

# Business Associate Agreement

## BACKGROUND

- Covered Entity, as defined below, is either a “covered entity” or “business associate” of one or more covered entities as each are defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the HITECH Act and the related regulations promulgated by HHS (collectively, “HIPAA”) and, as such, is required to comply with HIPAA’s provisions regarding the confidentiality and privacy of Protected Health Information (“PHI”);
- The Parties have entered into or will enter into one or more agreements under which Business Associate, as defined below, provides or will provide certain specified Services to Covered Entity (collectively, the “Master Agreement”);
- In providing Services pursuant to the Master Agreement, Business Associate may have access, use or disclose PHI of Covered Entity;
- Both Parties are committed to complying with 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”); and
- Both Parties intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the terms of this Business Associate Agreement (“BAA”), HIPAA and other applicable federal and state laws.

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein and the continued provision of PHI by Covered Entity to Business Associate under the Master Agreement in reliance on this BAA, the Parties agree as follows:

## **1. DEFINITIONS.**

- 1.1. Catch All Definitions.** The following terms used in this BAA shall have the same meaning as those terms set forth in the Privacy Rule, the Security Rule, and the HITECH Act, including: Breach, Business Associate, Covered Entity, Data Aggregation, Designated Record Set, De-Identify, Disclosure, Health Care Operations, Individual, Limited Data Set, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (“PHI”) as applied to the information created or received by Business Associate from or on behalf of Covered Entity, electronic PHI (“ePHI”), Required by Law, Secretary, Subcontractor, Unsecured Protected Health Information (“Unsecured PHI”), and Use. Terms used in this Agreement not otherwise defined herein shall have the meanings ascribed to them in the HIPAA Rules or the Master Agreement between Covered Entity and Business Associate, as applicable.
- 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 BAA, shall refer to **Company** as defined in the Master Agreement between the Parties.
- 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 BAA, shall refer to the **Client** as defined in the Master Agreement between the Parties.
- 1.4. “HIPAA Rules”** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.
- 1.5. “Successful Security Incident”** shall mean a security incident that results in the unauthorized access, use, disclosure, modification, or destruction of PHI. For the avoidance of doubt, Successful Security Incident shall NOT mean a security incident that does not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including, for example, and not for limitation, pings on Business Associate’s firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses).

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

- 2.1.** Business Associate may use or disclose PHI as necessary to perform the Services for, or on behalf of Covered Entity, as set forth in this BAA or in the Master Agreement between the Parties.
- 2.2.** Business Associate may use or disclose PHI as Required by Law.
- 2.3.** Business Associate may use PHI for Data Aggregation services or to De-Identify the information for any lawful purpose, in accordance with 45 C.F.R. § 164.514(a)–(c).
- 2.4.** Business Associate may use or disclose PHI for its proper management and administration or to carry out the Business Associate’s legal responsibilities, provided the disclosures are Required by Law, or Business Associate has obtained 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.

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

# Business Associate Agreement

---

## **Business Associate agrees to:**

- 3.1.** Except as otherwise permitted in this BAA, only use or disclose PHI as reasonably necessary to provide the Services described in the Master Agreement, and to undertake other activities of Business Associate permitted or required of Business Associate by this BAA, or as Required by Law;
- 3.2.** Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this BAA or the Master Agreement. Business Associate operates under the HITRUST Common Security Framework (CSF) to leverage industry recognized standards outlined further in the Information Security Program found [here](#), and which may be updated from time-time;
- 3.3.** Report to Covered Entity any use or disclosure of PHI not permitted under this BAA or the Master Agreement of which Business Associate becomes aware, including a Breach of Unsecured PHI as required at 45 C.F.R. § 164.410 and any Successful Security Incident, within five (5) business days of any Breach or Successful Security Incident. When applicable, and as soon as reasonably possible, Business Associate shall supplement with a written report containing any information known to the Business Associate at that time;
- 3.4.** In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractor(s) that creates, receives, maintains, or transmits PHI on behalf of Business Associate for Services provided to Covered Entity, agrees to substantially similar restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI;
- 3.5.** To the extent Business Associate has PHI contained in a Designated Record Set, Business Associate agrees to make such PHI available to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524 within fifteen (15) business days of receipt of such written request; provided, however, that Business Associate is not required to provide such access where the PHI contained in a Designated Record Set is duplicative of the PHI contained in a Designated Record Set possessed by Covered Entity. If an Individual makes a request for access pursuant to 45 C.F.R. § 164.524 directly to Business Associate, or inquires about his or her right to access, Business Associate shall direct the Individual to Covered Entity and any decision to disclose will be the sole responsibility of Covered Entity;
- 3.6.** To the extent Business Associate has PHI contained in a Designated Record Set, Business Associate agrees to make such PHI available to Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526; To the extent Business Associate has PHI contained in a Designated Record Set, it agrees to make such information available to Covered Entity for amendment pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526. If an Individual makes a request for an amendment pursuant to 45 C.F.R. § 164.526 directly to Business Associate, or inquires about his or her right to an amendment, Business Associate shall direct the Individual to Covered Entity and any decision to amend will be the sole responsibility of Covered Entity;
- 3.7.** In accordance with 45 C.F.R. § 164.509, when Business Associate receives a request for PHI potentially related to reproductive health care purposes specified in 45 C.F.R. §§ 164.512(d), (e), (f), or (g)(1), Business Associate shall direct the requestor to Covered Entity to obtain a valid attestation as required by 45 C.F.R. § 164.509(b)(1), and any decision to disclose such information will be the sole responsibility of Covered Entity;
- 3.8.** 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 C.F.R. § 164.528 by providing such information within thirty (30) business days of receipt of such written request;
- 3.9.** To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, it shall comply with the requirements of Subpart E that would similarly apply to Covered Entity in the performance of such obligation(s);
- 3.10.** Cooperate in good faith in all respects with Covered Entity in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry;
- 3.11.** To the extent practicable, cooperate in good faith with Covered Entity's efforts to mitigate a harmful effect that is known to Business Associate of a use or disclosure of PHI not provided for in this BAA;
- 3.12.** Request, use and disclose PHI, to the extent practicable, as a Limited Data Set or limited to the minimum amount of PHI necessary to carry out the intended purpose of the use or disclosure, in accordance with 45 C.F.R. § 164.514(d); and
- 3.13.** Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of, Covered Entity available to the Secretary for purposes of determining compliance with the HIPAA Rules.

# Business Associate Agreement

---

## 4. OBLIGATIONS OF COVERED ENTITY.

### Covered Entity agrees to:

- 4.1 Promptly notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices under 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI;
- 4.2 Promptly notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI;
- 4.3 Promptly notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI;
- 4.4 Cooperate in good faith in all respects with Business Associate in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry;
- 4.5 Not make a request of Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except that Business Associate may use or disclose PHI for management and administration and legal responsibilities as described herein; and
- 4.6 Abide by the Client General Requirements outlined in the Information Security Program found [here](#), and which may be updated from time-to-time.

## 5. TERM AND TERMINATION.

- 5.1 **Term.** The term of this BAA shall commence as of the Effective Date and shall terminate when all of the PHI 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 PHI, protections are extended to such information, in accordance with Section 5.3.
- 5.2 **Termination for Cause.** At such time as Covered Entity reasonably determines in good faith that Business Associate has violated a material term of this BAA and Business Associate has not cured the breach or ended the violation within thirty (30) business days after written notice from Covered Entity of the violation, Covered Entity may elect to terminate the Master Agreement and this BAA for cause.

### 5.3 **Obligations of Business Associate Upon Termination.**

Upon termination of this BAA for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall return to Covered Entity or destroy the PHI received by Business Associate on behalf of, Covered Entity. In the event Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall continue to extend the protections to such PHI as required by the HIPAA Rules and limit further use and disclosure for so long as Business Associate retains such PHI. If Business Associate so retains any PHI upon termination of this BAA as provided above, Business Associate shall:

- A. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
- B. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained;
- C. Return to Covered Entity or destroy the remaining PHI that Business Associate still maintains in any form;
- D. Return to Covered Entity or destroy the PHI 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; and
- E. Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI.

- 6. **Survival.** The respective rights and obligations of Business Associate under Section 5.3 of this BAA shall survive the termination of this BAA and the Master Agreement.

## Business Associate Agreement

---

7. **Effect of BAA.** In the event of any inconsistency between the provisions of this BAA and the Master Agreement, the provisions of this BAA shall control. In the event of inconsistency between the provisions of this BAA and mandatory provisions of the Privacy Rule, the Security Rule or the HITECH Act, as amended, or their interpretation by any court or regulatory agency with authority over Business Associate or Covered Entity, such interpretation shall control. Provided, however, that if any relevant provisions of the Privacy Rule, the Security Rule or the HITECH Act is amended in a manner that changes the obligations of Business Associate or Covered Entity that are embodied in the terms of this BAA, then the Parties agree to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations. Where provisions of this BAA are different from those mandated in the Privacy Rule, the Security Rule or the HITECH Act, but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this BAA shall control.

In the event of inconsistency between the provisions of this BAA and state law, applicable to Covered Entity's operations, the Parties agree to abide by the more stringent requirement, unless otherwise prohibited by federal law. The Parties will negotiate in good faith appropriate terms or amendments to this BAA to give effect to any obligations of Business Associate or Covered Entity required by the applicable state law. If either Party becomes aware of any changes in applicable state law that may affect the obligations of Business Associate or Covered Entity under this BAA, it shall notify the other Party.

8. **General.** This BAA is governed by, and shall be construed in accordance with, the laws of the State that govern the Master Agreement between the Parties. Covered Entity shall not assign this BAA without the prior written consent of Business Associate, which shall not be unreasonably withheld. If any part of a provision of this BAA is found illegal or unenforceable, it shall be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this BAA shall not be affected. All notices relating to the Parties' legal rights and remedies under this BAA shall be provided in accordance with the Notice Section of the Master Agreement and shall reference this BAA. This BAA may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both Parties. Nothing in this BAA shall confer any right, remedy, or obligation upon anyone other than Covered Entity and Business Associate. This BAA is the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter.