

# BUSINESS ASSOCIATE AGREEMENT

This Agreement is made by and between **Business Associate** and **Covered Entity** and modifies any other prior existing contract for this purpose.

The effective date of this agreement is: \_\_\_\_\_

## 1. DEFINITIONS.

- 1.1. **Breach** shall mean the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exceptions set forth, in 45 CFR Section 164.402.
- 1.2. **Business Associate** 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 \_\_\_\_\_.
- 1.3. **Covered Entity** 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 \_\_\_\_\_.
- 1.4. **HIPAA Rules** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- 1.5. **HITECH BA Provisions** shall mean those provisions of the HITECH Act of the American Reinvestment and Recovery Act of 2009 imposing requirements on business associates with respect to privacy, security and breach notification, plus any regulations adopted by the Secretary to implement the HITECH Act business associate provisions.
- 1.6. **Individual** shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- 1.7. **Privacy Rule** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
- 1.8. **Protected Health Information** shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

- 1.9. **Required by Law** shall have the same meaning as the term "required by law" in 45 CFR 164.501.
- 1.10. **Secretary** shall mean the Secretary of the Department of Health and Human Services or his designee.
- 1.11. **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.
- 1.12. **Service Agreement** shall mean that certain Agreement between Business Associate and Covered Entity dated \_\_\_\_\_.

All other capitalized terms not defined herein shall have the meanings assigned in the Privacy Rule, the Security Rule and the HITECH Act.

## **2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.**

- 2.1. Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as required by Law.
- 2.2. Business Associate agrees 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 by this Agreement.
- 2.3. Business Associate agrees to 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.
- 2.4. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this 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.
- 2.5. Business Associate agrees to 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, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2).

- 2.6. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, 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 CFR 164.524.
- 2.7. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.
- 2.8. Business Associate agrees to make internal practices, books, and records 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 Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- 2.9. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with CFR 164.528.
- 2.10. Within fifteen (15) days of receiving a request from Covered Entity, Business Associate agrees to make available the information necessary for Covered Entity to make an accounting of Disclosures of PHI about an Individual.
- 2.11. The provisions of the HITECH Act that apply to business associates and are required to be incorporated by reference in a business associate agreement are hereby incorporated into this Agreement, including, without limitation, 42 USC Sections 17935(b), (c),(d) & (e), and 17936(a) & (b).
- 2.12. Without limitation of the foregoing:
  - 2.12.1. Pursuant to 42 USC Section 17931(a), the following sections of the Security Rule shall apply to Business Associate in the same manner as they apply to the covered entity:
    - 2.12.1.1. Section 164.308 – Administrative Safeguards;
    - 2.12.1.2. Section 164.310 – Physical Safeguards;
    - 2.12.1.3. Section 164.312 – Technical Safeguard; and
    - 2.12.1.4. Section 164.316 – Policies and procedures and documentation requirements.
  - 2.12.2. Pursuant to 42 USC Section 17934(a), Business Associate may use or disclose PHI that it obtains or creates only if such use or disclosure,

respectively, is in compliance with each applicable requirements of Section 164.504(e) of the Privacy Rule.

2.12.3. Pursuant to 42 USC Sections 17931(b), 17934(b) & 17934(c), Section 164.504(e)(1)(ii) of the Privacy Rule shall apply to Business Associate with respect to compliance with such subsection, in the same manner that such section applies to Covered Entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of the Privacy Rule, except that in applying such Section 164.504(e)(1)(ii) each reference to Business Associate, with respect to a contract, shall be treated as a reference to the Covered Entity involved in such contract. To the extent necessary to achieve the purposes of the foregoing, Business Associate shall have the right to terminate this Agreement and all contracts to which it relates if Covered Entity is in material breach or violation of this Agreement and fails to cure such breach or violation.

2.12.4. 42 USC Sections 17931(b) & 17934(c) each apply to Business Associate with respect to its status as a business associate to the extent set forth in each such Section.

2.12.5. Pursuant to 42 USC Section 17932, without unreasonable delay, and in any event no later than sixty (60) calendar days after Discovery, Business Associate shall notify Covered Entity of any Breach of Unsecured PHI. The notification shall include, to the extent possible and subsequently as the information becomes available, the identification of all individuals whose Unsecured PHI is reasonably believed by Business Associate to have been Breached along with any other available information that is required to be included in the notification to the Individual, HHS and/or the media, all in accordance with the data breach notification requirements set forth in 42 USC Section 17932 and 45 CFR Parts 160 & 164 subparts A, D, & E.

### **3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.**

3.1. General Use and Disclosure Provisions: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the purposes discussed in this section, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity, for the purpose of performing the Service Agreement.

3.2. Specific Use and Disclosure Provisions:

3.2.1. 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.

- 3.2.2. 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 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.
- 3.2.3. 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 CFR 164.504(e)(2)(i)(B).

#### **4. OBLIGATIONS OF COVERED ENTITY.**

- 4.1. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.
- 4.2. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- 4.3. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.
- 4.4. Covered Entity shall 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 CFR 164.522.
- 4.5. 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 Rule if done by Covered Entity.

#### **5. TERM AND TERMINATION.**

- 5.1. Term. The Term of this Agreement shall be effective as of the date first

written above, 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 infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. Termination of this Agreement shall automatically terminate the Service Agreement.

5.2. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation, and Covered Entity shall:

5.2.1. Terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or

5.2.2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

5.2.3. If neither termination nor cure is feasible, Covered Entity will report the violation to the Secretary.

5.3. Effect of Termination.

5.3.1. Except as provided in the following paragraph, 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 in accordance with State and Federal retention guidelines. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate and its subcontractors, if any, shall retain no copies of the Protected Health Information.

5.3.2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, 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 infeasible, Business Associate shall extend the protections of this Agreement to 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.

5.3.3. In the event Covered Entity and Business Associate agree that

Business Associate shall retain Protected Health Information after the termination of this Agreement, with respect to Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, Business Associate shall:

- 5.3.3.1. Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration to carry out its legal responsibilities;
- 5.3.3.2. Return to Covered Entity the remaining Protected Health Information that Business Associate still maintains in any form;
- 5.3.3.3. 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;
- 5.3.3.4. Not to 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 to which applied prior to termination; and
- 5.3.3.5. 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. MISCELLANEOUS.

- 6.1. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.
- 6.2. 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, Public Law 104-191.
- 6.3. Survival. The respective rights and obligations of Business Associate under Section 5.3 of this Agreement shall survive the termination of this Agreement.
- 6.4. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

- 6.5. Indemnification. Business Associate shall defend and indemnify Covered Entity against, and hold Covered Entity (including Covered Entity’s affiliates, and its and their officers, directors, trustees, employees, and agents) harmless from any and all loss, damage, penalty, liability, cost and expense, including without limitation, reasonable attorneys fees and disbursements, that may be incurred, imposed upon, or asserted against Covered Entity by reason of any claim, regulatory proceeding, or litigation arising directly or indirectly from any act or omission of Business Associate or its officers, directors, employees, subcontractors, agents, representatives and/or other persons acting on its behalf, with respect to using or disclosing PHI, or maintaining the security, confidentiality, integrity and availability of Electronic PHI, in accordance with this Agreement or applicable federal or state law.
- 6.6. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.
- 6.7. Entire Agreement. This Agreement is the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements, negotiations, and communications of whatever type, whether written or oral, between the parties hereto with respect to the subject matter hereof, including any prior Agreement signed by the parties to comply with HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and/or the HITECH Standards, if any. Except to the extent specifically amended hereby, the provisions of the Agreement shall remain unmodified, and the Agreement as amended hereby is confirmed as being in full force and effect.

**COVERED ENTITY**

**BUSINESS ASSOCIATE**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

\_\_\_\_\_  
Address

\_\_\_\_\_  
Address