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.

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

[1] EOTSS, Enterprise Information Security Policies and Standards, https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards (last visited July 1, 2021).

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 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 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