

BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement (the “Agreement”) is made by and between _____ (“Covered Entity”), and _____ (“Business Associate”) (each a “Party” and collectively the “Parties”) on _____ (“Effective Date”).

1. BACKGROUND

Business Associate performs functions, activities or services for, or on behalf of Covered Entity and Business Associate receives, has access to or creates Protected Health Information (PHI), including Electronic Protected Health Information (ePHI), in order to perform such functions, activities or services. The purpose of this Agreement is to set forth the terms and conditions of disclosure of PHI by Covered Entity to Business Associate and to ensure the confidentiality, integrity and availability of ePHI that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity. It is the intent of Covered Entity and Business Associate that this Agreement will meet the requirements of the Privacy Rule and the Security Rule.

2. DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy Rule and Security Rule. 45 CFR Parts 160 and 164. Following are some of the key terms of this Agreement.

- 2.1 *Business Associate.* “Business Associate” is an individual or organization that creates, receives, maintains, or transmits protected health information on behalf of a covered entity, it shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement shall mean _____ ;
- 2.2 *Covered Entity.* “Covered Entity” is a health care provider who electronically transmits health information in connection with certain transactions for which HHS has established standards under the HIPAA Transactions Rule, it shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____ ;
- 2.3 *Subcontractor.* “Subcontractor” is a person (as defined in 45 CFR 160.103) who a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate, it shall generally have the same meaning as the term “subcontractor” at 45 CFR 160.103.

- 2.4 *HIPAA Rules.* “HIPAA Rules” shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160 and Part 164;
- 2.5 *Protected Health Information.* “Protected health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, but shall be limited to the information created or received by Business Associate from or on behalf of Covered Entity;
- 2.6 *Electronic Protected Health Information.* “Electronic Protected Health Information” or “ePHI” shall have the same meaning as the term “electronic protected health information” in 45 CFR § 160.103, but shall be limited to the EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

Business Associate Agrees to:

- 3.1 *Use and Disclosure.* Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
- 3.2 *Safeguards.* Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
- 3.3 *Reports of Non-Permitted Use or Disclosure.* Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;
- 3.4 *Reports of Security Incidents.* Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;
- 3.5 *Subcontractors.* In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and

requirements that apply to the business associate with respect to such information.

3.6 *Designated Record Set.*

- (a) Make available protected health information in a designated record set to the Covered Entity as necessary to satisfy covered entity's obligations under 45 CFR 164.524;
- (b) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

3.7 *Accounting of Disclosures.* Maintain and make available the information required to provide an accounting of disclosures to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

3.8 *Internal Practices.* Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules;

3.9 *Privacy of Individually Identifiable Health Information (Subpart E).* To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164.500-164.534, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s);

3.10 *Business Associates' Obligations Related to Breach of Unsecured PHI.*

- (a) For purposes of this section, "Breach" and "Unsecured PHI" shall have the same meaning as "breach" and "unsecured protected health information," respectively, as such terms are defined by 45 C.F.R. 164.402;
- (b) Following the discovery of a potential Breach of Unsecured PHI, Business Associate shall notify Covered Entity of the Breach within 10 days from the date of discovery. Such notification shall be made without unreasonable delay after discovering the Breach, but no later than sixty (60) calendar days after the discovery;
- (c) Business Associate's notice shall include, to the extent possible, the identification of each Individual who's Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during or as a result of the Breach. Business Associate shall also provide Covered Entity with at least the following information: a description of the Breach, including the date

of Breach and the date of discovery of the Breach, if known; a description of the types of Unsecured PHI involved in the Breach; any steps Individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what Business Associate is going to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and any other information requested by Covered Entity related to the Breach. Business Associate shall promptly supplement such notice with additional information as it becomes available;

- (d) Business Associate will secure all ePHI, as appropriate, so as to render it unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance issues pursuant to the requirements of the Omnibus Rule or notify Covered Entity of any Breach relating to Unsecured PHI, which notice shall be in compliance with the requirements of the Omnibus Rule and shall be given to Covered Entity as defined in 3.13 (b) above.

4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

- 4.1 Business Associate may only use or disclose protected health information as necessary to perform the services set forth in Service Agreement;
- 4.2 Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c);
- 4.3 Business Associate may use or disclose protected health information as required by law;
- 4.4 Business Associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures;
- 4.5 Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity, except for the specific uses and disclosures set forth below:
 - (a) Business Associate may use protected health information 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 protected health information 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 the covered entity.

5. PROVISIONS FOR COVERED ENTITY TO INFORM BUSINESS ASSOCIATE OF PRIVATE PRACTICES AND RESTRICTIONS

5.1 *Privacy Practices.* 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 protected health information;

5.2 *Notice of Changes and Restrictions.* Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information;

Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information 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 protected health information;

5.3 *Permissible Requests by Covered Entity.* Covered entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity, except if the Business Associate will use or disclose protected health information for data aggregation, management and administration, and legal responsibilities of the Business Associate.

6. TERM AND TERMINATION

6.1 *Term.* This Agreement shall be effective as of the date duly executed, and shall remain in effect for the duration of the relationship or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this section, whichever is sooner.

6.2 *Termination.*

(a) Termination resulting from the End of Relationship, Functions or Services.

This Agreement shall terminate in the event that the underlying relationship, functions, or services that gives rise to the necessity of a Business Associate Agreement terminates for any reason;

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity;

(c) Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, Business Associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions which applied prior to termination; and
5. Return to covered entity the protected health information 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.

6.3 *Return or Destruction of PHI.*

(a) Except as provided in paragraph (b) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI;

(b) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall extend the protections of this 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 Business Associate and/or subcontractors maintain such PHI.

6.4 *Survival.* The respective rights and obligations of Business Associate under this section of this Agreement shall survive the termination of this Agreement.

Covered Entity:

Business Associate:

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed and made effective as of the Effective Date specified in Section 6.1.

Signature: _____

Signature: _____

Print: _____

Print: _____

Title: _____

Title: _____

Date: _____

Date: _____