

BUSINESS ASSOCIATE NDA AGREEMENT

As of _____20____, the following parties have made and entered into this Business Associate NDA Agreement (the "BAA"):

Covered Entity: _____, a(n) (select one)

LLC

Corporation

Partnership

Other: _____ ("Covered Entity")

AND

Business Associate: _____, a(n) (select one)

Individual

LLC

Corporation

Partnership

Other: _____ ("Business Associate"), as defined by 45 CFR 164.501 for those terms.

Each party to this BAA, including the Covered Entity and Business Associate, is referred to as a "Party" and jointly as "Parties"

BACKGROUND

I. An entity that is covered under the Health Insurance Portability and Accountability Act of 1986, Public Law 104-191, is defined as a "covered entity" or a "business associate" of a covered entity. The provisions of HIPAA regarding the confidentiality and privacy of Protected Health Information (as defined below) must be followed by the HITECH Act (as defined below) and any related regulations issued by HHS (as defined below);

II. The Parties have entered into or will enter into one or more agreements (collectively, the "Agreement"), pursuant to which Business Associate has provided or will provide Covered Entity with certain specified services.

III. Business Associate will have access to Protected Health Information while performing services under the Agreement.

IV. Business Associate will become a "business associate" of the Covered Entity in accordance with the HIPAA definition of that term by rendering the services in accordance with the Agreement.

V. Both Parties are committed to adhering to all federal and state laws governing

the confidentiality and privacy of health information, including, but not limited to, the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Part 160 and Part 164, Subparts A and E (collectively, the "Privacy Rule");

VI. Both Parties intend to safeguard the privacy and guarantee the security of Protected Health Information disclosed to Business Associate in accordance with the Privacy Rule.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual obligations set forth herein and the Covered Entity's continued provision of PHI to Business Associate pursuant to the Agreement in reliance on this BAA, the Parties hereby agree as follows:

Definitions: For the purposes of this BAA, the Parties define each term in this Section 1 as follows. Any capitalized term used in this BAA that is not otherwise defined has the same definition as it does in the Privacy Rule or any other applicable law.

- a. "**Affiliate**": refers to a subsidiary or affiliate of a covered entity that is currently or has previously been regarded as a covered entity under HIPAA.
- b. "**Breach**" refers to the acquisition, access, use, and disclosure of PHI in a manner prohibited by the Privacy Rule which compromises its security or privacy. as defined in 45 CFR § 164.402.
- c. "**Breach Notification Rule**" refers to the section of HIPAA outlined in Subpart D of 45 CFR Part 164.
- d. "**Data Aggregation**" refers to the combining of PHI created or received by Business Associate in its capacity as the "business associate" under HIPAA of the Covered Entity with the PHI received by Business Associate in its capacity as the business associate of one or more other "covered entities" under HIPAA to enable data analyses pertaining to the Health Care Operations (defined below) of the respective covered entities. In this BAA, the term "data aggregation" shall have the same meaning as it does in the Privacy Rule.
- e. "**Designated Record Set**" means as defined under the Privacy Rule, including 45 CFR 164.501.B.
- f. "**De-Identify**" refers to changing PHI in a way that ensures the resulting data satisfies the criteria outlined in 45 CFR 164.514(a) and (b).
- g. "**Electronic PHI**" According to 45 CFR 160.103, it refers to any PHI stored on or transmitted through electronic media.
- h. "**Health Care Operations**" possesses the meaning ascribed to that phrase in 45 CFR 164.501.
- i. "**HHS**" means the U.S. Department of Health and Human Services.
- j. "**HITECH Act**" means the Health Information Technology for Economic and Clinical Act, enacted as part of the American Recovery and

Reinvestment Act of 2009, Public Law 111-005.

- k. **"Individual"** As outlined in 45 CFR 164.501 and 160.130, it includes a person who meets the criteria for personal representatives under 45 CFR 164.502(g)
- l. **"Privacy Rule"** means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E.
- m. **"Protected Health Information"** or **"PHI"** has the meaning given to the term "protected health information" in 45 CFR §§164.501 and 160.103, limited to the information created or received by Business Associate from or on behalf of the Covered Entity.
- n. **"Security Incident"** A "security incident" is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information, as well as any interference with an information system's normal operation.
- o. **"Security Rule"** It refers to Subparts A and C of 45 CFR Parts 160 and 164's Security Standards for the Protection of Electronic Health Information.
- p. **"Unsecured Protected Health Information"** or "Unsecured PHI" is any "protected health information" as defined in 45 CFR 164.501 and 160.103 that has not been made "unusable, unreadable, or indecipherable" by means of a technology or methodology specified by the HHS Secretary in the guidance issued in accordance with the HITECH Act and codified at 42 USC 17932(h).

Use and Disclosure of PHI.

- b. Except as otherwise specified in this BAA, Business Associate may use or disclose PHI as reasonably necessary to perform the services set forth in the Agreement with the Covered Entity and to carry out any other activities that are authorized or mandated by this BAA or by applicable law.
- c. With the exception of any other restrictions imposed by this BAA or federal or state law, the Covered Entity grants Business Associate permission to use the PHI it has in its possession for the necessary management and operation of Business Associate's operations as well as to fulfill its legal obligations. Business Associate may disclose PHI for its proper management and administration, provided that (i) the disclosures are required by law; or (ii) Business Associate obtains, in writing, prior to making any disclosure to a third party (a) reasonable assurances from this third party that the PHI will be kept confidential as provided by this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to this third party, and (b) an agreement from this third party that the PHI will be immediately of any breaches of the confidentiality of the PHI, to the extent it has knowledge of the breach.
- c. Other than what is specified in this BAA, what is allowed by the Privacy Rule, or what is required by law, Business Associate will not use or disclose PHI in any other way. In accordance with Section 13405(b) of the HITECH ACT (codified as 42 USC 17935(b)) and any of the act's

implementing regulations adopted by HHS, Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimal amount of PHI necessary to carry out the intended purpose.

- d. Any PHI belonging to the Covered Entity that Business Associate or any of its agents or subcontractors have in their possession will be made available to the Covered Entity upon request.
- e. In accordance with 45 CFR 164.502(j)(1), Business Associate may use PHI to report legal violations to the relevant federal and state authorities.

Safeguards Against Misuse of PHI.

Business Associate agrees to put in place administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate will take the necessary measures to prevent the use or disclosure of PHI outside of those circumstances specified by the Agreement or this BAA. To ensure compliance with this BAA and to prevent a breach of its terms by Business Associate due to the actions or inactions of its employees or agents, Business Associate agrees to take reasonable measures, including giving its employees the necessary training.

Reporting Disclosures of PHI and Security Incidents.

Any use or disclosure of PHI not permitted by this BAA must be reported to the covered entity in writing by the business associate. Additionally, the business associate agrees to notify the covered entity of any security incident affecting electronic PHI of the covered entity. Any such event will be reported within 30 business days, per Business Associate's agreement.

Reporting Breaches of Unsecured PHI.

In accordance with the requirements outlined in 45 CFR 164.410, Business Associate must immediately notify the Covered Entity in writing after learning of any breach of unsecure PHI, but no later than 30 calendar days after learning of the breach. Any expenses that Covered Entity incurs in order to comply with Subpart D of 45 CFR 164 as a result of a Breach committed by Business Associate will be reimbursed by Business Associate to Covered Entity.

Mitigation of Disclosures of PHI.

Any negative effects of any use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of the terms of this BAA that are known to Business Associate will be mitigated, to the extent practicable, by Business Associate by taking reasonable measures.

Agreements with Agents or Subcontractors.

Business Associate shall take steps to ensure that any of its agents or subcontractors that have access to, or to whom Business Associate provides, PHI, agree in writing to the restrictions and conditions regarding uses and disclosures of PHI contained in this BAA and agree to implement reasonable and appropriate safeguards to protect any Electronic PHI that it creates, receives, maintains, or transmits on behalf of Business Associate or, through the Business Associate, Covered Entities. Business Associate shall disclose all subcontracts and agreements pertaining to the Agreement in which the subcontractor or agent received PHI as described in section 1.M of this BAA to the Covered Entity or any upstream Business Associate. Within 30 days of the subcontract's execution, this notification must be made by posting a notice on the Business Associate's main website. Business Associate is responsible for making sure that all contracts and subcontracts offer the same level of security and privacy as this BAA.

Audit Report.

Business Associate shall make available to Covered Entity or upstream Business Associate upon request a copy of the Business Associate's most recent independent HIPAA compliance report (AT-C 315), HITRUST certification, or other mutually agreed upon independent standards based third party audit report. The Covered Entity agrees not to divulge the audit findings of the Business Associate again.

Access to PHI by Individuals.

- a. Upon request, Business Associate agrees to deliver copies of the PHI kept by Business Associate in a Designated Record Set to Covered Entity in the format and timeframe specified by Covered Entity. enable Covered Entity to respond to an Individual's request for access to PHI under 45 CFR §164.524.
- b. Any time an Individual or personal representative contacts a Business Associate directly to request access to their PHI, the Business Associate must forward that request to the Covered Entity within 10 business days. It is the sole responsibility of the Covered Entity to comply with the rules governing an Individual's right to obtain access to PHI and to make any disclosures of, or decisions not to disclose, the PHI that an Individual or a personal representative requests.

Amendment of PHI.

- a. Business Associate will amend PHI or a record about an Individual in a Designated Record Set that is maintained by, or otherwise in the possession of, Business Associate as directed by Covered Entity as per the guidelines established by 45 CFR 164.526 upon request and instruction from Covered Entity. Within 15 business days of receiving a request from a covered entity, the business associate will fulfill that request.
- b. If any Individual requests that Business Associate amend their PHI or record in a Designated Record Set, Business Associate will send this request to the Covered Entity within 10 business days. The sole responsibility of the Covered Entity shall be for any amendment of, or decision not to amend, the PHI or record as requested by an Individual, and for compliance with the laws governing an Individual's right to request an amendment of PHI.

Accounting of Disclosures.

- a. Business Associate will document any disclosures of PHI made by it to account for such disclosures as required by 45 CFR §164.528(a). Business Associate also will make available information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, Business Associate will furnish Covered Entity the following with respect to any covered disclosures by Business Associate: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.
- b. Business Associate will furnish to Covered Entity information collected in accordance with this Section 10, within 10 business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or in the event that Covered Entity elects to provide an Individual with a list of its business associates, Business Associate will provide an accounting of its disclosures of PHI upon request if the Individual, if and to the extent that such accounting is required under the HITECH ACT or under HHS regulations adopted in connection with the HITECH ACT.
- c. If an individual sends a business associate their initial request for an accounting, the business associate will send that request to the covered entity within 10 business days.

Availability of Books and Records.

The Secretary of HHS may request access to Business Associate's internal practices, books, agreements, records, and policies and procedures relating to the use and disclosure of PHI for the purpose of assessing HIPAA and this BAA compliance by the Covered Entity and Business Associate.

Responsibilities of Covered Entity.

In relation to the use and/or disclosure of Protected Health Information by a Business Associate, the Covered Entity agrees to:

- a. Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- b. Notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- c. Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- d. Except for data aggregation or management and administrative activities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

Data Ownership.

Business Associate does not acquire any ownership rights over any data shared with it under the Agreement, including any and all forms of such data, as a result of its role as data steward.

Term and Termination.

- a. This BAA will become effective on the date first written above and will continue in effect until all obligations of the Parties have been met under the Agreement and under this BAA.
- b. Covered Entity may terminate this BAA, the Agreement, and any other related agreements if Covered Entity makes a determination that Business Associate has breached a material term of this BAA and Business Associate has failed to cure that material breach, to Covered Entity's reasonable satisfaction, within 30 days after written notice from Covered Entity. Covered Entity may report the problem to the Secretary of HHS if termination is not feasible.
- c. If Business Associate determines that Covered Entity has breached a material term of this BAA, then Business Associate will provide Covered Entity with written notice of the existence of the breach and shall provide Covered Entity with 30 days to cure the breach. Covered Entity's failure to cure the breach within the 30-day period will be grounds for immediate termination of the Agreement and this BAA by Business Associate. Business Associate may report the breach to the HHS.

- d. Upon termination of the Agreement or this BAA for any reason, all PHI maintained by Business Associate will be returned to Covered Entity or destroyed by Business Associate. Business Associate will not retain any copies of such information. This provision will apply to PHI in the possession of Business Associate's agents and subcontractors. If return or destruction of the PHI is not feasible, in Business Associate's reasonable judgment, Business Associate will furnish Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate will extend the protections of this BAA to such information for as long as Business Associate retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. The Parties understand that this Section 14.D. will survive any termination of this BAA.

Effect of BAA.

- a. This BAA is a part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern.
- b. Except as expressly stated in this BA or as provided by law, this BAA will not create any rights in favor of any third party.

Regulatory References.

A reference in this BAA to a section in HIPAA means the section as in effect or as amended at the time.

Notices.

All notices, demands, and other communications owed to a Party under this BAA shall be sent to the Party at the following address by first class mail, registered mail, certified mail, express courier, or email:

- a. If to Covered Entity, to:
Name: _____
Attn: _____
Mailing Address: _____
Telephone: (____) ____ - _____
E-Mail: _____
- b. If to Business Associate, to:
Name: _____
Attn: _____
Mailing Address: _____
Telephone: (____) ____ - _____
E-Mail: _____

Amendments and Waiver.

No provision of this BAA may be waived or amended, nor may any provision be modified, except in a written document duly signed by authorized representatives of the Parties. A waiver with regard to one event cannot be taken to be perpetual, as a restriction on or waiver of any right or remedy with regard to subsequent events.

HITECH ACT Compliance.

The Parties agree that the Privacy Rule and the Security Rule have undergone and includes significant changes as a result of the HThe privacy subtitle of the HITECH Act contains provisions that materially alter the obligations placed on business associates and the contracts that they enter into with covered entities under HIPAA. Each Party commits to observing all relevant HITECH Act clauses as well as any HHS rules made in connection with the HITECH Act. guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective but, in the event that the Parties are unable to reach an agreement on such a modification, either Party will have the right to terminate this BAA upon 30 days' prior written notice to the other Party.

The Parties execute this BAA as of the first written above date in light of the mutual agreement and understanding described above.

Covered Entity Signature: _____

Date: _____ Name in Print _____

Title: _____

Business Associate Signature: _____

Date: _____ Name in Print: _____

Title: _____

