

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is entered into on _____ (Effective Date) by and between _____ (The Covered Entity) and _____ (Business Associate) in conformance with the Privacy Rule requirements of the Health Insurance Portability and Accountability Act of 1996 and its regulations (HIPAA).

RECITALS

Whereas, the Covered Entity has engaged the services of the Business Associate for or on behalf of the Covered Entity;

Whereas, the Covered Entity may wish to disclose individually identifiable health information to the Business Associate in the performance of services for or on behalf of the Covered Entity;

Whereas, such information may Protected Health Information (PHI) as defined by the Privacy Rules promulgated in accordance with the Administrative Simplification provisions of HIPAA;

Whereas, the Parties agree to establish safeguards for the protection of such information;

Now, Therefore, the parties hereby agree as follows:

SECTION I - DEFINITIONS

- 1.1 “Breach” shall mean the acquisition, access, use, or disclosure of protected health information in a manner not permitted under this part which compromises the security or privacy of the protected health information.
 - a. For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.
 - b. A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information. (45 CFR 164.402).
- 1.2 “Business Associate” shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR 160.103.
- 1.3 “Covered Entity” shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR 160.103.
- 1.4 “Data Aggregation” shall have the meaning given to such term under the Privacy Rule, including but not limited to, 45 CFR 164.501.
- 1.5 “Designated Record Set” shall have the meaning given to such term under the Privacy Rule, including, but not limited to 45 CFR 164.501.

- 1.6 “Effective Date” shall be the Effective Date of this Agreement.
- 1.7 “Health Care Operations” shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR 164.501.
- 1.8 “Individually Identifiable Health Information” shall have the meaning given to such term under the Privacy Rule, including, but not limited to 45 CFR 160.103.
- 1.9 “Privacy Rule” shall mean the HIPAA Regulation that is codified at 45 CFR 160 and 164.
- 1.10 “Protected Health Information” or “PHI” means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR 164.501. (45 CFR 160.103 and 164.501).
- 1.11 “Protected Information” shall mean PHI provided by the Covered Entity to Business Associate or created or received by Business Associate on Covered Entity’s behalf.
- 1.12 “Security Rule” shall mean the Security Regulations codified at 45 CFR 164.308.
- 1.13 “Unsecured Protected health Information” shall mean protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. (45 CFR 164.402).

SECTION II - OBLIGATIONS AND ACTIVITIES OF THE BUSINESS ASSOCIATE

The Business Associate agrees to the following:

- 2.1 Not to use or further disclose PHI other than as permitted or required by this Business Associate Agreement or as Required by Law (as defined in the Privacy Standards);
- 2.2 To use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Business Associate Agreement;
- 2.3 To mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of this Business Associate Agreement;
- 2.4 To report to the Covered Entity any use or disclosure of PHI not provided for by this Business Associate Agreement of which it becomes aware;
- 2.5 To ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by the Business Associate on behalf of the Covered Entity agrees to the same restrictions and conditions that apply through this Business Associate Agreement to the Business Associate with respect to such PHI;

- 2.6 To provide access, at the request of the Covered Entity, and in the time and manner designated by the Covered Entity, to PHI in a Designated Record Set (as defined in the Privacy Standards), to the Covered Entity or, as directed by the Covered Entity, to the person who is the subject of the PHI (as defined in the Privacy Standards, the “Individual”) to meet the requirements under 45 CFR 164.524; provided, however, that this Section 2.6 is applicable only to the extent the Designated Record Set is maintained by the Business Associate for the Covered Entity;
- 2.7 To make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of the Covered Entity or an Individual, and in the time and manner designated by the Covered Entity; provided, however, that this Section 2.7 is applicable only to the extent the Designated Record Set is maintained by the Business Associate for the Covered Entity;
- 2.8 To make internal practices, books and records, including policies and procedures on PHI, relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary of the U.S. Department of Health and Human Services, or his designee (collectively, the “Secretary”), in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary’s determining the Covered Entity’s compliance with the Privacy Standards;
- 2.9 To document such disclosures of PHI and information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosure of PHI in accordance with 45 CFR 164.528; and,
- 2.10 To provide to the Covered Entity or an Individual, in a time and manner designated by the Covered Entity, information collected in accordance with Section 2.9 of this Business Associate Agreement, to permit the Covered Entity to respond to a request by an accounting of disclosures of PHI in accordance with 45 CFR 164.528.
- 2.11 That if it creates, receives, maintains, or transmits any electronic PHI (other than enrollment/disenrollment information and Summary Health Information, which are not subject to these restrictions) on behalf of the covered entity, it will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information, and it will ensure that any agents (including subcontractors) to whom it provides such electronic PHI agrees to implement reasonable and appropriate security measures to protect the information. The Business Associate will report to the Plan any security incident of which it becomes aware.
- 2.12 To ensure that the provisions of this Section are supported by reasonable and appropriate security measures to the extent that the designees have access to electronic PHI.
- 2.13 To provide the Covered Entity with notice of a breach of Unsecured Protected Health Information pursuant to the requirements of 45 CFR 164.410.

SECTION III - THE PARTIES AGREE TO THE FOLLOWING PERMITTED USES AND DISCLOSURES BY THE BUSINESS ASSOCIATE:

- 3.1 Except as otherwise limited in this Business Associate Agreement, the Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, the Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Standards if done by the Covered Entity; and,
- 3.2 Except as otherwise limited in this Business Associate Agreement, the Business Associate may:
- a. **Use for management and administration.** Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate; and,
 - b. **Disclose for management and administration.** Disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required by Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

SECTION IV - NOTICE OF PRIVACY PRACTICES

- 4.1 The Covered Entity shall (a) provide the Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice; (b) provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures; (c) notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restrictions may affect the Business Associate's use or disclosure of PHI; and (d) not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Standards if done by the Covered Entity, except as set forth in Section 3.2 above.
- 4.2 With respect to any privacy breach, the Covered Entity shall notify each individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, used, or disclosed as a result of such breach, except when law enforcement requires a delay pursuant to 45 CFR 164.412:
- a. Without unreasonable delay and in no case later than 60 days after discovery of a breach.
 - b. By notice in plain language including and to the extent possible:
 - 1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - 2) A description of the types of Unsecured Protected Health Information that were involved in the breach (such as whether full name, social security number, date of

- birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- 3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - 4) A brief description of what the Covered Entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
 - 5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.
- c. Use a method of notification that meets the requirements of 45 CFR 164.404(d).
 - d. Provide notice to the media when required under 45 CFR 164.406 and to the Secretary pursuant to 45 CFR 164.408.

SECTION V - TERM AND TERMINATION

- 5.1 **Term.** The term of this Business Associate Agreement shall be effective as of the date set forth above in the first paragraph and shall terminate when all of the PHI provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- 5.2 **Termination for Cause.** Upon the Covered Entity's knowledge of a material breach of this Business Associate Agreement by the Business Associate, the Covered Entity shall provide an opportunity for the Business Associate to cure the breach or end the violation. The Covered Entity shall terminate this Business Associate Agreement and the Agreement if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity, or immediately terminate this Business Associate Agreement and cure is not possible. If neither termination nor cure is feasible, the Cover Entity shall report the breach or violation to the Secretary.
- 5.3 **Effect of Termination.**
- a. **Return or Destruction of PHI.** Except as provided in Section 5.3(b), upon termination of this Business Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of PHI.
 - b. **Return or Destruction of PHI Infeasible.** In the event that the Business Associate determines that returning or destroying PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of the PHI is infeasible, the

Business Associate shall extend the protections of this Business Associate Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

SECTION VI - GENERAL PROVISIONS

- 6.1 **Regulatory references.** A reference in this Agreement to the Privacy Rule or a section in the Privacy Rule means that Rule or Section as amended from time to time.
- 6.2 **Compliance with law.** In connection with its performance under this Agreement, Business Associate shall comply with all applicable laws, including but not limited to laws protecting the privacy personal information about individuals.
- 6.3 **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996.
- 6.4 **Indemnification by Covered Entity.** Covered Entity agrees to indemnify, defend and hold harmless the Business Associate and its employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "Indemnified Party," against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with Covered Entity's breach of Section 4.1 of this Business Associate Agreement. Accordingly, on demand, Covered Entity shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results for Covered Entity's breach hereunder. Covered Entity's obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement for any reason.
- 6.5 **Indemnification by Business Associate.** Business Associate agrees to indemnify, defend and hold harmless the Covered Entity and its employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "Indemnified Party," against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with Business Associate's breach of Section 2 of this Business Associate Agreement. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results for Business Associate's breach hereunder. The obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement for any reason.
- 6.6 **Survival.** The respective rights and obligations of Business Associate under Section Two of this Agreement shall survive the termination of this Agreement.

6.7 **Interpretation.** Any ambiguity in this Section (Obligations and Activities of Business Associate) shall be resolved to permit Covered Entity to comply with the Privacy Rule.

In Witness Whereof, the Parties hereto have duly executed this Agreement as of the Effective Date as defined hereabove.

Covered Entity

Business Associate

By: _____

By: _____

Title: _____

Title: _____

Date: _____

Date: _____