

## BUSINESS ASSOCIATE ADDENDUM

THIS BUSINESS ASSOCIATE ADDENDUM (“**BAA**”) supplements and is made part of a Membersy Direct Plan Administration Agreement (hereinafter, the “**Agreement**”) by and between Membersy (hereinafter, the “**Business Associate**”) and Client (hereinafter, the “**Covered Entity**”) to be effective upon execution of the Agreement. Business Associate and Covered Entity are sometimes singularly referred to as “**Party**” and collectively as “**Parties**”. All capitalized terms used but not defined herein shall have the meanings assigned to such terms in the Agreement.

WHEREAS, Business Associate and Covered Entity anticipate that the Agreement may require Business Associate to use, disclose, access, create, maintain, transmit and/or receive Protected Health Information (as defined herein) on behalf of Covered Entity; and

WHEREAS, the Parties seek to comply with the standards for privacy and security of Protected Health Information set forth in the Health Insurance Portability and Accountability Act of 1996, Health Information for Economic and Clinical Health Act, and the rules and regulations promulgated thereunder (including the HIPAA Omnibus regulations promulgated on January 25, 2013), all as the same may be amended from time to time (collectively, “**HIPAA**”), as well as other applicable state and federal laws and regulations protecting Protected Health Information.

NOW THEREFORE, in consideration of the mutual covenants contained herein and intending to be legally bound, the Parties agree as follows:

### A. DEFINITIONS.

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the HIPAA Rules. The following required definitions are as set forth in 45 C.F.R. Parts 160 and 164 (the “**Privacy Rule**”):

1. “**Business Associate**” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103.
2. “**Covered Entity**” shall generally have the same meaning as the term “covered entity” at 45 C.F.R. 160.103.
3. “**Designated Record Set**” means: (1) A group of records maintained by or for a Covered Entity that is: (i) The medical records and billing records about Individuals maintained by or for a covered Health Care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. For purposes of this paragraph, the term “record” means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.
4. “**Disclosure**” means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
5. “**Health Care**” means care, services, or supplies related to the health of an Individual. Health Care includes, but is not limited to, the following: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
6. “**Health Information**” means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a Health Care provider, health plan, public health authority, employer, life insurer, school or university, or Health Care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future payment for the provision of Health Care to an Individual.
7. “**HIPAA Rules**” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.
8. “**Individual**” means the person who is the subject of Protected Health Information.

9. **“Individually Identifiable Health Information”** is information that is a subset of Health Information, including demographic information collected from an Individual, and: (1) is created or received by a Health Care provider, health plan, employer, or Health Care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future payment for the provision of Health Care to an Individual; and (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.
10. **“Protected Health Information”** or **“PHI”** means Individually Identifiable Health Information that is: (i) transmitted by electronic media; (ii) maintained in any medium of electronic media; or (iii) transmitted or maintained in any other form or medium. PHI shall specifically include electronic protected health information, or EPHI. PHI excludes Individually Identifiable Health Information: (i) in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232 (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv), (iii) in employment records held by a covered entity in its role as employer and (iv) regarding a person who has been deceased for more than 50 years.
11. **“Use”** means with respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

**B. DUTIES AND RESPONSIBILITIES OF BUSINESS ASSOCIATE.**

1. Business Associate shall use, disclose, access, create, maintain, transmit and/or receive PHI on behalf of Covered Entity only as permitted or required by applicable law, as required to perform the services under the Agreement or as permitted or required by the terms of this BAA.
2. Business Associate shall ensure that all disclosures of PHI by Business Associate comply with the principle of **“minimum necessary use and disclosure,”** (i.e., in accordance with 45 C.F.R. §164.502(b), only the minimum PHI that is necessary to accomplish the intended purpose may be disclosed).
3. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except as follows:
  - a. Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
  - b. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
  - c. Business Associate may provide data aggregation services relating to the Health Care operations of Covered Entity.
4. Business Associate shall use appropriate safeguards and shall comply with Subpart C of 45 C.F.R. Part 164 with respect to EPHI, to prevent use or disclosure of PHI other than as provided for by this BAA. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA.
5. Business Associate shall report in writing to Covered Entity without unreasonable delay, and in no event more than thirty (30) days following discovery, any use or disclosure of PHI not provided for by this BAA of which it becomes aware, including breaches of unsecured PHI as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware. Covered Entity shall be responsible for performing all required notifications with respect to any potential breach reported hereunder.
6. If Business Associate uses or contracts with any agent, including a subcontractor, that uses, discloses, accesses, creates, receives, maintains or transmits PHI on behalf of the Business Associate, Business Associate shall require any such agent to agree in writing to the same restrictions and conditions that apply to Business Associate under this BAA.

7. To the extent that Business Associate possesses or maintains PHI in a Designated Record Set, Business Associate agrees to:
  - a. Provide Covered Entity with access to such PHI within three (3) business days of request from the Covered Entity;
  - b. Make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to in accordance with HIPAA Rules within three (3) business days of any such request; and
  - c. Notify Covered Entity within three (3) business days if Business Associate receives a request from an Individual to access or amend the Individual's PHI and cooperate with Covered Entity to permit Covered Entity to respond to such Individual.
8. Business Associate will report to Covered Entity, within thirty (30) days of a request by Covered Entity, sufficient information for Covered Entity to comply with the accounting for disclosures requirements of 45 C.F.R. § 164.528.
9. To the extent that Business Associate agrees to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
10. Business Associate shall make its internal practices, books, and records directly relating to the use and disclosure of PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the United States Department of Health or Human Services or his or her designee ("**Secretary**"), for purposes of determining compliance with the HIPAA Rules.
11. Business Associate may disclose the PHI received by Business Associate if either:
  - a. The disclosure is required by law; or
  - b. Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

## **C. DUTIES AND RESPONSIBILITIES OF COVERED ENTITY.**

1. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
2. Covered Entity shall be responsible for obtaining valid authorization(s) from any and all individuals as required for the use and disclosure of PHI for all purposes of the Agreement and this BAA.
3. Covered Entity shall notify Business Associate of any changes to, or revocation of, the authorization of an individual regarding the use or disclosure of PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
4. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
5. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity, except as set forth in Section B.3 above.

## **D. GENERAL PROVISIONS**

1. Indemnification. Each Party agrees to indemnify, defend and hold harmless the other Party and its officers, directors, employees and agents against any loss, claim, damage or liability if and to the extent proximately caused by the indemnifying Party's (i) violation of a material term of this BAA, (ii) violation of HIPAA, or (iii) gross negligence or willful misconduct.
2. Regulatory References. A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.
3. Amendment. The Parties agree to take such action as may be necessary to amend this BAA to comply with the requirements of the HIPAA Rules and any other applicable law.
4. Interpretation. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity and the Business Associate to comply with the HIPAA Rules.

5. No Waiver. The failure of any Party at any time to require performance of any provision or to resort to any remedy provided under this BAA shall in no way affect the right of that Party to require performance or to resort to a remedy at any time thereafter, nor shall the waiver by any Party of a breach be deemed to be a waiver of any subsequent breach. A waiver shall not be effective unless it is in writing and signed by the Party against whom the waiver is being enforced.
6. Notices. All notices, demands, and all other communications required or permitted to be given or made under this BAA shall be given or made in the same manner as set forth in the Agreement.

**E. TERM/TERMINATION.**

1. Term and Termination. The term of this BAA shall become effective upon execution of the Agreement and shall continue thereafter until the Agreement expires or is terminated for any reason, whereupon this BAA shall terminate automatically.
2. Termination for Cause. A breach or violation of this BAA by Business Associate shall constitute a material breach of the Agreement and shall provide grounds for termination of the Agreement as follows:
  - a. If Covered Entity knows or reasonably believes that an activity or practice of Business Associate constitutes a breach or violation of the duties and responsibilities of Business Associate under this BAA, Covered Entity shall provide written notice to Business Associate of such breach or violation. If Business Associate is unable to cure such breach or end such violation within thirty (30) days of such notice, Covered Entity may terminate the Agreement by providing written notice of termination to Business Associate.
3. Obligations of Business Associate Upon Termination. Upon termination of this BAA for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:
  - a. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
  - b. Return to Covered Entity or, if agreed to by Covered Entity, destroy the remaining PHI that the Business Associate still maintains in any form; however, if such return or destruction is not feasible, then Business Associate shall extend the protections of the BAA to such PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible;
  - c. With respect to electronic PHI, continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 to prevent use or disclosure of the PHI, other than as provided for in this section, for as long as Business Associate retains the PHI;
  - d. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions which applied prior to termination; and
  - e. Return to Covered Entity or, if agreed to by Covered Entity, destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.
4. Survival. The obligations of Business Associate set forth in Section E.3 above shall survive the termination of this BAA.