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'

_____   Date:

Sharon Donovan, Director
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)

Daniel Tsai   Date:
Assistant Secretary and Director of MassHealth
Massachusetts Executive Office of Health and Human Services