APPENDIX H
BUSINESS ASSOCIATE DATA MANAGEMENT AND CONFIDENTIALITY AGREEMENT

This Business Associate Data Management and Confidentiality Agreement (this "**Agreement**") is made by and between the Executive Office of Health and Human Services, Office of Medicaid ("**EOHHS**"), and the Contractor identified in **Appendix K** (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

In accordance with the Primary Care Accountable Care Organization Contract (the "Contract") , the Parties are amending the Contract and entering into this Agreement to establish certain privacy, security and related obligations of the Contractor with respect to PI (defined below), including substance use disorder data subject to 42 CFR Part 2, that the Contractor uses, maintains, discloses, receives, creates, transmits or otherwise obtains in connection with its provision of a certain service to, and/or its performance of a certain 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 Section 2.2.A.2 of the Contract that requires PI with substance use disorder data governed under 42 CFR Part 2.

"**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, each as pertaining to the use, disclosure, maintenance, privacy or security of PI.

"**Breach Notification Rule**" shall mean the Breach Notification Rule at 45 CFR Part 164, Subpart D.

"**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 or other similar Applicable Law requiring notice to consumers and/or oversight agencies in connection with an impermissible use or disclosure or breach of PI.

"**HIPAA Rules**" shall mean 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 1.3.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 under this Agreement. 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 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 1.3 <u>Data Management and Confidentiality Obligations of the Contractor</u>

A. **Compliance with Applicable Laws.** The Contractor acknowledges that for the performance of Activities where such performance uses or contains any PI with substance use disorder data subject to 42 CFR Part 2 and/or PI flagged by EOHHS as data governed under this Agreement, 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 in addition to all other applicable requirements. The Contractor shall implement appropriate safeguards for PI provided under this Agreement, including keeping PI under this Agreement separate and distinct from the member-level data or reports provided pursuant to the Data Use Agreement (DUA) referenced in Section 7 of the Contract. 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 will become 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 Section 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, 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 with respect to drug or alcohol abuse information that the Contractor receives, stores, processes, uses, creates or transmits that was obtained by EOHHS or a Part 2 Program (as such terms are used in 42 CFR PART 2), it is bound by the version of 42 CFR Part 2 effective January 1, 2020, and shall not use or disclose such information except as permitted under 42 CFR §2.33(b), including, but not limited to, the use of such information for the purposes of Treatment (as defined by 42 CFR Part 2), care coordination, or case management shall not be permitted. Notwithstanding any changes to 42 CFR Part 2, or its authorizing statue, 42 U.S. Code § 290dd–2, the Contractor shall not modify its use of such drug or alcohol abuse information, including for the use of Treatment, care coordination, or case management, unless approved by the EOHHS Privacy Office in writing, or amendment to this Agreement.
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. Notwithstanding the foregoing, the Contractor shall not be required to comply (or ensure compliance) with a Third Party Agreement under this paragraph unless it has been provided with a copy of the applicable Third Party Agreement or notified of its requirements.

C. **Tracking of PI Governed under this Agreement.** EOHHS shall track PI subject to this Agreement in Exhibit 1. The process for tracking shall be instituted for convenience of the Parties, and the Contractor acknowledges that the inclusion of PI in Exhibit 1 shall not be dispositive to determine the scope of PI subject to this Agreement. PI subject to this Agreement shall be determined by the terms and conditions in Section 1.3.A. Exhibit 1 shall be amended from time to time at the sole discretion of EOHHS and shall not be subject to the amendment process stated in Section 6.13 of the Contract. The Contractor may request a copy of Exhibit 1 at any time.

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 must be limited to approved subcontractors, agents, employees and other workforce members who require access to such PI 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 2** 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 Material Subcontractors and Agents.

   a. In the event that the Contractor intends to hire and disclose PI under this Agreement to a

Material Subcontractor (as defined in the Contract), the Contractor shall hire such Material Subcontractor pursuant to Section 6.18 of the Contract. In the event the Contractor intends to hire and disclose PI under this Agreement to an agent, the Contractor shall notify EOHHS for specific approval of agents. The Contractor shall enter into written agreements memorializing the material requisite terms of this Agreement with each Material Subcontractor and approved agent that will have access to PI under this Agreement (each, a "Subcontract"), and shall maintain such written agreements.

b. All such Subcontracts must contain all relevant provisions 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 Material Subcontractor or approved 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 require any such Material Subcontractor or approved agent to satisfy 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 Material Subcontractor's or approved 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 Material Subcontractor or approved agent.

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 and other Commonwealth security and information technology resource policies, processes and mechanisms, including the EOHHS Enterprise Information Security Standards (attached in **Exhibit 3**), and the EOTSS Enterprise Information Security Policies and Standards (found online at mass.gov) and any standards contained in any applicable Third Party Agreement (collectively, the "**Standards**"). The Contractor shall comply with any new or updated standards issued by federal, state, or other issuing agency or entity.

When accessing any System to perform the Activities, the Contractor shall comply with all applicable EOHHS, EOTSS and other Commonwealth security and information technology resource policies, processes and mechanisms regarding access to PI, and any specific security mechanisms and processes adopted by EOHHS for access to the System each to the extent made known by EOHHS in writing to the Contractor. The Contractor shall protect from inappropriate use or disclosure any password, user ID or other mechanism or code permitting access to any System containing PI or through which PI may be accessed. The Contractor shall give EOHHS prior notice of any change in personnel whenever the change requires a termination or modification of any such password, user ID or other security mechanism or code, to maintain the integrity of the System.

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.

Upon reasonable advance written notice, the Contractor agrees to allow representatives of EOHHS or, with respect to Third Party Data, other data owners, access to the Contractor's premises where PI is stored 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 made known by EOHHS in writing to the Contractor.

2. 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.

3. Written Information Security Program. The Contractor shall ensure that it maintains a written information security Program (WISP) incompliance with the terms of this Agreement and the requirements set forth in, M.G.L. c. 93H, to the extent that the PI subject to this Agreement meets the definition of "Personal Information", as such term is defined by such statute.

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; c) take such other action(s) as may be required in connection with the Event to comply with any Applicable Law.

Upon becoming aware of an Event, the Contractor shall also perform a root cause analysis, prepare a corrective action plan, and, in accordance with terms and deadlines of subsection 2 below, shall deliver a resolution report to EOHHS including root cause, and actions taken to resolve the Event and prevent its recurrence. If an Event is the result of a data security vulnerability, such as hacking, ransomware, or other data security related instance, the Contract shall provide a written forensics report to EOHHS that shall, at a minimum, describe the attack, security vulnerabilities, and any other information EOHHS deems necessary to determine compliance with this Agreement. Such report shall not be withheld by the Contractor.

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 1.3G,** 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 to the extent known:

   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 in connection with the PI.

      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, if appropriate.

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 or other Applicable Law as a result of the Event, the Contractor shall, at EOHHS' request, assist EOHHS in drafting such notices for EOHHS' review and approval, and shall take such other action(s) as EOHHS may reasonably request in connection with EOHHS' compliance with the Breach Notification Rule, M.G.L. c. 93H or other Applicable Law, but in no event shall the Contractor have the authority to give any such notifications on EOHHS' behalf unless EOHHS authorizes and directs the Contractor to do so in writing. Additionally, at EOHHS' direction, if Contractor is defined as a "Person" under M.G.L. c. 93H, §1, Contractor shall provide credit monitoring services to affected Individuals to the extent required under M.G.L. c. 93H, §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 PI 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. For the avoidance of doubt, this provision shall apply in addition to any generally applicable indemnification provision applicable to the Contractor in connection with the Activities, including such terms in the Commonwealth Terms and Conditions.

H. **Response to Legal Process.** To the extent legally permissible, 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). To the extent legally permissible, 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 in accordance with 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 that is provided pursuant to the DUA referenced in **Section 7** of the Contract, the Contractor shall notify EOHHS' Privacy Officer within two (2) business days of the Individual's request 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 the Contractor or 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 in accordance with Applicable Law. For any third party request for PI provided pursuant to the DUA referenced in **Section 7** of the Contract, within three business days of receipt of such consent, authorization, or other written document, notify EOHHS and shall cooperate with EOHHS in confirming the validity and sufficiency of such document before releasing any PI to the third party.

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 obtained under this Agreement, and the security and integrity of Systems containing PI 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. **Compliance Officer.** The Contractor designates as its Compliance Officer, who shall be responsible for overseeing the Contractor's compliance with this Agreement. Such designations may be changed during the period of this Agreement only by written notice.

M. **Destruction of PI during Contract Term**. The Contractor shall retain PI during the course of the Contract in accordance with the terms of this Agreement 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, 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 made known to the Contractor. Within five (5) days of destroying PI 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 1.4 Permitted Uses and Disclosures of PI by the Contractor

Except as otherwise limited in this Agreement, including in this **Section 1.4**, 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: (a) violate the Privacy Rule or other Applicable Law if done by EOHHS; (b) violate the EOHHS' Minimum Necessary policies and procedures that are made known to the Contractor or that EOHHS advises the Contractor in writing; or (c) 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 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. 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 1.5 Data Management and Confidentiality Obligations of EOHHS

A. **Changes in Notice of Privacy Practices.** EOHHS shall 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 and shall provide the Contractor with a new copy of the Notice of Privacy Practices reflecting such change.

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 1.6 Effect of Termination

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 the Contractor shall not retain any copies of such PI in any form. In no event shall the Contractor destroy any PI without first obtaining EOHHS' approval. In the event destruction is permitted, the Contractor shall destroy PI 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 and made known to the Contractor. This provision shall apply to all PI in the possession of the Contractor's subcontractors, and the Contractor shall require that all such PI 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 PI in any form, in accord with EOHHS' instructions. The Contractor shall, within three (3) business days of the return or destruction of PI, certify to EOHHS in writing that all PI has been returned or destroyed in accordance with this **Section 1.6** and neither the Contractor nor any of its subcontractors or agents retains any PI.

B. If the Contractor determines that returning or destroying PI 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 set forth in this Agreement to all such PI and shall limit further uses and disclosures of such PI 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.

Exhibit 1 – PI Tracker

Report	Information Contained in Report (Including Time Period Covered)	Report Frequency
1. SUD-related raw claims extract	The SUD-related raw claims extract includes information for members currently or formerly enrolled in the Contractor, as described below: • Current members are enrolled in the Contractor on the date the data is pulled from MassHealth's Data Warehouse or other MassHealth data source to inform the report. • Former members were enrolled in the Contractor at some point during the 24 months prior to the day the data is pulled from MassHealth's Data Warehouse or other MassHealth data source to inform the report. Member-level information is provided including SUD-related medical claims, SUD-related pharmacy claims, and SUD-related MBHP encounter data. Data fields show member identifying information (e.g. Medicaid ID, date of birth); member plan and provider affiliations including provider identification and tax identification numbers; claim identifiers, type, and source; dates of service; admission and discharge information; patient status; bill information; price information including billed, paid, and allowed amounts; diagnoses, accident diagnoses, and present on admission indicators; procedure and revenue codes; DRGs; information on billing and servicing providers including provider identification numbers and tax identification numbers; claim status; quantity; prescription information including therapeutic class, dispense as written indicator, dosage, days' supply, refill quantity NDC code, GCN, brand versus generic indicator, and route of administration; and prescriber information. Information is included for the 24 months prior to the day the data is pulled from MassHealth's Data Warehouse or other MassHealth data source to inform the report. For members currently enrolled in the Contractor, information will be included for any time span the member was enrolled in MassHealth over the 24-month period. For members formerly enrolled in the Contractor at the time the data is pulled to inform the report, member information is included only for spans when the member was enrolled in MassHealth and enrolled in the Contractor.	Monthly

Exhibit 2

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:_____

Exhibit 3 - EOHHS ENTERPRISE INFORMATION SECURITY STANDARDS