

## HIPAA BUSINESS ASSOCIATE AGREEMENT

**THIS HIPAA BUSINESS ASSOCIATE AGREEMENT** (“BAA”) is entered into effective the day of \_\_\_\_\_, 20\_\_\_\_ (“Effective Date”), by and between the Regents of the University of Michigan, a Michigan constitutional corporation on behalf of its affiliates (“UM”) and \_\_\_\_\_ (“Business Associate”). UM is a hybrid entity under the Health Insurance Portability and Accountability Act of 1996, its amendments and implementing regulations (“HIPAA”). UM has designated most of its health care providers and all of its health plans as covered entity components under HIPAA (individually and collectively, “Covered Entity”).

Business Associate may perform functions or activities on behalf of Covered Entity involving the creation, receipt, maintenance, access, transmission, use and/or disclosure of protected health information (“PHI”) received from or on behalf of Covered Entity. Therefore, Business Associate agrees to the following terms and conditions set forth in this BAA.

- 1.0 **Definitions.** For purposes of this BAA, any terms used herein, unless otherwise defined, shall have the same meanings as used in the HIPAA Privacy and Security Standards, as amended by the Health Information Technology for Economic and Clinical Health Act (Title XIII of the American Recovery and Reinvestment Act of 2009) and its implementing regulations (“HITECH”), including modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH.
- 2.0 **Scope and Interpretation.** The terms and conditions of this BAA shall supplement and amend all agreements and relationships between the parties (“Base Agreement(s)”) which provide for Business Associate’s creation, receipt, maintenance, access, transmission, use, and/or disclosure of PHI, in any form or medium, including electronic PHI (“ePHI”), in Business Associate’s capacity as “Business Associate” to Covered Entity. Any ambiguity in this BAA shall be resolved to permit Covered Entity to comply with HIPAA. In case of any inconsistency or conflict between the Base Agreement(s) and the terms and conditions of this BAA, the terms and conditions of this BAA shall control. Except as supplemented and/or amended, the terms of the Base Agreement(s) shall continue to govern matters addressed in the Base Agreement(s).
- 3.0 **Compliance with Applicable Law.** Beginning with the relevant effective date, to the extent Business Associate meets the definition of a “Business Associate” of Covered Entity as such term is defined under HIPAA, Business Associate and its subcontractors, as applicable, shall comply with its obligations under this BAA and with all obligations of a business associate under HIPAA, HITECH, as modified, and other related laws, for so long as Business Associate creates, receives, maintains, accesses, or transmits PHI.
- 4.0 **OBLIGATIONS OF BUSINESS ASSOCIATE**
  - 4.1 **Permissible Use and Disclosure of PHI.** In addition to the uses and disclosures permitted by the Base Agreement(s), Business Associate may use and disclose PHI:
    - a. For its own proper management and administration,
    - b. To carry out its legal responsibilities, and
    - c. For data aggregation purposes as required or requested by Covered Entity.

4.2 **Limitations on Use and Disclosure of PHI.** Business Associate shall not, and shall ensure that its directors, officers, employees, agents, and subcontractors do not, use or disclose PHI in any manner that is not permitted or required by the Base Agreement(s) or this BAA, or as Required by Law. All uses and disclosures of, and requests by Business Associate for, PHI are subject to the Privacy Standards' Minimum Necessary Rule and shall be limited to the information contained in a Limited Data Set, to the extent practical, unless additional information is needed to accomplish the intended purpose, or as otherwise permitted in accordance with Section 13405(b) of HITECH, and any other subsequently adopted guidance. Additionally, Business Associate must ensure that neither it nor its directors, officers, employees, agents, or subcontractors, access, store, share, maintain, use, or disclose PHI outside of the United States of America.

4.3 **Safeguards Prior to Disclosure.** If Business Associate discloses PHI to a third party for any reason listed in paragraph 4.1, Business Associate shall obtain the following prior to disclosure:

- a. Reasonable assurances from the receiving party that such PHI will be held confidential and be disclosed only for the purposes for which it was disclosed to such receiving party or as Required by Law in accordance with HIPAA, and
- b. An agreement from the receiving party to immediately notify Business Associate of any known breaches of the confidentiality of the PHI.

In the event that Business Associate is authorized by Covered Entity to de-identify PHI, Business Associate must specify to Covered Entity the manner in which Business Associate will de-identify information.

4.4 **Security.** To the extent that Business Associate creates, receives, maintains, or transmits ePHI on behalf of Covered Entity, Business Associate shall:

- a. Comply with the security provisions found at 45 C.F.R. §§ 164.308, .310, .312, and .316 in the same manner as such provisions apply to Covered Entity, pursuant to Section 13401(a) of HITECH, and otherwise implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI;
- b. Ensure that any agent to whom Business Associate provides ePHI agrees in writing to implement reasonable and appropriate safeguards to protect such ePHI; and
- c. Report to Covered Entity within five (5) business days any Security Incident of which Business Associate becomes aware and which results in a use or disclosure of ePHI in violation of the Base Agreement(s) or this BAA. For Security Incidents that do not result in a use or disclosure of ePHI in violation of the Base Agreement(s) or this BAA, reports may be made in the aggregate on at least a quarterly basis. In this context, the term "Security Incident" shall have the same meaning as such term is defined at 45 C.F.R. § 164.304.

4.5 **Privacy.** To the extent that Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the

performance of its obligation(s) under this BAA. Business Associate shall also otherwise implement appropriate safeguards in accordance with the Privacy Standards to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of this BAA.

- 4.6 **Mitigation of Harmful Effects.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA, including, but not limited to, compliance with any state law or contractual data breach requirements.
- 4.7 **Breach of Security or Privacy Obligations.**
- a. Business Associate shall report to Covered Entity, within five (5) business days of discovery, a use or disclosure of PHI not provided for in this BAA by Business Associate, its officers, directors, employees, agents, or subcontractors or by a third party to whom Business Associate disclosed PHI.
  - b. Business Associate shall report to Covered Entity, within five (5) business days of discovery, a breach of unsecured PHI in accordance with the requirements set forth in 45 C.F.R. §§ 164.400-414. Business Associate shall fully cooperate with Covered Entity's breach notification and mitigation activities, and shall be responsible for all costs incurred by Covered Entity for those activities.
- 4.8 **Agreements by Third Parties.** Business Associate shall enter into an agreement with any agent or subcontractor of Business Associate that will have access to PHI hereunder. Pursuant to such agreement, the agent or subcontractor shall agree to be bound by the same restrictions, terms, and conditions that apply to Business Associate under this BAA with respect to such PHI. Business Associate agrees to provide Covered Entity a list of all its agents or subcontractors upon request.
- 4.9 **Access to Information.** Within ten (10) business days of a request by Covered Entity for access to PHI about an individual contained in a Designated Record Set, Business Associate shall make available to Covered Entity such PHI for so long as such information is maintained by Business Associate in the Designated Record Set, as required by 45 C.F.R. § 164.524. In the event any individual delivers a request for access to PHI directly to Business Associate, Business Associate shall, within five (5) business days, forward such request to Covered Entity.
- 4.10 **Availability of PHI for Amendment.** Within ten (10) business days of a request by Covered Entity for the amendment of an individual's PHI or a record regarding an individual contained in a Designated Record Set, Business Associate shall provide such information to Covered Entity for so long as PHI is maintained in the Designated Record Set, as required by 45 C.F.R. § 164.526. In the event any individual delivers a request for amendment of PHI directly to Business Associate, Business Associate shall, within five (5) business days, forward such request to Covered Entity.
- 4.11 **Documentation of Disclosures.** Business Associate agrees to document uses and disclosures of PHI and information related to such uses and disclosures as required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

- 4.12 **Accounting of Disclosures.** Within ten (10) business days of notice by Covered Entity to Business Associate that Covered Entity has received a request for an accounting of disclosures of PHI regarding an individual during the six (6) year period prior to the date on which the accounting was requested, Business Associate shall make available to Covered Entity information to permit Covered Entity to respond to the request for an accounting of disclosures of PHI, as required by 45 C.F.R. § 164.528. In the case of an electronic health record maintained or hosted by Business Associate on behalf of Covered Entity, the accounting period shall be three (3) years and the accounting shall include disclosures for treatment, payment, and health care operations, in accordance with the applicable effective date of Section 13402(a) of HITECH. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward such request to Covered Entity within five (5) business days of receipt.
- 4.13 **Judicial and Administrative Proceedings.** In the event Business Associate receives a subpoena, court or administrative order or other discovery request or mandate for release of PHI, Business Associate shall notify Covered Entity in writing prior to responding to such request to enable Covered Entity to object. Business Associate shall notify Covered Entity of the request as soon as reasonably practicable, but in any event within two (2) business days of receipt of such request.
- 4.14 **Availability of Books and Records.** Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy Standards.
- 4.15 **Restrictions.** Business Associate shall comply with any restrictions on disclosure of PHI requested by an individual and agreed to by Covered Entity in accordance with 45 C.F.R. § 164.522.
- 4.16 **Breach of Contract by Business Associate.** In addition to any other rights Covered Entity may have in the Base Agreement(s), this BAA, or by operation of law or in equity, Covered Entity may, upon a breach or violation of this BAA, provide a reasonable opportunity for Business Associate to cure or end any such violation within the time specified by Covered Entity. If cure is not possible or if Business Associate does not cure such breach or violation, Covered Entity may immediately terminate the Base Agreement(s). Covered Entity's option to have a breach cured shall not be construed as a waiver of any other rights Covered Entity has in the Base Agreement(s), this BAA, or by operation of law or in equity.
- 4.17 **Effect of Termination of Agreement(s).** Upon the termination of the Base Agreement(s) or this BAA for any reason, Business Associate shall return all PHI created by Business Associate or received from Covered Entity to Covered Entity or, at Covered Entity's direction, destroy all PHI received from Covered Entity that Business Associate maintains in any form, recorded on any medium, or stored in any storage system. This provision shall apply to PHI that is in the possession of Business Associate, its agents and subcontractors. Business Associate shall retain no copies of the PHI and must certify destruction upon Covered Entity's request. Business Associate shall remain bound by the provisions of this BAA, even after termination of the Base Agreement(s) or BAA, until all PHI has been returned or otherwise destroyed as provided in this Section.

- 4.18 **Injunctive Relief.** Business Associate stipulates that its unauthorized use or disclosure of PHI while performing services pursuant to this BAA would cause irreparable harm to Covered Entity, and in such event, Covered Entity shall be entitled to institute proceedings in any court of competent jurisdiction to obtain damages and injunctive relief.
- 4.19 **Indemnification.** Business Associate shall indemnify and hold harmless Covered Entity and its officers, trustees, employees, agents, and subcontractors, from any and all claims, penalties, fines, costs, liabilities, or damages, including but not limited to reasonable attorney fees, incurred by Covered Entity arising from a violation by Business Associate of its obligations under this BAA.

## 5.0 OBLIGATIONS OF COVERED ENTITY

- 5.1 **Notice of Privacy Practices.** Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent such limitations affect Business Associate's use or disclosure of PHI.
- 5.2 **Revocation of Authorization of Individual.** Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, if and to the extent such changes affect Business Associate's use and disclosure of PHI.
- 5.3 **Restrictions on Use and Disclosure.** Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent such restriction may affect Business Associate's use or disclosure of PHI.

## 6.0 MISCELLANEOUS

- 6.1 **Third Party Rights.** The terms of this BAA do not grant any rights to any third parties.
- 6.2 **Independent Contractor Status.** For the purposes of this BAA, Business Associate is an independent contractor of Covered Entity, and shall not be considered an agent of Covered Entity.
- 6.3 **Changes in the Law.** The parties shall amend this BAA to conform to any new or revised legislation, rules, or regulations to which Covered Entity is subject now or in the future including, without limitation, HIPAA, HITECH, the Privacy Standards, Security Standards or Transactions Standards.
- 6.4 **Owner of PHI.** Under no circumstances shall Business Associate be deemed in any respect to be the owner of any PHI of Covered Entity.

This BAA becomes binding when signed by authorized representatives of both parties.

BUSINESS ASSOCIATE:

THE REGENTS OF THE UNIVERSITY OF MICHIGAN:

By: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_