

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made as of the _____ day of _____, 20____, by and between _____, a _____ corporation organized under the laws of _____, and _____.

In consideration of the mutual covenants contained in this Agreement and intending to be legally bound, the parties agree as follows:

Section 1. Definitions

- (a) Business Associate. "Business Associate" shall mean _____.
- (b) Covered Entity. "Covered Entity" shall mean _____.
- (c) Breach. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner that: (i) is not permitted by the HIPAA Privacy Regulations; (ii) poses a significant risk of financial, reputational, or other harm to the individual; and (iii) is not excluded from the definition of "Breach" found at 45 C.F.R. §164.402. In the event of any inconsistency between the definition of "Breach" in this Agreement and the definition in the Privacy Regulations, the definition in the Privacy Regulations will control.
- (d) HITECH Act. "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act, Pub. L. No. 111-5.

- (e) Privacy Regulations. "Privacy Regulations" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.
- (f) Security Regulations. "Security Regulations" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C.
- (g) Secretary. "Secretary" shall mean the Secretary of the federal Department of Health and Human Services.
- (h) Unsecured Protected Health Information. "Unsecured Protected Health Information" shall mean Protected Health Information in any form, including electronic, paper or verbal, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary pursuant to the HITECH Act, as such guidance may be updated by the Secretary from time to time.

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R. §§160.103, 164.304 and 164.501.

Section 2. Obligations and Activities of Business Associate

Business Associate agrees to:

- (a) not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law;
- (b) use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement;

- (c) mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement;
- (d) immediately report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware; with respect to Breaches of Unsecured Protected Health Information, such report shall include at least the following information:
 - (1) the identity of each individual whose information was accessed, acquired or disclosed during the breach;
 - (2) a brief description of what happened;
 - (3) the date of discovery of the breach;
 - (4) the nature of the Unsecured Protected Health Information that was involved (e.g., social security numbers, date of birth, etc.);
 - (5) any steps individuals should take to protect themselves from potential harm resulting from the breach; and
 - (6) a brief description of what the Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches;
- (e) ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by, Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information;
- (f) provide access to Protected Health Information in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. §164.524;

- (g) make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity;
- (h) make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy Regulations;
- (i) document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity or Business Associate to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528;
- (j) provide to Covered Entity or an Individual information collected in accordance with Section 2(i) of this Agreement, to satisfy the requirements for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528 or Section 13405(c)(3) of the HITECH Act;
- (k) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, and, effective February 17, 2010, to comply with the provisions of the Security Rule identified in Section 3(a)(1)(B) of this Agreement;
- (l) ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect it; and

- (m) report to Covered Entity any material attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Section 3. Permitted Uses and Disclosures by Business Associate

(a) Statutory Duties

- (1) Business Associate acknowledges that it has a statutory duty under the HITECH Act to, among other duties:
 - (A) effective February 17, 2010, use and disclose Protected Health Information only in compliance with 45 C.F.R. § 164.504(e) (the provisions of which have been incorporated into this Agreement); and
 - (B) effective February 17, 2010, comply with 45 C.F.R. §§ 164.308 ("Security Standards: General Rules"), 164.310 ("Administrative Safeguards"), 164.312 ("Technical Safeguards"), and 164.316 ("Policies and Procedures and Documentation Requirements"). In complying with 45 C.F.R. § 164.312 ("Technical Safeguards"), Business Associate shall consider guidance issued by the Secretary pursuant to Section 13401(c) of the HITECH Act and, if a decision is made to not follow such guidance, document the rationale for that decision.
- (2) Business Associate acknowledges that its failure to comply with these or any other statutory duties could result in civil and/or criminal penalties under 42 U.S.C. §§1320d-5 and 1320d-6.

(b) General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity pursuant to the underlying service agreement between the parties, provided that such use or disclosure would not violate the Privacy Regulations if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

(c) Specific Use and Disclosure Provisions

- (1) Except as otherwise limited in this Agreement, 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.
- (2) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- (3) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. §164.504(e)(2)(i)(B).
- (4) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. §164.502(j)(1).

- (5) As of the effective date of Section 13405(d) of the HITECH Act, Business Associate may not receive direct or indirect remuneration in exchange for Protected Health Information unless permitted by the Act or regulations issued by the Secretary.

Section 4. Obligations of Covered Entity

Covered Entity shall:

- (a) notify Business Associate of any limitation(s) in its Notice of Privacy Practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information;
- (b) notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information;
- (c) notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Section 5. 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 the Privacy Regulations if done by Covered Entity.

Section 6. Term and Termination

- (a) Term. The Term of this Agreement shall be effective as of _____ and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity or, if it is not feasible to return or destroy the Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.
- (b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
- (1) provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
 - (2) immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
 - (3) if neither termination nor cure is feasible, report the violation to the Secretary.
- (c) Effect of Termination.
- (1) Except as provided in paragraph (2) of this section, upon termination of this Agreement for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

- (2) In the event that Business Associate determines that returning or destroying the Protected Health Information is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of Protected Health Information is not feasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Section 7. Miscellaneous

- (a) Regulatory References. A reference in this Agreement to a section in the Privacy Regulations or Security Regulations means the section in effect, or as amended.
- (b) 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 Regulations, the Security Regulations, the Health Insurance Portability and Accountability Act, and the HITECH Act and its implementing regulations.
- (c) Survival. The respective rights and obligations of Business Associate under Section 6(c) of this Agreement shall survive the termination of this Agreement.
- (d) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Regulations, the Security Regulations, the Health Insurance Portability and Accountability Act, and the HITECH Act.
- (e) Identity Theft Regulations. To the extent that Business Associate provides services in connection with an account maintained by the Covered Entity that permits patients to make multiple payments for services rendered by the Covered Entity (including, but not limited to, billing and collection services), Business Associate shall have and follow policies to detect and prevent identity

theft in accordance with the identity theft regulations of the Federal Trade Commission, 16 C.F.R. §681.2. In addition, in such case Business Associate shall: (1) report to Covered Entity any pattern, practice, or specific activity that indicates the possible existence of identity theft ("Red Flags") involving anyone associated with Covered Entity, including its patients, employees, and contractors, and (2) take appropriate steps to prevent or mitigate identity theft when a Red Flag is detected.

The parties have caused this Agreement to be executed on the date first written above.

DATE: _____

[COVERED ENTITY]

WITNESS: _____

BY: _____

DATE: _____

[BUSINESS ASSOCIATE]

WITNESS: _____

BY: _____

