dispose of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

	c. Use organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records). SSA. Dispose of, destroy, and/or erase all data received from SSA to administer benefit programs after the required processing of such data for the applicable benefit programs.
Supplemental Guidance (from NIST 800-53)	NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

2.7 Identification and Authentication

Control Number	IA-2
Title	Identification and Authentication (Organizational Users)
SSA Requirement	The organization's information system must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
Supplemental Guidance (from NIST 800-53)	Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to

	provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.
Control Number	IA-5
Title	Authenticator Management
SSA Requirement	The organization must manage information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators within organization-defined time period; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
Supplemental Guidance (from NIST 800-53)	Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.
Control Number	IA-5(1)
Title	Authenticator Management | Password-Based Authentication
SSA Requirement	The information system, for password-based authentication, must: a. Enforces minimum password complexity of requirements for: * case sensitivity (upper and lower case letters), * number of characters (equal to or greater than eight characters), * mix of upper-case letters, lower-case letters, numbers, and special characters (at least one of each type);

	c. Stores and transmits only cryptographically-protected passwords; d. Enforces password minimum and maximum lifetime restrictions; e. Prohibits password reuse for organization-defined number of generations; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.
Supplemental Guidance (from NIST 800-53)	This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.

2.8 Incident Response

Control Number	IR-1
Title	Incident Response Policy and Procedures
SSA Requirement	The organization must: a. Develops, documents, and disseminates to organization-defined personnel or roles: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy with organization-defined frequency; and 2. Incident response procedures with organization-defined frequency. *The incident response procedures must include the following information:* *If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact* ***within one hour****, the responsible State Agency official or delegate must report the incident by contacting* ***SSA's National Network Service Center (NNSC) toll free at 1-877-697-4889*** *(select "Security and PII Reporting" from the options list). As the final option, in the event SSA contacts and NNSC both cannot be reached, the EIEP is to contact SSA's Office of Information Security,* ***Security Operations Center (SOC) toll free at 1-866-718-6425.*** *The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.* *If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ), determines that the risk presented by a breach or security incident requires that the state organization notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches. SSA and NIST Guidelines encourage*

	agencies to consider establishing incident response teams to address PII and SSA data breaches.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	IR-2
Title	Incident Response Training
SSA Requirement	The organization must provide incident response training to information system users consistent with assigned roles and responsibilities: a. Within organization-defined time period of assuming an incident response role or responsibility; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.
Control Number	IR-4
Title	Incident Handling
SSA Requirement	The organization must: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
Supplemental Guidance (from NIST 800-53)	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.
Control Number	IR-8
Title	Incident Response Plan
SSA Requirement	The organization must: a. Develop an incident response plan that:

	1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by organization-defined personnel or roles; b. Distribute copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements; c. Review the incident response plan organization-defined frequency; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicate incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protect the incident response plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

2.9 Media Protection

Control Number	MP-2
Title	Media Access
SSA Requirement	The organization must: Restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].
Supplemental Guidance (from NIST 800-53)	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.
Control Number	MP-6
Title	Media Sanitization
SSA Requirement	The organization must: a. Sanitize media containing SSA data prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance (from NIST 800-53)	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

2.10 Personnel Security

Control Number	PS-3
Title	Personnel Screening
SSA Requirement	The organization must: a. Screen individuals (employees, contractors and agents) prior to authorizing access to the information system and SSA data.
Supplemental Guidance (from NIST 800-53)	Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.
Control Number	PS-4
Title	Personnel Termination
SSA Requirement	The organization, upon termination of individual employment, must: a. Disable information system access; b. Terminate/revoke any authenticators/credentials associated with the individual; c. Conduct exit interviews, as needed; d. Retrieve all security-related organizational information system-related property; e. Retain access to organizational information and information systems formerly controlled by terminated individual; and f. Notified organization-defined personnel upon termination.
Supplemental Guidance (from NIST 800-53)	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

Control Number	PS-6
Title	Access Agreements
SSA Requirement	The organization must: a. Develop and document access agreements for organizational information systems; b. Reviews and updates the access agreements at organization-defined frequency; and c. Ensure that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at an organization-defined frequency. *SSA requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA data.*
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.
Control Number	PS-7
Title	Third-Party Personnel Security
SSA Requirement	The organization must: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within organization-defined time period; and e. Monitors provider compliance. *The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to SSA data.* *The state organization must retain the non-disclosure agreements for at least five (5) to seven (7) years for all contractors and agents who processes, views, or encounters SSA data as part of their duties*
Supplemental Guidance (from NIST 800-53)	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.
Control Number	PS-8

Title	Personnel Sanctions
SSA Requirement	The organization must: a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notify organization personnel within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. *If an employee, contractor, or agent is subject to an adverse administrative action by the organization (e.g., reduction in pay, disciplinary action, termination of employment), SSA recommends the organization remove his or her access to SSA data in advance of the adverse action to reduce the possibility that will the employee will perform unauthorized activities that involve SSA data.*
Supplemental Guidance (from NIST 800-53)	Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

2.11 Physical and Environmental Protection

Control Number	PE-3
Title	Physical Access Control
SSA Requirement	The organization must: a. Enforce physical access authorizations at entry and exit points to the facility where the information system resides by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards; b. Maintain physical access audit logs for entry and exit points; c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escort visitors and monitors visitor activity; e. Secure keys, combinations, and other physical access devices; f. Inventory physical access devices; and g. Changes combinations and keys at minimum when keys are lost, combinations are compromised, or individuals are transferred or terminated
Supplemental Guidance (from NIST 800-53)	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID

	provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.
Control Number	PE-6
Title	Monitoring Physical Access
SSA Requirement	The organization must: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs organization-defined frequency and upon occurrence of security incidents; and c. Coordinates results of reviews and investigations with the organizational incident response capability.
Supplemental Guidance (from NIST 800-53)	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

2.12 Planning

Control Number	PL-1
Title	Security Planning Policy and Procedures
SSA Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to SSA Data: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy; and 2. Security planning procedures.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	PL-2

Title	System Security Plan
SSA Requirement	The organization must: a. Develop a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distribute copies of the security plan and communicates subsequent changes to the plan to personnel and organizations with security responsibilities; c. Review the security plan for the information system; d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protect the security plan from unauthorized disclosure and modification. *Organization's security plan should include detail information specific to safeguarding SSA data.*
Supplemental Guidance (from NIST 800-53)	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

2.13 Risk Assessment

Control Number	RA-1
Title	Risk Assessment Policy and Procedures
SSA Requirement	The organization must: a. Develop, document, and disseminate to system owners using SSA Data: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	RA-3
Title	Risk Assessment
SSA Requirement	The organization must: a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in a risk assessment report or organization defined risk report document. c. Review risk assessment results annually; and e. Update the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Supplemental Guidance (from NIST 800-53)	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in

	security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.
Control Number	RA-5
Title	Vulnerability Scanning
SSA Requirement	The organization must: a. Scan for vulnerabilities in the information system and hosted applications with organization defined regularity and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; a. Analyze vulnerability scan reports and results from security control assessments; b. Remediate legitimate vulnerabilities within organization defined time periods in accordance with an organizational assessment of risk; and c. Share information obtained from the vulnerability scanning process and security control assessments with all impacted system owners to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Supplemental Guidance (from NIST 800-53)	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

2.14 Security Assessment and Authorization

Control Number	CA-2
Title	Security Assessments
SSA Requirement	The organization must: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation with organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

	c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to organization-defined individuals or roles.
Supplemental Guidance (from NIST 800-53)	Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.
Control Number	CA-3
Title	System Interconnections
SSA Requirement	The organization must: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].
Supplemental Guidance (from NIST 800-53)	This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization,

	organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.
Control Number	CA-7
Title	Continuous Monitoring
SSA Requirement	The organization must develop a continuous monitoring strategy and implement a continuous monitoring program that includes: a. Establishment of SSA data security controls to be monitored; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of SSA data security controls in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to organization-defined personnel or roles and to SSA when requested.
Supplemental Guidance (from NIST 800-53)	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.
Control Number	CA-8
Title	Penetration Testing
SSA Requirement	The organization must conduct penetration testing [Assignment: organization-defined frequency] on systems storing, processing, or transmitting SSA Data.
Supplemental Guidance (from NIST 800-53)	Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of

	potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

2.15 System and Communications Protection

Control Number	SC-7
Title	Boundary Protection
SSA Requirement	The organization information system must: a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
Supplemental Guidance (from NIST 800-53)	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.
Control Number	SC-8
Title	Transmission Confidentiality and Integrity
SSA Requirement	The organization information system must: Protect the confidentiality of transmitted information.
Supplemental Guidance (from NIST 800-53)	This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Number	SC-8(1)
Title	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
SSA Requirement	The organization information system must implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
Supplemental Guidance (from NIST 800-53)	Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.
Control Number	SC-13
Title	Cryptographic Protection
SSA Requirement	The organization information system must implement FIPS 140-3 compliant encryption modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Supplemental Guidance (from NIST 800-53)	Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
Control Number	SC-28
Title	Protection of Information at Rest
SSA Requirement	The organization information system must: Protect the confidentiality of SSA Data at rest.
Supplemental Guidance (from NIST 800-53)	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

2.16 System and Information Integrity

Control Number	SI-2
Title	Flaw Remediation
SSA Requirement	The organization must: a. Identify, report, and correct information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and

	potential side effects before installation; c. Installs security-relevant software and firmware updates, within acceptable organization standards, of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.
Supplemental Guidance (from NIST 800-53)	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.
Control Number	SI-3
Title	Malicious Code Protection
SSA Requirement	The organization must: a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the information system and real-time scans of files from external sources at the endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block malicious code or quarantine malicious code, and send alert to administrator for incident handling in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
Supplemental Guidance (from NIST 800-53)	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back

	doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.
Control Number	SI-4
Title	Information System Monitoring
SSA Requirement	The organization must: a. Monitor the information system to detect: 1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the information system through organization-defined techniques and methods; c. Deploy monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides organization-defined information system monitoring information to organization-defined personnel and SSA as needed.
Supplemental Guidance (from NIST 800-53)	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that

	bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.
Control Number	SI-4(5)
Title	Information System Monitoring | System Generated Alerts
SSA Requirement	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].
Supplemental Guidance (from NIST 800-53)	Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.
Control Number	SI-4(13)
Title	Information System Monitoring | Analyze Traffic / Event Patterns
SSA Requirement	The organization must: a. Analyzes communications traffic/event patterns for the information system; b. Develops profiles representing common traffic patterns and/or events; and c. Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
Supplemental Guidance (from NIST 800-53)	None

2.17 System and Services Acquisition

Control Number	SA-9
Title	External Information System Services
SSA Requirement	The organization must: a. Require that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with SSA TSSR, applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. *The state organization will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state organization will obtain from its contractors and agents a current list of the*

	employees of such contractors and agents with access to SSA data and provide such lists to SSA.
Supplemental Guidance (from NIST 800-53)	External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.
Control Number	SA-11
Title	Developer Security Testing And Evaluation
SSA Requirement	The organization must require the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Appendix A. Acronyms

Acronyms and terms used throughout this TSSR are defined in table below.

Table 1: Acronyms and Terms

Acronym	Definition
BCP	Business Continuity Plan
BIA	Business Impact Analyses
CMPPA	Computer Matching and Privacy Protection Act
CP	Contingency Plan
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DEC	Data Exchange Coordinator
DRP	Disaster Recovery Plan
EIE	Electronic Information Exchange
EIEP	Electronic Information Exchange Partners
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HTTP	Hyper Text Transfer Protocol
ID	Identification
IEA	Information Exchange Agreements
IP	Internet Protocol
ISA	Interconnection Security Agreement
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NNSC	National Network Service Center
NSA	National Security Agency
NVD	National Vulnerability Database
ODX	Office of Data Exchange
OIS	Office of Information Security
OMB	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Public Law
POC	Point of Contact
RBAC	Role-Based Access Control

SEQ	Security Evaluation Questionnaire
SOR	Systems of Records
SP	Special Publication
SSA	Social Security Administration
SSN	Social Security Number
STC	State Transmission/Transfer Component
TSSR	Technical System Security Requirements
URL	Uniform Resource Locator
USC	United States Code
WORM	Write-Once-Read-Many

Appendix B. Additional Definitions

Terms used throughout this TSSR and additional definitions are defined in table below.

Table 2: Additional Definitions

Term	Definition
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorizing Official	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Blacklisting	The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited Universal Resource Locators (URL)/websites.
Breach	Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where unauthorized persons have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording
Browsing	Requests for or queries of SSA data for purposes not related to the performance of official job duties
Cloud Computing	Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Controlled Area	Any area or space for which an organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Security	The ability to protect or defend the use of cyberspace from cyber attacks.
Data Exchange	Data Exchange is a logical transfer of information from one government entity's systems of records (SOR) to another agency's application or mainframe through a secure and exclusive connection.
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Degaussing	Degaussing is the method of using a "special device" (i.e., a device that generates a magnetic field) in order to disrupt magnetically recorded information. Degaussing can be effective for purging damaged media and media with exceptionally large storage capacities. Degaussing is not effective for purging non-magnetic media (e.g., optical discs).
Destruction	Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual medium should be able to withstand a laboratory attack.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Function	One or more persons or organizational components assigned to serve a particular purpose, or perform a particular role. The purpose, activity, or role assigned to one or more persons or organizational components.
Hub	As it relates to electronic data exchange with SSA, a hub is an organization, which serves as an electronic information conduit or distribution collection point. The term Hub is interchangeable with the terms "State Transmission Component," "State Transfer Component," or "STC."
Hybrid cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information Leakage	The intentional or unintentional release of information to an untrusted environment.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Infrastructure as a Service (IaaS)	The capability provided to the cloud consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Legacy System	A term usually referring to a corporate or organizational computer system or network that utilizes outmoded programming languages, software, and/or hardware that typically no longer receives support from the original vendors or developers.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Manual Transaction	A user-initiated operation (also referred to as a "user-initiated transaction"). This is the opposite of a system-generated automated process. Example: A user enters a client's information including the client's SSN and presses the "ENTER" key to acknowledge that input of data is complete. A new screen appears with multiple options, which include "VERIFY SSN" and "CONTINUE". The user has the option to verify the client's SSN or perform alternative actions.
Media Sanitization	Process by which data is irreversibly removed from media or the media is permanently destroyed.
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).
Overlay	A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.
Permission module	A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA data to an authorized process or transaction before initiating a transaction. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN. A properly configured Permission Module also enforces referential integrity and prevents unauthorized random browsing of PII.
Personally Identifiable Information	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Platform as a Service (PaaS)	The capability provided to the cloud consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Privileged User	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Screen Scraping	Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data. A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system. More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.
Security Breach	An act from outside an organization that bypasses or violates security policies, practices, or procedures.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems.
Security Control Assessment	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.
Security Incident	A security incident happens when a fact or event signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats.

Security Information Management (SIM)	SIM is software that automates the collection of event log data from security devices such as firewalls, proxy servers, intrusion detection systems and anti-virus software. The SIM translates the data into correlated and simplified formats.
Security Violation	An act from within an organization that bypasses or disobeys security policies, practices, or procedures.
Sensitive data	Sensitive data is a special category of personally identifiable information (PII) that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. It is sensitive information protected against unwarranted disclosure and carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse. Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.
Switched Multimegabit Data Service (SMDS)	SMDS is a telecommunications service that provides connectionless, high-performance, packet- switched data transport. Although not a protocol, it supports standard protocols and communications interfaces using current technology.
Software as a Service (SaaS)	The capability provided to the cloud consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
STC	A State Transmission/Transfer Component is an organization, which performs as an electronic information conduit or collection point for one or more other entities (also referred to as a hub).
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

System-generated transaction	A transaction automatically triggered by an automated system process. Example: A user enters a client's information including the client's SSN on an input screen and presses the "ENTER" key to acknowledge that input of data is complete. An automated process then matches the SSN against the organization's database and when the systems finds no match, automatically sends an electronic request for verification of the SSN to SSA.
Systems process	Systems Process refers to a software program module that runs in the background within an automated batch, online, or other process.
The Federal Risk and Authorization Program (FedRAMP)	FedRAMP is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.
Third Party	Third Party pertains to an entity (person or organization) provided access to SSA data by an EIEP or other SSA business partner for which one or more of the following apply: • is not stipulated access to SSA data by an information- sharing agreement between an EIEP and SSA • has no data exchange agreement with SSA • SSA does not directly authorize access to SSA data
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Transaction-driven	This term pertains to an automatically initiated online query of or request for SSA data by an automated transaction process (e.g., driver license issuance, etc.). The query or request will only occur the automated process meets prescribed conditions.
Uncontrolled transaction	This term pertains to a transaction that falls outside a permission module. An uncontrolled transaction is not subject to a systematically enforced relationship between an authorized process or application and an existing client record.
User	Individual, or (system) process acting on behalf of an individual, authorized to access an information system.
Verification Account Number	Unique agency-level account identifier used to determine account status prior to processing the verification or data exchange request.
Virtual Private Network	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Whitelisting	The process used to identify: (i) software programs that are authorized to execute on an information system; or (ii) authorized Universal Resource Locators (URL)/websites.

Security Certification Requirements for use of the *SSA Data Set* via the Centers for Medicare & Medicaid Services' (CMS) Hub

The Social Security Administration (SSA) does not allow new data exchange partners to begin receiving data electronically until the Authorized State Agency submits an approved Security Design Plan (SDP). SSA's Office of Information Security (OIS) usually performs an onsite security review to verify and validate that the management, operational, and technical controls conform to the requirements of the signed agreements between SSA and the Authorized State Agency, as well as applicable Federal law and SSA's technical systems security requirements (Attachment 4 to the Information Exchange Agreement (IEA)). As it concerns the use of the *SSA Data Set* via the Hub, OIS will waive the initial SDP/Certification for an existing Authorized State Agency if it meets all the following criteria:

1. The Authorized State Agency already has a functioning CMS-approved Integrated Eligibility Verification System (IEVS).
2. The Authorized State Agency is already receiving data from the Hub to support the Medicaid program and/or the Children's Health Insurance Program (CHIP).
3. The Authorized State Agency will only process requests for the *SSA Data Set* for administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency agrees that the SSA security controls identified in the IEA and Attachment 4 to the IEA will prevail for all SSA data received by the State Agency, including the *SSA Data Set*.
5. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through the Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.
6. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.

In the event that an Authorized State Agency decides to implement a new integrated eligibility system or use a different Authorized State Agency to implement the health or income maintenance data exchange process through the Hub, the Authorized State Agency will submit to SSA's OIS an SDP and be approved/certified prior to receipt of the *SSA Data Set* through the Hub. The Authorized State Agency will adhere to the following criteria, in addition to those stated in the IEA, section C, Program Questionnaire:

1. The Authorized State Agency agrees to provide an attestation to SSA that it has received certification through the CMS Hub approval MARS-E process.
2. The Authorized State Agency attests that it operates and has a CMS-approved IEVS and the IEVS initiates the request for the *SSA Data Set* for the State Agency's administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.

3. The Authorized State Agency uses a streamlined multi-benefit application. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency will not request the *SSA Data Set* through the Hub until it has successfully begun using the Hub for administration of Insurance Affordability Programs eligibility determinations. SSA will begin sending the *SSA Data Set* to the Authorized State Agency after the State Agency verifies that the Hub process works, as required by the CMS Hub approval MARS-E process.
5. The Authorized State Agency agrees to participate in SSA's SDP/Certification process prior to transmitting requests for the *SSA Data Set* through the Hub and to participate in SSA's triennial security compliance reviews on an ongoing basis.
6. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.

ATTACHMENT 6

09/27/06

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information

1. Information about the individual making the report to the NCSC:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					
Check one of the following:					
Management Official		Security Officer		Non-Management	

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic? (circle one):

If Electronic, what type of device?

Laptop		Tablet		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Blackberry Phone #	
Hard Drive		Floppy Disk		USB Drive			
Other (describe):							

Additional Questions if Electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name:			
Cardholder's SSA logon PIN:			
Hardware Make/Model:			
Hardware Serial Number:			

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. **If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:**

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					

5. **Circumstances of the loss:**
   a. When was it lost/stolen?

   b. Brief description of how the loss/theft occurred:

   c. When was it reported to SSA management official (date and time)?

6. **Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)**

09/27/06

7. **Which reports have been filed? (include FPS, local police, and SSA reports)**

Report Filed	Yes	No	Report Number
Federal Protective Service			
Local Police			

	Yes	No
SSA-3114 (Incident Alert)		
SSA-342 (Report of Survey)		
Other (describe)		

8. **Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):**

INFORMATION EXCHANGE AGREEMENT
BETWEEN
CENTERS FOR MEDICARE & MEDICAID SERVICES
AND
THE PARTICIPATING MEDICAID AGENCY
FOR THE
DISCLOSURE AND EXCHANGE OF CERTAIN MEDICARE AND MEDICAID DATA
OF DUALLY ELIGIBLE INDIVIDUALS

CMS AGREEMENT NO. 2020-50

I. PURPOSE, LEGAL AUTHORITIES, AND DEFINITIONS

A. Purpose

This Information Exchange Agreement, hereinafter the "Agreement," establishes the terms, conditions, safeguards, and procedures under which the Centers for Medicare & Medicaid Services (CMS) and the undersigned state (through or on behalf of the agency that operates the state's or territory's Medicaid plan – hereinafter the "Participating Medicaid Agency" (PMA)) will exchange certain Personally Identifiable Information (PII) derived from CMS Data regarding dually eligible beneficiaries, including Protected Health Information (PHI), for the purpose of the administration of a number of programs for Dually Eligible Individuals for the ***Massachusetts Executive Office of Health and Human Services***. This IEA and the corresponding Data Request Attestation (DRA) document the PMA's assertions regarding its legal authority to request and receive such data, as well as the terms, conditions, safeguards and procedures CMS imposes on the PMA as a condition of the PMA's receipt of such data.

When executed, this IEA, along with a corresponding DRA, will offer PMAs a single streamlined data request process for such data (herein collectively referred to as "CMS Data") for use in the administration of a number of programs for dually eligible beneficiaries, including opportunities to request certain elective data files, as well as the means of carrying out operational data exchanges that support the dually eligible population. These activities are described more fully in Section III.A., below. The data request process for such data will be managed by CMS' Federal Coordinated Health Care Office (known as the "Medicare-Medicaid Coordinated Office" or "MMCO").

The elective data files and exchange programs may include, but are not limited to, the Territory Beneficiary Query (TBQ) File, the ability to make Enrollment Data Base (EDB) File queries, and the data files shared under the Medicare-Medicaid Data Sharing Program. Again, depending on the PMA's status as a State or Territory, the operational exchanges are the data exchanged for the State Buy-In File Exchange and the Medicare

For each entity signatory to this Agreement, CMS and the relevant PMA are each a "Party" and collectively "the Parties." By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein, as well as applicable law and regulations. The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of CMS and the respective PMA.

This Agreement, and any data disclosures under it, do not constitute a "matching program" as defined by the Privacy Act of 1974 (5 United States Code (U.S.C.) § 552a(a)(8)). The purpose of the disclosures described herein is not for establishing or verifying initial or continuing entitlement to or eligibility of individuals with respect to federal benefit programs.

Any disclosure(s) of CMS Data, or any individually-identifiable derivative of this CMS Data, by the undersigned or its agents to a Downstream User, as defined below, shall be made in accordance with applicable law as well as any applicable provisions in this or other governing documents.

B. Legal Authorities

Among other potential provisions, the following statutes and regulations govern the exchange and/or disclosure of data under this agreement and the corresponding DRA:

1. CMS:

   a. The Privacy Act of 1974 (5 U.S.C. § 552a), and the regulations and applicable system of record (SOR) notices (SORNs) as detailed in Section III.B; the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, published at 81 Federal Register (FR) 49689 (July 28, 2016).

   b. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules at 45 CFR parts 160 and 164.

   c. The data exchanged under this Agreement supports the responsibilities of the MMCO as established by section 2062 of Public Law (Pub. L.) 111-148, which specifically includes providing states with the tools necessary to develop programs to align Medicare and Medicaid benefits for dually eligible individuals (not applicable to territories).

   d. Section 1106 of the Social Security Act of 1935 (the Act), which authorizes the disclosure of data where such disclosures are authorized by statute or regulation.

   e. Section 1843 of the Act (Hospital Insurance (HI), § 1818(g)), as amended, and the implementing regulations at 42 CFR § 407.40 et seq., and § 406.26 which require the Secretary of the U.S. Department of Health and Human Services to enter into a State Buy-in agreement at the request of any state or territory.

   f. 42 CFR § 423.505(m), which defines what Part D Prescription Drug Event (PDE) Data may be exchanged/disclosed.

2. PMAs:

   a. The HIPAA Privacy and Security Rules at 45 CFR parts 160 and 164.

   b. Section 1935(c) of the Act.

   c. The Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA) (Pub. L. 108-173, enacted on December 8, 2003) and the implementing regulations at 42 CFR § 423.910, which established reporting by states, and the frequency with which states must submit a data file identifying Dually Eligible Individuals in their state (not applicable to territories). The file is called the "MMA File," but is occasionally referred to as the "State Phasedown File."

C. Definitions

The following terms have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information, or (2) an authorized user accesses, or potentially accesses personally identifiable information for an other than authorized purpose [HHS Policy and Plan for Preparing for the Responding to a Breach of Personally Identifiable Information (PII) (June 29, 2017)].

2. "Care Coordination" means uses of the data (e.g., analysis, monitoring, or feedback) to support interventions — and/or the design of interventions — at the individual beneficiary level that have the potential to improve the care of Dually Eligible Individuals. Depending on circumstances, such activities may include activities that qualify as "treatment" when performed by providers, and may include certain activities listed in the first and second paragraphs of the definition of "Health Care Operations" in the HIPAA Privacy Rule at 45 CFR § 164.501.

3. "CMS" means the Centers for Medicare & Medicaid Services. CMS regulatory authority includes the oversight of the Medicare program, the federal portion of the Medicaid program and State Children's Health Insurance Program, the Health Insurance Marketplace, and related quality assurance activities.

4. "CMS Data" means any of the data retrieved from the SORs cited in Section III.B, below, that are sent from CMS to the PMA under this Agreement and the corresponding DRA. CMS Data includes Specified Medicare Data (see below for definition of "Specified Medicare Data").

5. "CMS DRA" or "DRA" means the executed "Medicaid-Medicare Dual Eligible Data Request and Attestation Form" that corresponds to this IEA. The CMS DRA tracks the disclosure(s) of CMS Data to the PMA.

6. "CMS DRA Custodian Form" means the "Medicaid-Medicare Dual Eligible Data Request and Attestation Custodian Form." The CMS DRA Custodian Form supplements the CMS DRA Form. The CMS DRA Custodian Form tracks data custodians that provide data storage for the PMA and, by signing, the data custodians acknowledge the terms specified in the CMS DRA and CMS DRA Custodian Form.

7. "Custodian" means the individual or entity that is tasked by the PMA with primary responsibility for ensuring that the data received under this Agreement is used, disclosed and maintained in accordance with the terms, conditions, safeguards and procedures laid out in this Agreement and applicable law.

8. "Downstream User" means any person or entity (e.g., a treating practitioner contractor, business associate or subcontractor of the PMA) that receives CMS Data or individually identifiable derivative data from the PMA in accordance with the terms of this Agreement and the corresponding DRA.

9. "Dually Eligible Individual" or "Dually Eligible Beneficiary" means an individual who is entitled to both Medicare benefits under Title XVIII of the Act and medical assistance under Title XIX of the Act.

10. "Enrollment Database File" or "EDB File" refers to the file produced from the EDB data query process between CMS and a state to determine eligibility and enrollment information for Dually Eligible Individuals. The EDB File includes detailed Medicare beneficiary information on Medicare Parts A and B only.

11. "Encounter Data" means the record submitted to CMS about an enrollee receiving any item(s) or service(s) provided through Medicaid or Medicare under a prepaid, capitated, or any other risk based payment methodology. Encounter Data records are maintained in the CMS Encounter Data System (EDS).

12. "Health Care Operations" means those activities described in the first and second paragraph of the HIPAA Privacy Rule at 45 CFR § 164.501, or the fraud and abuse-related activities described in § 164.506(c)(4).

13. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 as amended by the subsequent enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009).

14. "Incident" is defined by OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

15. "Medicaid" means the health benefit program established under Title XIX of the Act.

16. "Medicare" means the health benefit program established under Title XVIII of the Act.

17. "Medicare-Medicaid Coordination Office" or "MMCO" means the Federal Coordinated Health Care Office of CMS.

18. "MMA File" or "State Phasedown File" means the file states submit to CMS to identify Dually Eligible Individuals in their state, including full-benefit and partial-benefit Dually Eligible Individuals (that is, those individuals who get Medicaid help with Medicare premiums, and, often, for cost-sharing). It is called the "MMA File" based on the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA) (Pub. L. 108-173, enacted on December 8, 2003). This is not applicable to territories.

19. "Medicare-Medicaid Data Sharing Program" means the elective process under which CMS shares Medicare data with PMAs for the purposes of Care Coordination, Program Integrity, and/or Quality Improvement. Under this process, CMS discloses Specified Medicare Data to the PMA. This is not applicable to territories.

20. "Participating Medicaid Agency" or "PMA" means a state or territory Medicaid agency or other agency of the state or territory tasked with assisting the Medicaid agency. PMA includes such parties' contractors, subcontractors, and agents that work on behalf of such Medicaid agency to carry out Medicaid program functions.

21. "PDE Data" means Medicare Part D Prescription Drug Event data that are reported to CMS by Part D prescription drug plan sponsors.

22. "Personally Identifiable Information" or "PII" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual [HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII) (June 29, 2017)].

23. "Program Integrity" refers to activities designed to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat health care fraud, waste, or abuse, to include the improper payments in the PMA's Medicaid program. When done by a HIPAA-covered entity, these are the "health care fraud and abuse detection or compliance" activities described in the fourth paragraph of the HIPAA Privacy Rule's definition of "Health Care Operations," and at 45 CFR § 164.506(c)(4). When done by a government actor under a legal mandate, these activities may qualify as "Health Care Oversight" under the HIPAA Privacy Rule.

24. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 CFR § 160.103.

25. "Quality Improvement" means uses of the data (e.g., analysis, monitoring, or feedback) to support interventions — and/or the design of interventions — at the individual dual eligible beneficiary level that have the potential to improve or assess the quality of care of Dually Eligible Individuals and include certain activities described in the first and second paragraphs of the definition of "Health Care Operations" in the HIPAA Privacy Rule at 45 CFR § 164.501.

26. "Specified Medicare Data" means any of the following types of data that CMS shares as part of the Medicare-Medicaid Data Sharing Program for Care Coordination, Quality Improvement, or Program Integrity, including, but not limited to: Medicare Part A and Part B claims data, PDE data, eligibility and enrollment data, Minimum Data Set (MDS) data, Outcome and Assessment Information Set (OASIS) data, and encounter data from Encounter Data System (EDS). Specified Medicare Data includes derivative files built by or for the PMA out of Specified Medicare Data that is subject to this Agreement. PMAs request these data via the CMS DRA. Specified Medicare Data represents a specific subset of CMS Data.

27. "State Buy-in File" or "Buy-in File" means the data exchange between CMS and a state or territory where the state or territory sends CMS a data file to determine beneficiary Part A and B premiums liability.

28. "Territory Beneficiary Query" or "TBQ" means the data query where a PMA requests data from the CMS MDB to determine eligibility and enrollment information for Dually Eligible Individuals. Under this query process, PMAs query for detailed Medicare beneficiary information on Medicare Parts A, B, C (Medicare Advantage), and D (including plan enrollment and Low Income Subsidy (LIS) eligibility).

II. RESPONSIBILITIES OF CMS AND THE PARTICIPATING MEDICAID AGENCY

A. Responsibilities of CMS

CMS will track and maintain a record of any PMA disclosures conducted pursuant to this Agreement.

Following the execution of this Agreement and the corresponding CMS DRA, CMS will send CMS Data to the PMA in a timely and secure manner. The CMS Data may be sent electronically or physically, as determined by CMS.

B. Responsibilities of the PMA

The PMA attests that it will maintain, use, and disclose the CMS Data in accordance with this Agreement, the corresponding DRA, and other applicable law, including any applicable state laws.

CMS Data obtained under this Agreement may be used only for purposes specifically indicated in this Agreement; other uses are not permitted. However, the PMA may request re-use of the CMS Data for additional purposes outside of this Agreement; such requests are subject to CMS review and approval before re-use may occur.

1. CMS Medicare-Medicaid Data Sharing Program, only:

   In order to receive Specified Medicare Data under the Medicare-Medicaid Data Sharing Program, the PMA must submit a request to CMS that includes the following: (1) an acknowledgement that the PMA is a HIPAA-covered entity; (2) a list of the requested data files and, if applicable, data elements; and (3) an attestation that the Specified Medicare Data being requested is the "minimum necessary" to carry out the stated use of the data, as defined in the HIPAA Privacy Rule at 45 CFR § 164.502(b). CMS will only approve requests for Specified Medicare Data that assert that the PMA is requesting it for the PMA's Quality Improvement, Care Coordination, and/or Program Integrity purposes. The PMA should consult with legal or other counsel if it is unsure of whether it is requesting the data for those purposes. If such assertions can be made, the request should be made using the CMS DRA.

   The PMA should maintain a:

   a. list of all Downstream Users to whom the PMA shares CMS Data; and,

   b. data management plan that should be available upon CMS request.

III. DESCRIPTION OF THE DATA THAT MAY BE DISCLOSED

A. Exchanges and Data Files Covered by this Agreement

1. CMS Medicare-Medicaid Data Sharing Program – CMS shares (upon state request and CMS approval) Specified Medicare Data with state PMAs for the purposes of Care Coordination, Program Integrity, and/or Quality Improvement related to the state's dually eligible population. If approved, CMS discloses (subject to the provisions of this Agreement, the corresponding DRA and applicable law) Specified Medicare Data. The Medicare-Medicaid Data Sharing Program is elective.

2. Enrollment Database (EDB) File – The EDB process is a batch data query in which PMAs request data from CMS EDB to determine dual status eligibility. The PMA submits a finder file and CMS returns information on Medicare Part A entitlement and Part B enrollment only. The EDB File is elective.

3. Territory Beneficiary Query (TBQ) File – The TBQ File is produced by a batch data query in which PMAs request data from CMS MBD to determine dual status eligibility. For territories, CMS uses the data to establish Medicare Part D LIS. The PMA submits a finder file, and CMS returns information on Medicare Parts A, B, C (Medicare Advantage), and D, including LIS eligibility. PMAs can submit TBQ Request Files to obtain batch data from the CMS Medicare Beneficiary Database (MBD) (i.e., the data populated from the MMA file exchange). The TBQ File is elective.

4. Medicare Modernization Act (MMA) File Exchange – State PMAs submit files at least monthly to the CMS MBD to identify all Dually Eligible Individuals in the state to CMS. CMS automatically returns a response file to the state upon processing the

MMA File submission. The MMA File Exchange is operational, and open to state PMAs, only.

5. State Buy-In File Exchange – CMS and PMAs exchange data on who is enrolled in Medicare and which parties are liable for paying that beneficiary's Parts A and B premiums. These data exchanges support state/territory, CMS, and the Social Security Administration (SSA) premium accounting, collections, and enrollment functions. To effectuate the state payment of Medicare Part A or Part B premiums, a state submits data on a buy-in file to CMS, which includes a record for each Medicare beneficiary for whom the state is adding or deleting coverage, or changing buy-in status. In response, CMS returns an updated transaction record, as well as a Part A or Part B billing record showing the state's premium responsibility. The State Buy-in File Exchange is operational, and open to state and territory PMAs.

B. Systems of Records

CMS will provide CMS Data from the following SORs:

1. CMS Encounter Data System (EDS), System No. 09-70-0506, published at 79 FR 34539 (June 17, 2014), as amended at February 14, 2018 (83 FR 6591). Data maintained in the EDS will be released pursuant to routine use number 2 and number 7, as set forth in the SORN.

2. Enrollment Data Base (EDB), System No. 09-70-0502; last modified at 73 FR 10249 (February 26, 2008), as amended at April 23, 2013 (78 FR 23938), February 18, 2016 (81 FR 8204) and February 14, 2018 (83 FR 6591). Data maintained in the EDB will be released pursuant to routine use number 2 and 10, as set forth in the SORN.

3. Home Health Agency Outcome and Assessment Information Set (OASIS), System No. 09-70-0522, published at 72 FR 63906 (November 13, 2007), as amended at April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257) and February 14, 2018 (83 FR 6591). Data maintained in the OASIS will be released pursuant to routine use number 2 and number 8, as set forth in the SORN.

4. Long-term Care Minimum Data Set (MDS), System No. 09-70-0528, published at 72 FR 12801 (March 19, 2007), as amended at April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257) and February 14, 2018 (83 FR 6591). Data maintained in the MDS will be released pursuant to routine use number 2 and number 9, as set forth in the SORN.

5. Medicare Beneficiary Database (MBD), System No. 09-70-0536 last modified at 71 FR 70396 (February 14, 2018), as amended at April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257), February 14, 2018 (83 FR 6591). Data maintained in the MBD will be released pursuant to routine use number 2 and 11, as set forth in the SORN.

6. Third Party System (TPS), System No. 09-70-0505; published at 72 FR 36000 (July 2, 2007), as amended at February 14, 2018 (83 FR 6591). Data maintained in the TPS will be released pursuant to routine use number 2 and 7, as set forth in the SORN.

C. CMS Data Repositories

7. Chronic Condition Warehouse (CCW), System No. 09-70-0573, published at 79 FR 64802 (October 31, 2014), as amended at February 14, 2018 (83 FR 6591). Data maintained in the CCW will be released pursuant to routine use number 2 and number 11, as set forth in the SORN.

8. Medicare Integrated Data Repository (IDR), System No. 09-70-0571, published at 71 FR 74915 (December 13, 2006), as amended at October 20, 2011 (76 FR 65196), April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257) and February 14, 2018 (83 FR 6591). Data maintained in the IDR will be released pursuant to routine use number 2 and number 11, as set forth in the SORN.

D. Number of Records Involved and Operational Time Factors

As of 2018, the nationwide CMS Data records include approximately 12 million beneficiaries who are identified as Dually Eligible Individuals. Medicare records disclosed to the PMA under this Agreement will be limited to Dually Eligible Individuals residing in the PMA's state or territory.

The records exchanged under this agreement and the corresponding DRA, specifically through the MMA File Exchange, will be used, in part, to confirm and/or add to CMS's current records regarding dually eligible Medicare beneficiaries.

E. Data Elements Involved

The CMS Data made available in accordance with applicable law upon the request of the PMA and approval by CMS includes data elements for Dually Eligible Individuals residing in the PMA's state or territory to support activities as detailed in the Agreement. CMS Data made available under this agreement may include records that include some or all of the following data elements: beneficiary data (name, date of birth, gender, Social Security Number, mailing address, and Medicare Beneficiary Identifier (MBI)) and provider data (Provider Identification Number). Data elements may vary depending on data file.

Under the MMA File Exchange and State Buy-in File Exchange, the PMA will provide the following data elements to CMS for purposes of identifying individuals for whom data will be exchanged: name, date of birth, gender, and Social Security Number.

Under the TBQ File and EDB File, CMS does not retain the data from the PMA finder files and therefore the PMA does not provide data to CMS.

Under CMS Medicare-Medicaid Data Sharing Program, the PMA does not provide data to CMS.

IV. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The parties acknowledge that CMS retains all ownership rights to the CMS Data that PMA

obtains under the terms of this Agreement, and that PMA does not obtain any right, title, or interest in any of the data furnished by CMS. The PMA will only retain the CMS Data and any derivative of the CMS Data for the period of time required by law or for any processing or purpose related to the approved uses for which the data were received.

V. PROCEDURES FOR PRIVACY AND SECURITY

A. In signing this agreement and the corresponding DRA, the PMA attests that the requested CMS Data will be protected as required by applicable law, including but not limited to the HIPAA Privacy and Security Rules at 45 CFR parts 160 and 164, including through the establishment of appropriate administrative technical and physical safeguards to protect the integrity, security, and confidentiality of the data, and to prevent unauthorized use or access to it. Additionally, the PMA acknowledges that various provisions of the U.S. Code, including, but not limited to, the Privacy Act (5 U.S.C. § 552a), 42 U.S.C. 1320d–6 (HIPAA), and Title 18, as well as the corresponding regulations, specify civil and/or criminal penalties that may be applied by applicable law enforcement authorities with respect to various misuse, including wrongful acquisition or use of, data. In signing this agreement, the PMA further affirms that such safeguards will provide a level and scope of security that is not less than the level and scope of security requirements established for federal agencies by the OMB in:

1. OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems,

2. Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems," and

3. Special Publication 800-53 "Recommended Security Controls for Federal Information Systems."

The PMA acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, bidder identifiable or deducible information derived from the shared file(s) is prohibited. Further, the PMA agrees that the data must not be physically moved, transmitted, or disclosed in any way from or by the Data Custodians' site(s) to an entity not listed on the IEA or DRA without written approval from CMS unless such movement, transmission or disclosure is required by a law. For example, CMS expects the PMA to, at minimum:

1. Protect PII and PHI that is furnished by CMS under this Agreement from loss, theft or inadvertent disclosure;

2. Ensure that laptops and other electronic devices/media containing PII or PHI are encrypted and password-protected; and,

3. Send emails containing PII or PHI only if encrypted and being sent to and being received by e-mail addresses of persons authorized to receive such information.

B. CMS reserves the right to conduct onsite inspections to monitor compliance with this Agreement and the corresponding DRA until such time CMS Data is destroyed and/or the CMS DRA is terminated.

C. In signing this agreement and the corresponding DRA, the PMA attests that the requested data will be maintained, used, and disclosed only in a manner that is in accordance with the requirements of this agreement and the corresponding CMS DRA.

VI. LOSS REPORTING

Incidents and/or Breaches that implicate PHI must be addressed and reported, as applicable, in accordance with the HIPAA Breach Notification Rule, 45 CFR §§ 164.400 - 414.

The PMA shall further handle and report Incidents and Breaches in accordance with CMS' documented Incident Handling and Breach Notification procedures and in accordance with 42 CFR §§ 431.300 - 306. In addition to, and notwithstanding, PMA's compliance with all applicable obligations and procedures, PMA procedures must also address how the PMA will report the following to MMCO:

A. Identify Incidents and/or Breaches;

B. Determine if personally identifiable information is involved in Incidents;

C. Determine whether Breach notification is required, and, if so, bear costs associated with the Breach notice as well as any mitigation measures; and,

D. Immediately notify CMS of any actual or suspected access, use, or disclosure of the data requested herein that is not in accordance with applicable law, including, but not limited to, the HIPAA Privacy Rule. PMA further affirms that it will report any breaches of PII from the CMS data files, loss of these data or disclosure to any unauthorized persons to the CMS Action Desk by telephone at (410) 786-2580 or by email notification at cms_it_service_desk@cms.hhs within one hour of discovery, and will cooperate fully in the federal security incident process.

VII. RECORDS USAGE AND REDISCLOSURE RESTRICTIONS

The PMA agrees that the CMS Data will be used and disclosed only as provided in this Agreement and the corresponding DRA.

VIII. REIMBURSEMENT AND REPORTING

No funds will be exchanged under this Agreement for any work to be performed by the PMA and CMS to carry out the requirements of this Agreement. CMS and PMA will provide data to each other at no cost.

IX. APPROVAL AND DURATION OF AGREEMENT

A. Effective Date: This Agreement will become effective when signed by authorized officials of both parties.

B. Duration: The duration of this Agreement is five years. Parties to this Agreement may execute a new agreement prior to the close of a five-year period. The IEA remains in effect if both parties are working towards executing a new agreement.

C. Modification: The parties may modify this Agreement at any time by a written modification agreed upon by both parties.

D. Termination: Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 30 days after the date of that notice or at a later date specified in the notice. PMA agrees that it has the duty to protect and maintain the privacy and security of CMS Data, and that duty shall continue in full force and effect until such CMS Data is returned and/or destroyed. For any CMS Data or derivative data with respect to which destruction is not feasible, the privacy and security requirements of this Agreement and the corresponding DRA shall survive the termination or expiration of this Agreement.

E. Breach: If CMS determines that there may have been an Incident or Breach of the CMS Data or individually identifiable derivative data or information by the PMA, its contractors and/or agents, and/or any Downstream Users that violates the terms of this Agreement, CMS may, in its sole discretion, immediately and unilaterally terminate this Agreement upon notice to PMA. PMA covenants and agrees to cease using and return and/or destroy all CMS Data and derivatives therefrom in its possession, contractors'/agents' possession, or Downstream Users' possession immediately upon notice of termination for an Incident or Breach unless otherwise required by law. PMA agrees that it has the duty to protect and maintain the privacy and security of CMS Data, and that duty shall continue in full force and effect until such data are returned and/or destroyed. For any such data with respect to which return/destruction is not feasible, the privacy and security requirements of this Agreement and the corresponding DRA shall survive the termination or expiration of this Agreement.

X. PERSONS TO CONTACT

A. CMS program and policy contact:

Central MMCO Data Sharing mailbox: MMCODataSharing@cms.hhs.gov

Sharon Donovan, Director
Federal Coordinated Health Care Office
Program Alignment Group
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Location: S3-13-23
Baltimore, MD 21244-1850
Telephone: (410) 786-9187

E-Mail: sharon.donovan1@cms.hhs.gov

Candace Anderson, Management Analyst
Medicare-Medicaid Coordination Office
Program Alignment Group
Federal Coordinated Health Care Office
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Location: S3-13-05
Baltimore, MD 21244-1850
Telephone: (410) 786-1553
E-Mail: candace.anderson@cms.hhs.gov

B. Privacy Policy and Agreement Issues:

Barbara Demopulos, CMS Privacy Act Officer
Division of Security, Privacy Policy and Governance
Information Security and Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Location: N1-14-40
Baltimore, MD 21244-1850
Telephone: (410) 786-6340
E-mail: Barbara.Demopulos@cms.hhs.gov

C. Participating Medicaid Agency Points of Contact (POC)

Jason Gong
Data Service Analyst, Data Integrity
Office of Medicaid
Massachusetts Executive Office of Health and Human Services
1 Ashburton Pl. 11th Fl.
Boston, MA 02108
Telephone: (617) 276-4213
E-mail: jason.gong@mass.gov

With a copy to:

Office of the General Counsel
Attn: Privacy Officer
Massachusetts Executive Office of Health and Human Services
1 Ashburton Pl. 11th Fl.
Boston, MA 02108
E-mail: privacy.officer@mass.gov

XI. APPROVALS

A. Centers for Medicare & Medicaid Services Program Official

The authorized program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: (Signature of Authorized CMS Program Official)

Sharon M. Donovan -S Digitally signed by Sharon M. Donovan -S Date: 2021.06.03 15:39:18 -04'00'

Sharon Donovan, Director Date:
Program Alignment Group
Federal Coordinated Health Care Office
Centers for Medicare & Medicaid Services

B. Centers for Medicare & Medicaid Services Approving Official

The authorized approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved By: (Signature of Authorized CMS Approving Official)

Michael E. Pagels -S Digitally signed by Michael E. Pagels -S
Date: 2021.06.24 15:41:36 -04'00'

Michael Pagels, Director **Date:**
Division of Security, Privacy Policy and Governance,
and
Senior Official for Privacy
Information Security and Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services

C. Participating Medicaid Agency Approving Official

The authorized Participating Medicaid Agency approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

NAME OF PARTICIPATING MEDICAID AGENCY

State Name: Massachusetts

Medicaid Agency Name: MassHealth

Approved By: (Signature of Authorized State or Territory Approving Official)

6/1/21

Daniel Tsai **Date:**
Assistant Secretary and Director of MassHealth
Massachusetts Executive Office of Health and Human Services

Appendix K-2

Artificial Intelligence (AI)

1. DEFINITIONS OF TERMS

The following terms or their abbreviations, when capitalized in this Appendix are defined as follows, unless context clearly indicates otherwise.

AI System – any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

Artificial Intelligence (AI) – a machine-based system that can, for a given set of human objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. AI includes Generative Artificial Intelligence and Machine Learning.

Commonwealth Training Data – training prompts, and PI regardless of whether they can be linked to a specific individual or have otherwise been de-identified in accord with the standards set forth in 45 CFR § 164.514, used for training an AI system through fitting its learnable parameters.

Generative Artificial Intelligence (Generative AI) – a type of artificial intelligence that emulates the structure and characteristics of input data in order to generate derived synthetic content. This can include text, images, audio, video, or other formats.

Input Data – data provided to or directly acquired by an AI system on the basis of which the system produces an output.

Machine Learning – a set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

Model Weight – a numerical parameter within an AI model that helps determine the model's outputs in response to inputs.

Output Data – data generated by an AI System after processing input data.

2. CONTRACTOR RESPONSIBILITIES

The Contractor shall meet the following requirements related to AI in addition to all other requirements set forth in the Contract.

A. Effect of Termination

1. The Contractor shall ensure that all Model Weights, Output Data, and Commonwealth Training Data (collectively, ("EOHHS Data") are either securely purged or returned to the Commonwealth as directed by EOHHS. In no event shall the Contractor destroy any EOHHS Data without first obtaining EOHHS' approval. If EOHHS directs the Contractor to purge EOHHS Data, the Contractor shall ensure EOHHS Data is purged and rendered unrecoverable in accordance with all Applicable Laws, retention laws and regulations, and EOHHS and EOTSS data security policies. If EOHHS directs the Contractor to return EOHHS Data, EOHHS Data shall be returned in a format specified by EOHHS through a secure transfer method agreed upon by both parties. The Contractor shall, within three (3) business days of the return or purging of EOHHS Data, certify to EOHHS in writing that all PI and Security Information has been returned or purged in accordance with this Section and neither the Contractor nor any of its subcontractors or agents retains any EOHHS Data. The Contractor is prohibited from using any EOHHS Data or derivative works for any purpose beyond the termination of this Agreement without EOHHS prior written consent. EOHHS reserves the right to verify compliance with these requirements.

B. Representation and Warranty of Non-Deceptive, Non-Discriminatory AI System

The Contractor represents and warrants as follows:

1. Any AI system the Contractor creates or uses in connection with the Contract has been rigorously tested and validated to ensure it is free of harmful biased and discriminatory results and complies with all applicable laws, regulations, and guidelines, ensuring that its deployment and use do not violate any statutory, regulatory requirements or guidelines related to non-discrimination, fairness and accurate results including but not limited to 89 FR 37522, Massachusetts Attorney General's AI Advisory, EOTSS Generative AI Guidelines;
2. The AI system's results will not be unfair or deceptive and will adhere to all applicable standards of accuracy and reliability including but not limited to 89 FR 37522, Massachusetts Attorney General's AI Advisory, EOTSS Generative AI Guidelines; and
3. The Contractor shall proactively and continuously validate and monitor the AI system for any instances of bias or discrimination and will take immediate corrective actions to rectify any identified issues and prevent future occurrences.

C. Indemnification

1. For the avoidance of doubt and consistent with the Commonwealth Terms and Conditions, the Contractor shall indemnify and hold harmless EOHHS from any and all claims, liabilities, and costs arising from personal injury, property damage,

intellectual property rights infringement, security or data breaches, unauthorized disclosure of data, and any other claims arising from the design, use, or implementation of any AI system the Contractor creates or uses in connection with this Contract. Upon prompt notification by EOHHS, the Contractor may participate in the defense of any claims and any settlement or judgment. EOHHS shall not be liable for any costs incurred by the Contractor under this provision.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
MH and SA OP Services	90791*	UG - Doctoral Level (Child Psychiatrist)	Psychiatric Diagnostic Evaluation	$208.27
MH and SA OP Services	90791*	U6 - Doctoral Level (MD / DO)	Psychiatric Diagnostic Evaluation	$167.15
MH and SA OP Services	90791*	AH - Doctoral Level (PhD, PsyD, EdD)	Psychiatric Diagnostic Evaluation	101 CMR 329
MH and SA OP Services	90791*	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Psychiatric Diagnostic Evaluation	$144.66
MH and SA OP Services	90791*	HO - Master's Level	Psychiatric Diagnostic Evaluation	101 CMR 329
MH and SA OP Services	90791*	U3 - Intern (PhD, PsyD, EdD)	Psychiatric Diagnostic Evaluation	$81.83
MH and SA OP Services	90791*	U4 - Intern (Master's)	Psychiatric Diagnostic Evaluation	$72.20
MH and SA OP Services	90791	HA - CANS; UG-Doctoral Level (Child Psychiatrist)	CANS - Psychiatric Diagnostic Evaluation, Members under 21	$223.27
MH and SA OP Services	90791	HA - CANS; U6-Doctoral Level (MD / DO)	CANS - Psychiatric Diagnostic Evaluation, Members under 21	$182.15
MH and SA OP Services	90791	HA - CANS; AH-Doctoral Level (PhD, PsyD, EdD)	CANS - Psychiatric Diagnostic Evaluation, Members under 21	101 CMR 329
MH and SA OP Services	90791	HA - CANS; SA, UF -Nurse Practitioner/Board Certified RNCS and APRN-BC	CANS - Psychiatric Diagnostic Evaluation, Members under 21	$159.66
MH and SA OP Services	90791	HA - CANS; HO-Master's Level	CANS - Psychiatric Diagnostic Evaluation, Members under 21	101 CMR 329
MH and SA OP Services	90791	HA - CANS; U3-Intern (PhD, PsyD, EdD)	CANS - Psychiatric Diagnostic Evaluation, Members under 21	$96.83
MH and SA OP Services	90791	HA - CANS; U4-Intern (Master's)	CANS - Psychiatric Diagnostic Evaluation, Members under 21	$87.20
MH and SA OP Services	90792	UG - Doctoral Level (Child Psychiatrist)	Psychiatric Diagnostic Evaluation with Medical Services	$131.80
MH and SA OP Services	90792	U6 - Doctoral Level (MD / DO)	Psychiatric Diagnostic Evaluation with Medical Services	$114.31
MH and SA OP Services	90792	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Psychiatric Diagnostic Evaluation with Medical Services	$104.57
MH and SA OP Services	90832	UG - Doctoral Level (Child Psychiatrist)	Individual Psychotherapy, approximately 20-30 minutes	$69.60
MH and SA OP Services	90832	U6 - Doctoral Level (MD / DO)	Individual Psychotherapy, approximately 20-30 minutes	$69.60
MH and SA OP Services	90832	AH - Doctoral Level (PhD, PsyD, EdD)	Individual Psychotherapy, approximately 20-30 minutes	101 CMR 329
MH and SA OP Services	90832	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Individual Psychotherapy, approximately 20-30 minutes	$59.16
MH and SA OP Services	90832	HO - Master's Level	Individual Psychotherapy, approximately 20-30 minutes	101 CMR 329
MH and SA OP Services	90832	U7 - Certified Addiction Counselor / Certified Alcohol & Drug Abuse Counselor	Individual Psychotherapy, approximately 20-30 minutes	$52.20

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
MH and SA OP Services	90832	U3 - Intern (PhD, PsyD, EdD)	Individual Psychotherapy, approximately 20-30 minutes	$35.49
MH and SA OP Services	90832	U4 - Intern (Master's)	Individual Psychotherapy, approximately 20-30 minutes	$31.32
MH and SA OP Services	90833	U6 - Doctoral Level (MD / DO)	Add-On Code; Psychotherapy, 30 minutes, when Performed with an Evaluation and Management Service	$63.83
MH and SA OP Services	90833	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Add-On Code; Psychotherapy, 30 minutes, when Performed with an Evaluation and Management Service	$54.25
MH and SA OP Services	90834	UG - Doctoral Level (Child Psychiatrist)	Individual Psychotherapy, approximately 45 minutes	$115.70
MH and SA OP Services	90834	U6 - Doctoral Level (MD / DO)	Individual Psychotherapy, approximately 45 minutes	$101.66
MH and SA OP Services	90834	AH - Doctoral Level (PhD, PsyD, EdD)	Individual Psychotherapy, approximately 45 minutes	101 CMR 329
MH and SA OP Services	90834	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Individual Psychotherapy, approximately 45 minutes	$95.46
MH and SA OP Services	90834	HO - Master's Level	Individual Psychotherapy, approximately 45 minutes	101 CMR 329
MH and SA OP Services	90834	U3 - Intern (PhD, PsyD, EdD)	Individual Psychotherapy, approximately 45 minutes	$47.98
MH and SA OP Services	90834	U4 - Intern (Master's)	Individual Psychotherapy, approximately 45 minutes	$47.26
MH and SA OP Services	90836	U6 - Doctoral Level (MD / DO)	Add-On Code; Psychotherapy, 45 minutes, when Performed with an Evaluation and Management Service	$82.90
MH and SA OP Services	90836	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Add-On Code; Psychotherapy, 45 minutes, when Performed with an Evaluation and Management Service	$82.90
MH and SA OP Services	90837	UG - Doctoral Level (Child Psychiatrist)	Psychotherapy, 60 minutes	$135.04
MH and SA OP Services	90837	U6 - Doctoral Level (MD / DO)	Psychotherapy, 60 minutes	$135.04
MH and SA OP Services	90837	AH - Doctoral Level (PhD, PsyD, EdD)	Psychotherapy, 60 minutes	101 CMR 329
MH and SA OP Services	90837	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Psychotherapy, 60 minutes	$125.69
MH and SA OP Services	90837	HO - Master's Level	Psychotherapy, 60 minutes	101 CMR 329
MH and SA OP Services	90837	U3 - Intern (PhD, PsyD, EdD)	Psychotherapy, 60 minutes	$68.87
MH and SA OP Services	90837	U4 - Intern (Master's)	Psychotherapy, 60 minutes	$60.77
MH and SA OP Services	90838	U6 - Doctoral Level (MD / DO)	Add-On Code; Psychotherapy, 60 minutes, when Performed with an Evaluation and Management Service	$106.08
MH and SA OP Services	90838	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Add-On Code; Psychotherapy, 60 minutes, when Performed with an Evaluation and Management Service	$91.42
MH and SA OP Services	90846	UG - Doctoral Level (Child Psychiatrist)	Family Psychotherapy (without patient present)	$141.42
MH and SA OP Services	90846	U6 - Doctoral Level (MD / DO)	Family Psychotherapy (without patient present)	$107.62

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
MH and SA OP Services	90846	AH - Doctoral Level (PhD, PsyD, EdD)	Family Psychotherapy (without patient present)	Effective 1/1/25 through 4/24/25: $100.47 Effective 4/25/25: 101 CMR 329
MH and SA OP Services	90846	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Family Psychotherapy (without patient present)	$97.55
MH and SA OP Services	90846	HO - Master's Level	Family Psychotherapy (without patient present)	101 CMR 329
MH and SA OP Services	90846	U3 - Intern (PhD, PsyD, EdD)	Family Psychotherapy (without patient present)	$50.23
MH and SA OP Services	90846	U4 - Intern (Master's)	Family Psychotherapy (without patient present)	$48.77
MH and SA OP Services	90847	UG - Doctoral Level (Child Psychiatrist)	Family Psychotherapy (conjoint psychotherapy) (with patient present)	$141.42
MH and SA OP Services	90847	U6 - Doctoral Level (MD / DO)	Family Psychotherapy (conjoint psychotherapy) (with patient present)	$107.62
MH and SA OP Services	90847	AH - Doctoral Level (PhD, PsyD, EdD)	Family Psychotherapy (conjoint psychotherapy) (with patient present)	101 CMR 329
MH and SA OP Services	90847	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Family Psychotherapy (conjoint psychotherapy) (with patient present)	$101.43
MH and SA OP Services	90847	HO - Master's Level	Family Psychotherapy (conjoint psychotherapy) (with patient present)	101 CMR 329
MH and SA OP Services	90847	U3 - Intern (PhD, PsyD, EdD)	Family Psychotherapy (conjoint psychotherapy) (with patient present)	$50.23
MH and SA OP Services	90847	U4 - Intern (Master's)	Family Psychotherapy (conjoint psychotherapy) (with patient present)	$48.77
MH and SA OP Services	90849	UG - Doctoral Level (Child Psychiatrist)	Multi-family group psychotherapy	$46.29
MH and SA OP Services	90849	U6 - Doctoral Level (MD / DO)	Multi-family group psychotherapy	$38.84
MH and SA OP Services	90849	AH - Doctoral Level (PhD, PsyD, EdD)	Multi-family group psychotherapy	101 CMR 329
MH and SA OP Services	90849	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Multi-family group psychotherapy	$33.00
MH and SA OP Services	90849	HO - Master's Level	Multi-family group psychotherapy	101 CMR 329
MH and SA OP Services	90849	U3 - Intern (PhD, PsyD, EdD)	Multi-family group psychotherapy	$17.96
MH and SA OP Services	90849	U4 - Intern (Master's)	Multi-family group psychotherapy	$16.50
MH and SA OP Services	90853	UG - Doctoral Level (Child Psychiatrist)	Group psychotherapy (other than of a multiple-family group)	$46.29
MH and SA OP Services	90853	U6-Doctoral Level (MD / DO)	Group psychotherapy (other than of a multiple-family group)	$38.84
MH and SA OP Services	90853	AH - Doctoral Level (PhD, PsyD, EdD)	Group psychotherapy (other than of a multiple-family group)	101 CMR 329
MH and SA OP Services	90853	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Group psychotherapy (other than of a multiple-family group)	$33.12
MH and SA OP Services	90853	HO - Master's Level	Group psychotherapy (other than of a multiple-family group)	101 CMR 329
MH and SA OP Services	90853	U3 - Intern (PhD, PsyD, EdD)	Group psychotherapy (other than of a multiple-family group)	$17.96

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
MH and SA OP Services	90853	U4 - Intern (Master's)	Group psychotherapy (other than of a multiple-family group)	$16.50
MH and SA OP Services	90882	UG - Doctoral Level (Child Psychiatrist)	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$51.11
MH and SA OP Services	90882	U6-Doctoral Level (MD / DO)	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$44.33
MH and SA OP Services	90882	AH-Doctoral Level (PhD, PsyD, EdD)	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$23.97
MH and SA OP Services	90882	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$38.36
MH and SA OP Services	90882	HO - Master's Level	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$23.63
MH and SA OP Services	90882	U3 - Intern (PhD, PsyD, EdD)	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$12.00
MH and SA OP Services	90882	U4-Intern (Master's)	Environmental intervention for medical management purposes on a psychiatric patient's behalf with agencies, employers or institutions.	$11.81
MH and SA OP Services	90887	UG-Doctoral Level (Child Psychiatrist)	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	$79.19
MH and SA OP Services	90887	U6-Doctoral Level (MD / DO)	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	$79.19
MH and SA OP Services	90887	AH-Doctoral Level (PhD, PsyD, EdD)	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	101 CMR 329
MH and SA OP Services	90887	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	$67.32
MH and SA OP Services	90887	HO - Master's Level	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	101 CMR 329
MH and SA OP Services	90887	U3 - Intern (PhD, PsyD, EdD)	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	$40.39
MH and SA OP Services	90887	U4-Intern (Master's)	Interpretation or explanation of results of psychiatric, other medical examinations and procedures, or other accumulated data to family or other responsible persons, or advising them how to assist patient	$35.64
MH and SA OP Services	96372	U6 - Doctoral Level (MD / DO)	Therapeutic, Prophylactic or Diagnostic Injection; subcutaneous or intramuscular	$31.25

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
MH and SA OP Services	96372	SA - Nurse Practitioner/Board Certified RNCS and APRN-BC	Therapeutic, Prophylactic or Diagnostic Injection; subcutaneous or intramuscular	$23.22
MH and SA OP Services	97810	*N/A*	Acupuncture, 1 or more needles; without electrical stimulation, initial 15 minutes of personal one-to-one contact	$19.84
MH and SA OP Services	97811	*N/A*	Add-On Code; Acupuncture, 1 or more needles; without electrical stimulation, each additional 15 minutes of personal one-to-one contact with re-insertion of needle(s).	$19.84
MH and SA OP Services	99202	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for New Patient, 15-29 minutes	$75.25
MH and SA OP Services	99202	U6-Doctoral Level (MD / DO)	Evaluation and Management for New Patient, 15-29 minutes	$67.91
MH and SA OP Services	99202	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for New Patient, 15-29 minutes	$60.78
MH and SA OP Services	99203	UG- Doctoral Level (Child Psychiatrist)	Evaluation and Management for New Patient, 30-44 minutes	$108.55
MH and SA OP Services	99203	U6-Doctoral Level (MD / DO)	Evaluation and Management for New Patient, 30-44 minutes	$103.65
MH and SA OP Services	99203	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for New Patient, 30-44 minutes	$88.11
MH and SA OP Services	99204	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for New Patient, 45-59 minutes	$164.00
MH and SA OP Services	99204	U6-Doctoral Level (MD / DO)	Evaluation and Management for New Patient, 45-59 minutes	$153.89
MH and SA OP Services	99204	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for New Patient, 45-59 minutes	$133.25
MH and SA OP Services	99205	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for New Patient, 60-74 minutes	$203.69
MH and SA OP Services	99205	U6-Doctoral Level (MD / DO)	Evaluation and Management for New Patient, 60-74 minutes	$203.31
MH and SA OP Services	99205	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for New Patient, 60-74 minutes	$172.81
MH and SA OP Services	99211	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for an Established Patient, 5 minutes	$22.06
MH and SA OP Services	99211	U6-Doctoral Level (MD / DO)	Evaluation and Management for an Established Patient, 5 minutes	$22.06
MH and SA OP Services	99211	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for an Established Patient, 5 minutes	$18.75
MH and SA OP Services	99212	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for an Established Patient, 10-19 minutes	$52.73
MH and SA OP Services	99212	U6-Doctoral Level (MD / DO)	Evaluation and Management for an Established Patient, 10-19 minutes	$52.73
MH and SA OP Services	99212	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for an Established Patient, 10-19 minutes	$44.82
MH and SA OP Services	99213	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for an Established Patient, 20-29 minutes	$84.11

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
MH and SA OP Services	99213	U6-Doctoral Level (MD / DO)	Evaluation and Management for an Established Patient, 20-29 minutes	$84.11
MH and SA OP Services	99213	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for an Established Patient, 20-29 minutes	$71.49
MH and SA OP Services	99214	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for an Established Patient, 30-39 minutes	$143.98
MH and SA OP Services	99214	U6-Doctoral Level (MD / DO)	Evaluation and Management for an Established Patient, 30-39 minutes	$118.51
MH and SA OP Services	99214	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for an Established Patient, 30-39 minutes	$100.73
MH and SA OP Services	99215	UG-Doctoral Level (Child Psychiatrist)	Evaluation and Management for an Established Patient, 40-54 minutes	$166.57
MH and SA OP Services	99215	U6-Doctoral Level (MD / DO)	Evaluation and Management for an Established Patient, 40-54 minutes	$166.57
MH and SA OP Services	99215	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Evaluation and Management for an Established Patient, 40-54 minutes	$141.58
MH and SA OP Services	99231	UG-Doctoral Level (Child Psychiatrist)	Subsequent Hospital Care for Eval and Management, 15 minutes	$78.07
MH and SA OP Services	99231	U6-Doctoral Level (MD / DO)	Subsequent Hospital Care for Eval and Management, 15 minutes	$59.27
MH and SA OP Services	99231	AH-Doctoral Level (PhD, PsyD, EdD)	Subsequent Hospital Care for Eval and Management, 15 minutes	$56.89
MH and SA OP Services	99231	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Subsequent Hospital Care for Eval and Management, 15 minutes	$47.47
MH and SA OP Services	99232	UG-Doctoral Level (Child Psychiatrist)	Subsequent Hospital Care for Eval and Management, 25 minutes	$117.11
MH and SA OP Services	99232	U6-Doctoral Level (MD / DO)	Subsequent Hospital Care for Eval and Management, 25 minutes	$88.19
MH and SA OP Services	99232	AH-Doctoral Level (PhD, PsyD, EdD)	Subsequent Hospital Care for Eval and Management, 25 minutes	$84.66
MH and SA OP Services	99232	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Subsequent Hospital Care for Eval and Management, 25 minutes	$70.63
MH and SA OP Services	99233	UG-Doctoral Level (Child Psychiatrist)	Subsequent Hospital Care for Eval and Management, 35 minutes	$156.16
MH and SA OP Services	99233	U6-Doctoral Level (MD / DO)	Subsequent Hospital Care for Eval and Management, 35 minutes	$117.59
MH and SA OP Services	99233	AH-Doctoral Level (PhD, PsyD, EdD)	Subsequent Hospital Care for Eval and Management, 35 minutes	$112.88
MH and SA OP Services	99233	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Subsequent Hospital Care for Eval and Management, 35 minutes	$94.18
MH and SA OP Services	99251	UG-Doctoral Level (Child Psychiatrist)	Initial Inpatient Consultation, 20 minutes	$104.74
MH and SA OP Services	99251	U6-Doctoral Level (MD / DO)	Initial Inpatient Consultation, 20 minutes	$79.50
MH and SA OP Services	99251	AH-Doctoral Level (PhD, PsyD, EdD)	Initial Inpatient Consultation, 20 minutes	$76.32
MH and SA OP Services	99251	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Initial Inpatient Consultation, 40 minutes	$63.67
MH and SA OP Services	99252	UG-Doctoral Level (Child Psychiatrist)	Initial Inpatient Consultation, 40 minutes	$157.11

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
MH and SA OP Services	99252	U6-Doctoral Level (MD / DO)	Initial Inpatient Consultation, 40 minutes	$118.32
MH and SA OP Services	99252	AH-Doctoral Level (PhD, PsyD, EdD)	Initial Inpatient Consultation, 40 minutes	$113.58
MH and SA OP Services	99252	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Initial Inpatient Consultation, 40 minutes	$94.77
MH and SA OP Services	99253	UG-Doctoral Level (Child Psychiatrist)	Initial Inpatient Consultation, 55 minutes	$209.47
MH and SA OP Services	99253	U6-Doctoral Level (MD / DO)	Initial Inpatient Consultation, 55 minutes	$157.74
MH and SA OP Services	99253	AH-Doctoral Level (PhD, PsyD, EdD)	Initial Inpatient Consultation, 55 minutes	$151.44
MH and SA OP Services	99253	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Initial Inpatient Consultation, 55 minutes	$126.35
MH and SA OP Services	99254	UG-Doctoral Level (Child Psychiatrist)	Initial Inpatient Consultation, 80 minutes	$280.95
MH and SA OP Services	99254	U6-Doctoral Level (MD / DO)	Initial Inpatient Consultation, 80 minutes	$210.98
MH and SA OP Services	99254	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Initial Inpatient Consultation, 80 minutes	$169.00
MH and SA OP Services	99255	UG-Doctoral Level (Child Psychiatrist)	Initial Inpatient Consultation - Comprehensive, 110 minutes	$370.12
MH and SA OP Services	99255	U6-Doctoral Level (MD / DO)	Initial Inpatient Consultation - Comprehensive, 110 minutes	$277.57
MH and SA OP Services	99255	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Initial Inpatient Consultation - Comprehensive, 110 minutes	$222.33
MH and SA OP Services	99281	U6-Doctoral Level (MD/DO)	Emergency Department visit for the evaluation and management of a patient, which requires 3 key components: A problem-focused history; A problem-focused examination; and Straightforward medical decision making. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are self limited or minor.	$20.14
MH and SA OP Services	99282	UG-Doctoral Level (Child Psychiatrist)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: An expanded problem-focused history; An expanded problem-focused examination; and Medical decision-making of low complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of low to moderate severity.	$35.37

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
MH and SA OP Services	99282	U6-Doctoral Level (MD/DO)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: An expanded problem focused history; An expanded problem focused examination; and Medical decision making of low complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of low to moderate severity.	$33.68
MH and SA OP Services	99282	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: An expanded problem focused history; An expanded problem focused examination; and Medical decision making of low complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of low to moderate severity.	$32.70
MH and SA OP Services	99283	UG-Doctoral Level (Child Psychiatrist)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: An expanded problem focused history; An expanded problem focused examination; and Medical decision making of moderate complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of moderate severity.	$53.52
MH and SA OP Services	99283	U6-Doctoral Level (MD/DO)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: An expanded problem focused history; An expanded problem focused examination; and Medical decision making of moderate complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of moderate severity.	$50.97

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
MH and SA OP Services	99283	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: An expanded problem focused history; An expanded problem focused examination; and Medical decision making of moderate complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of moderate severity.	$49.49
MH and SA OP Services	99284	UG-Doctoral Level (Child Psychiatrist)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: A detailed history; A detailed examination; and Medical decision making of moderate complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of high severity, and require urgent evaluation by the physician but do not pose an immediate significant threat to life or physiologic function.	$100.58
MH and SA OP Services	99284	U6-Doctoral Level (MD/DO)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: A detailed history; A detailed examination; and Medical decision making of moderate complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of high severity, and require urgent evaluation by the physician but do not pose an immediate significant threat to life or physiologic function.	$95.80
MH and SA OP Services	99284	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components: A detailed history; A detailed examination; and Medical decision making of moderate complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of high severity, and require urgent evaluation by the physician but do not pose an immediate significant threat to life or physiologic function.	$93.01

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
MH and SA OP Services	99285	UG-Doctoral Level (Child Psychiatrist)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components within the constraints imposed by the urgency of the patient's clinical condition and/or mental status: A comprehensive history; A comprehensive examination; and Medical decision making of high complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of high severity and pose an immediate significant threat to life or physiologic function.	$148.78
MH and SA OP Services	99285	U6-Doctoral Level (MD/DO)	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components within the constraints imposed by the urgency of the patient's clinical condition and/or mental status: A comprehensive history; A comprehensive examination; and Medical decision making of high complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of high severity and pose an immediate significant threat to life or physiologic function.	$141.69
MH and SA OP Services	99285	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Emergency department visit for the evaluation and management of a patient, which requires these 3 key components within the constraints imposed by the urgency of the patient's clinical condition and/or mental status: A comprehensive history; A comprehensive examination; and Medical decision making of high complexity. Counseling and/or coordination of care with other providers or agencies are provided consistent with the nature of the problem(s) and the patient's and/or family's needs. Usually, the presenting problem(s) are of high severity and pose an immediate significant threat to life or physiologic function.	$136.30
MH and SA OP Services	99402	AH-Doctoral Level (PhD, PsyD, EdD)	Preventative Medicine Counseling , 30 minutes (Psychological Testing)	$40.98
MH and SA OP Services	99402	U3 - Intern (PhD, PsyD, EdD)	Preventative Medicine Counseling, 30 minutes (Psychological Testing)	$20.50
MH and SA OP Services	99404	U6-Doctoral Level (MD / DO)	Preventative Medicine Counseling, 60 minutes (Counseling and/or Risk Factor Reduction Intervention)	$194.82
MH and SA OP Services	99404	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Preventative Medicine Counseling, 60 minutes (Counseling and/or Risk Factor Reduction Intervention)	$168.60
MH and SA OP Services	99417	U6-Doctoral Level (MD / DO)	Add-On Code; Prolonged office or other outpatient evaluation and management service, requiring total time with or without direct patient contact beyond usual service, on the date of the primary service (e.g., 99205 or 99215), each 15 minutes	$26.08

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
MH and SA OP Services	99417	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Add-On Code; Prolonged office or other outpatient evaluation and management service, requiring total time with or without direct patient contact beyond usual service, on the date of the primary service (e.g., 99205 or 99215), each 15 minutes	$26.08
Diversionary Services	H0010		Alcohol and/or drug services; sub-acute detoxification (residential addiction program inpatient) (Clinically Managed Detoxification Services)	101 CMR 346
Diversionary Services	H0011		Alcohol and/or drug services; acute detoxification (residential addiction program inpatient) (medically monitored inpatient detoxification services)	101 CMR 346
Diversionary Services	H0015	TF	Alcohol and/or drug services; intensive outpatient (treatment program that operates at least 3 hours/day and at least 3 days/week and is based on an individualized treatment plan) including assessment, counseling; crisis intervention, and activity therapies or education. (Enhanced Structured Outpatient Addiction Program - (E-SOAP))	Effective 1/1/25 through 3/27/25: 101 CMR 306 Effective 3/28/25: 101 CMR 444
Diversionary Services	H0015	N/A	Alcohol and/or drug services; intensive outpatient (treatment program that operates at least 3 hours/day and at least 3 days/week and is based on an individualized treatment plan) including assessment, counseling; crisis intervention, and activity therapies or education. (Structured Outpatient Addiction Program - SOAP)	Effective 1/1/25 through 3/27/25: $78.75 Effective 3/28/25: 101 CMR 444
Diversionary Services	H0037	*N/A*	Community Psychiatric Supportive Treatment Program, per diem (Community Based Acute Treatment - CBAT)	$847.46
Diversionary Services	H0037	U2-Autism Diagnosis	Community Psychiatric Supportive Treatment Program, per diem (CBAT Autism Speciality)	$1,380.98
Diversionary Services	H2012	+	Behavioral Health Day Treatment, per hour (Psychiatric Day Treatment)	101 CMR 307
Diversionary Services	H2012	U1	Behavioral Health Day Treatment, per hour (Psychiatric Day Treatment, preadmission evaluation visit)	101 CMR 307
Diversionary Services	H2015	HF-Substance Abuse Program	Recovery Support Navigator , per 15-minute units including when provided in an Emergency Department or in a medical or surgical inpatient setting	101 CMR 444
Diversionary Services	H2015	HF-Substance Abuse Program HD-Pregnant/Postpartum	Recovery Support Navigator , per 15-minute units, serving pregnant members or members who have been pregnant in the previous 12 months	Effective 9/1/25: $25.35
Diversionary Services	H2015	*N/A*	Comprehensive community support services, per 15 minutes (Community Support Program)	101 CMR 362

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Unique Code/Modifier Combinations

Category of Service	Procedure Code	Modifier Group	Procedure Description	Unit Cost
Diversionary Services	H2016	HH-Integrated Mental Health/Substance Abuse Program	Comprehensive community support program, per diem (Enrolled Client Day) (behavioral health service by a navigator trained to support members with justice involvement) (CSP-JI)	101 CMR 362
Diversionary Services	H2016	HK - Specialized mental health programs for high-risk populations	Comprehensive community support program, per diem, for members who are 1) experiencing Homelessness and are frequent users of acute health MassHealth services, or 2) are experiencing chronic homelessness	101 CMR 362
Diversionary Services	H2016	HE - Mental Health Program	Comprehensive community support program, per diem, for members who are At Risk of Homelessness and facing Eviction as a result of behavior related to a disability	101 CMR 362
Diversionary Services	H2016	HM-Less than bachelor degree level	Comprehensive community support program, per diem (Enrolled Client Day) (recovery support service by a recovery advocate trained in Recovery Coaching)	101 CMR 346
Diversionary Services	H2016	HM-Less than bachelor degree level; HD- Pregnant/Postpartum	Comprehensive community support program, per diem (Enrolled Client Day) (recovery support service by a recovery advocate trained in Recovery Coaching for pregnant member or members who have been pregnant in the previous 12 months)	Effective 9/1/25: $33.16
Diversionary Services	H2020	*N/A*	Therapeutic behavioral services, per diem (Dialectical Behavior Therapy)	$26.50
Diversionary Services	S9484	*N/A*	Crisis intervention mental health services, per hour (Urgent Outpatient Services)	$147.57
MH and SA OP Services	H0014	*N/A*	Alcohol and/or drug services; ambulatory detoxification (Adult or Adolescent)	$227.65
Crisis Intervention Services	S9485	*ET-Emergency Services*	Crisis intervention mental health services, per diem. (Adult Community Crisis Stabilization per day rate)	101 CMR 305
Crisis Intervention Services	S9485	*ET-Emergency Services; HA-Child/Adolescent Program*	Crisis intervention mental health services, per diem. (Youth Community Crisis Stabilization Per day rate)	101 CMR 305
Crisis Intervention Services	S9485	*HE-Mental Health Program*	Crisis intervention mental health services, per diem. (Adult Mobile Crisis Intervention provided at CBHC site. Inclusive of initial evaluation and first day crisis interventions.)	101 CMR 305
Crisis Intervention Services	S9485	*HA-Child/Adolescent Program; HE-Mental Health Program*	Crisis intervention mental health services, per diem. (Youth Mobile Crisis Intervention provided at CBHC site. Inclusive of initial evaluation and first day crisis interventions.)	101 CMR 305
Crisis Intervention Services	S9485	*U1-MCI - Mobile Non-Emergency Department*	Crisis intervention mental health services, per diem. (Adult Mobile Crisis Intervention provided at community-based sites of service outside of the CBHC site. Inclusive of initial evaluation and first day crisis interventions. Use Place of Service 15.)	101 CMR 305
Crisis Intervention Services	S9485	*HA-Child/Adolescent Program; U1-MCI - Mobile Non-Emergency Department*	Crisis intervention mental health services, per diem. (Youth Mobile Crisis Intervention provided at community-based sites of service outside of the CBHC site. Inclusive of initial evaluation and first day crisis interventions Use Place of Service code 15.)	101 CMR 305

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
Crisis Intervention Services	S9485	U1-ESP - Mobile Non-Emergency Department	Crisis intervention mental health service, per diem (Emergency Service Program Adult Mobile Crisis Intervention, Community based location Non-Emergency Department - Uninsured)	$1,024.64
Crisis Intervention Services	S9485	*HA-Child/Adolescent Program; U1-MCI - Mobile Non-Emergency Department*	Crisis intervention mental health service, per diem (Emergency Service Program Youth Mobile Crisis Intervention, Community-based location Non-Emergency Department - Uninsured)	$1,075.87
Crisis Intervention Services	S9485	HE-Mental Health Program	Crisis intervention mental health services, per diem (Emergency Service Program Mobile Crisis Intervention SiteCommunity Based - Uninsured)	$695.29
Other Outpatient	90870	*N/A*	Electroconvulsive therapy (includes necessary monitoring)	$630.95
Other Outpatient	96112	AH-Doctoral Level (PhD, PsyD, EdD)	Developmental Testing administration (including assessment of fine and/or gross motor, language, cognitive level, social, memory and/or executive functions by standardized developmental instruments when performed), by physician or other qualified health care professional, with interpretation and report; first hour (Learning Disorders)	101 CMR 329
Other Outpatient	96113	AH-Doctoral Level (PhD, PsyD, EdD)	Add-On Code; Each additional 30 minutes (List separately in addition to code for primary procedure) (Developmental/Behavioral Screening and Testing)	101 CMR 329
Other Outpatient	96116	AH-Doctoral Level (PhD, PsyD, EdD)	Neurobehavioral status exam (clinical assessment of thinking, reasoning and judgment, e.g., acquired knowledge, attention, language, memory, planning and problem solving, and visual spatial abilities), by physician o rother qualified health professional, both face-to-face time with the patient and time interpreting test results and preparing the report; first hour	101 CMR 329
Other Outpatient	96121	AH-Doctoral Level (PhD, PsyD, EdD)	Add-On Code; Each additional hour (List separately in addition to code for primary procedure)	101 CMR 329
Other Outpatient	96130	AH-Doctoral Level (PhD, PsyD, EdD)	Psychological testing evaluation services by physician or other qualified health care professional, including integrating of patient data, interpretation of standardized test results and clinical data, clinical decision making, treatment planning and report, and interactive feedback to the patient, family member(s) or caregiver(s), when performed; first hour	Effective 1/1/25 through 4/24/25: $107.49 Effective 4/25/25: 101 CMR 329
Other Outpatient	96131	AH-Doctoral Level (PhD, PsyD, EdD)	Add-On Code; Each additional hour (List separately in addition to code for primary procedure)	101 CMR 329

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
Other Outpatient	96132	AH-Doctoral Level (PhD, PsyD, EdD)	Neuropsychological testing evaluation services by physician or other qualified health care professional, including integration of patient data, interpretation of standardized test results and clinical data, clinical decision making, treatment planning and report, and interactive feedback to the patient, family member(s) or caregiver(s), when performed; first hour	Effective 1/1/25 through 4/24/25: $121.84 Effective 4/25/25: 101 CMR 329
Other Outpatient	96133	AH-Doctoral Level (PhD, PsyD, EdD)	Add-On Code; Each additional hour (List separately in addition to code for primary procedure)	101 CMR 329
Other Outpatient	96136	AH-Doctoral Level (PhD, PsyD, EdD)	Psychological or neuropsychological test administration and scoring by physician or other qualified health care professional, two or more tests, any method; first 30 minutes (Test administration and scoring by professional)	101 CMR 329
Other Outpatient	96137	Doctoral Level (PhD, PsyD, EdD)	Add-On Code; Each additional 30 minutes (List separately in addition to code for primary procedure) (Test administration and scoring by professional)	101 CMR 329
Other Outpatient	96138	*N/A*	Psychological or neuropsychological test administration and scoring by technician, two or more tests, any method; first 30 minutes	101 CMR 329
Other Outpatient	96139	*N/A*	Add-On Code; Each additional 30 minutes (List separately in addition to code for primary procedure) (Test administration and scoring by technician)	101 CMR 329
Other Outpatient	H0032	HO-Master's Level	Mental health service plan development by a nonphysician (Bridge consultation inpatient/outpatient)	$166.67
Other Outpatient	H0046	UG-Doctoral Level (Child Psychiatrist)	Mental health services, not otherwise specified (Collateral Contact)	$46.46
Other Outpatient	H0046	U6-Doctoral Level (MD/DO)	Mental health services, not otherwise specified (Collateral Contact)	$40.30
Other Outpatient	H0046	AH-Doctoral Level (PhD, PsyD, EdD)	Mental health services, not otherwise specified (Collateral Contact)	$21.79
Other Outpatient	H0046	SA-Nurse Practitioner/Board Certified RNCS and APRN-BC	Mental health services, not otherwise specified (Collateral Contact)	$34.87
Other Outpatient	H0046	HO-Master's Level	Mental health services, not otherwise specified (Collateral Contact)	$21.48
Other Outpatient	H0046	U7-Certified Addiction Counselor / Certified Alcohol & Drug Abuse Counselor	Mental health services, not otherwise specified (Collateral Contact)	$21.48
Other Outpatient	H0046	U3-Intern (PhD, PsyD, EdD)	Mental health services, not otherwise specified (Collateral Contact)	$10.91
Other Outpatient	H0046	U4-Intern (Master's)	Mental health services, not otherwise specified (Collateral Contact)	$10.74
Other Outpatient	H0046	HE-Mental Health Program	Mental health services, not otherwise specified (Certified Peer Specialist) (Enrolled client day)	101 CMR 306
Other Outpatient	H2028	*N/A*	Sexual offender treatment service, per 15 minutes (ASAP - Assessment for Safe and Appropriate Placement)	$22.79

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix L: Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule

Exhibit 1: Commonwealth of Massachusetts Behavioral Health Outpatient and Certain Other Services Minimum Fee Schedule				
Unique Code/Modifier Combinations				
Category of Service	**Procedure Code**	**Modifier Group**	**Procedure Description**	**Unit Cost**
MH and SA OP Services	H0001	U1--MAT	MAT - Alcohol and/or drug assessment (buprenorphine and naltrexone medication evaluation by physician and/or midlevel practitioner)	$146.93
MH and SA OP Services	H0004		Behavioral health counseling and therapy, per 15 minutes (individual counseling)	101 CMR 346
MH and SA OP Services	H0005		Alcohol and/or drug services; group counseling by a clinician (per 45 minutes, group counseling, one unit maximum per day)	101 CMR 346
MH and SA OP Services	H0005	HG	Alcohol and/or drug services group counseling by a clinician (per 90-minute unit) (one unit maximum per day)	101 CMR 346
MH and SA OP Services	T1006		Alcohol and/or substance abuse services; family/couple counseling (per 30 minutes, one unit maximum per day)	$48.77
MH and SA OP Services	T1006	HF	Alcohol and/or substance abuse services; family/couple counseling (per 60 minutes, one unit maximum per day)	$101.43
Diversionary Services	S9480	N/A	Intensive outpatient psychiatric services, per diem	101 CMR 306

* See Section 2.7.B.5.a for adjustment to unit cost if using CANS Tool.

Appendix O
HRSN Supplemental Services

Exhibit 1: HRSN Supplemental Services

✓ Denotes a covered service

Exhibit 1.1: HRSN Category 1 Supplemental Nutrition Services

	Coverage Types		
Service	**MassHealth Standard & CommonHealth Covered Individuals**	**MassHealth Family Assistance Covered Individuals**	**CarePlus**
Medically Tailored Food Boxes – Selection of minimally prepared grocery items that meet appropriate nutritional standards.	✓	✓	✓
Nutritionally Appropriate Food Boxes – Minimally prepared grocery items or a Community Supported Agricultural (CSA) share.	✓	✓	✓
Medically Tailored Food Prescriptions and Vouchers – Nutrition vouchers and grocery store gift cards to procure healthy food from an approved purchase list.	✓	✓	✓
Nutritionally Appropriate Food Prescriptions and Vouchers – Nutrition vouchers and grocery store gift cards to procure healthy food.	✓	✓	✓
Medically Tailored Home Delivered Meals – Prepared medically tailored meals that reflect appropriate nutritional needs based on defined medical diagnosis and standards reflecting evidence-based practice guidelines, deliver to the Covered Individual.	✓	✓	✓
Nutritionally Appropriate Home Delivered Meals – Healthy, well-balanced meals delivered to the Covered Individual.	✓	✓	✓

Exhibit 1.2: HRSN Category 2 Supplemental Nutrition Services

	Coverage Types		
Service	**MassHealth Standard & CommonHealth Covered Individuals**	**MassHealth Family Assistance Covered Individuals**	**CarePlus**
Kitchen Supplies – Provision of and assistance with obtaining cooking supplies (e.g., pots and pans, utensils, refrigerator) to meet the Covered Individual's nutritional and dietary needs.	✓	✓	✓
Nutrition Counseling – Provision of nutrition counseling for the purposes of meeting the Covered Individual's nutritional and dietary needs.	✓	✓	✓
Nutrition Education Classes and Skills Development – Provision of nutrition education classes and skills development (e.g., cooking classes as education) for the purposes of meeting the Covered Individual's nutritional and dietary needs.	✓	✓	✓

Exhibit 1.3: HRSN Supplemental Housing Services

	Coverage Types		
Service	**MassHealth Standard & CommonHealth Covered Individuals**	**MassHealth Family Assistance Covered Individuals**	**CarePlus**
Healthy Homes – Goods and/or remediation services proven to improve housing conditions related to health needs that are not the responsibility of the housing owner/landlord.	✓	✓	✓
Housing Navigation – Assistance to help a Covered Individual experiencing housing instability to access benefits, negotiate with landlords, seek out legal assistance, apply for new housing (if needed), or take other actions in order to help stabilize a Covered Individual's housing situation.	✓	✓	✓
Housing Search - Assistance to help a Covered Individual, ages 55 and over, experiencing homelessness locate, move into, and maintain housing.	✓	✓	✓
Transitional Goods – Move-in costs (e.g., security deposits, first month's rent, movers), furnishings, and other items necessary to make new housing habitable and comfortable.	✓	✓	✓

Exhibit 1.4 – Items and Services Excluded from HRSN Supplemental Services

In the course of providing HRSN Supplemental Services, the Contractor shall not provide:

- Construction costs (bricks and mortar) or capital investments;
- Room and board outside of specifically enumerated care or housing transitions;
- Research grants and expenditures not related to monitoring and evaluation;
- Costs for services in prisons, correctional facilities or services for people who are civilly committed and unable to leave an institutional setting, except those HRSN-related case management services provided as part of an approved reentry demonstration initiative;
- Services provided to individuals who are not lawfully present in the United States or are undocumented;
- Expenditures that supplant services and activities funded by other state and federal governmental entities;
- School-based programs for children that supplant Medicaid state plan programs, or that are funded under the Department of Education and/or state or the local education agency; or
- Any other projects or activities not specifically approved by CMS as qualifying for coverage as a HRSN item or service under this demonstration.

Appendix O, Exhibit 2

The Contractor shall work with each PCACO, as listed below, to provide the following HRSN Supplemental Services in accordance with **Section 2.6.D.12** and all other applicable sections of the Contract:

A. Community Care Cooperative's (CCC) HRSN Supplemental Services

HRSN Supplemental Service	CCC's Selected HRSN Supplemental Service (as indicated by "X")
HRSN Category 1 Supplemental Nutrition Services	
Medically Tailored Food Boxes	X
Nutritionally Appropriate Food Boxes	
Medically Tailored Food Prescriptions and Vouchers	X
Nutritionally Appropriate Food Prescriptions and Vouchers	
Medically Tailored Home Delivered Meals	X
Nutritionally Appropriate Home-Delivered Meals	
HRSN Category 2 Supplemental Nutrition Services	
Kitchen Supplies	X
Nutrition Counseling	X
Nutrition Education Classes and Skills Development	X
HRSN Supplemental Housing Services	
Healthy Homes	X
Housing Navigation	
Housing Search	X
Transitional Goods	X

B. Revere Health Choice's HRSN Supplemental Services

HRSN Supplemental Service	Revere Health Choice's Selected HRSN Supplemental Service (as indicated by "X")
HRSN Category 1 Supplemental Nutrition Services	
Medically Tailored Food Boxes	
Nutritionally Appropriate Food Boxes	X
Medically Tailored Food Prescriptions and Vouchers	X
Nutritionally Appropriate Food Prescriptions and Vouchers	
Medically Tailored Home Delivered Meals	
Nutritionally Appropriate Home-Delivered Meals	
HRSN Category 2 Supplemental Nutrition Services	
Kitchen Supplies	X
Nutrition Counseling	X
Nutrition Education Classes and Skills Development	X
HRSN Supplemental Housing Services	
Healthy Homes	X
Housing Navigation	X
Housing Search	X
Transitional Goods	X

APPENDIX P
Network Availability Standards

In accordance with **Section 2.9** of the Contract, the Contractor shall ensure its Provider Network meets the following availability standards in addition to all other requirements set forth in the Contract. Specifically, at least 90% of Covered Individuals in each of the Contractor's Service Areas must have access to Providers in accordance with the time and distance standards below. As set forth in **Section 2.9** in determining compliance with the time and distance standards below, the Contractor shall take into account shall consider both walking and public transportation.

A. Behavioral Health Services (as set forth in Appendix A-1)

For each Provider type, for each Service Area, the Contractor shall have at least the specified number of Providers within at least the specified time or the specified distance of Covered Individual' residences. If no time or distance is indicated, the Contractor shall have at least one Provider located anywhere in the Commonwealth.

Behavioral Health Providers

Provider Type	**Minimum Number of Providers**	**Time (min)**	**Distance (miles)**
Psychiatric inpatient adult[1]	2	60	60
Monitored inpatient Acute Treatment Services (ATS) level 3.7[2]	2	60	60
Clinical Stabilization Services (CSS) level 3.5[3]	2	60	60
Partial Hospitalization (PHP)	1	60	60
Applied Behavior Analysis (ABA)	2	30	30
In-Home Behavioral Services	2	30	30
In-Home Therapy	2	30	30
Therapeutic Mentoring Services	2	30	30
Structured Outpatient Addiction Program (SOAP)	2	60	60
BH outpatient (including psychology and psych APN)	2	30	30
Opioid Treatment Program (OTP)	2	60	60
Psychiatry	1	40	20

[1] For the Nantucket and Oak Bluffs Service Areas only, the Contractor may meet this requirement by including in its Provider Network the two closest Providers that provide Psychiatric Inpatient Adult services.
[2] For the Adams Service Area only, the Contractor may meet this requirement by including in its Provider Network the two closest Providers that provide ATS level 3.7 services.
[3] For the Adams Service Area only, the Contractor may meet this requirement by including in its Provider Network the two closest Providers that provide CSS level 3.5 services.