

Rutgers University
HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement
Is Related To and a Part of the Following
Underlying Agreement:

Effective Date of Underlying Agreement: _____

School/Unit: _____

Vendor: _____

This HIPAA Business Associate Agreement (“Agreement”) is entered into as of the _____ day of _____, 20__ by and between (the “Covered Entity”) and _____ with an address of _____ (the “Business Associate”).

W I T N E S S E T H:

WHEREAS, the Covered Entity is required under the HIPAA Rules to obtain written assurances from a business associate that the business associate will appropriately safeguard protected health information (“PHI”) as defined under the HIPAA Rules; and

WHEREAS, the Business Associate recognizes and is willing to comply with the specific requirements imposed pursuant to the HIPAA Rules as required by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009, commonly known as the Health Information Technology for Economic and Clinical Health Act (“HITECH”) and the Omnibus Rule (2013); and

WHEREAS, the Covered Entity has or shall engage the Business Associate to provide services involving the use of PHI.

NOW, THEREFORE, in consideration of the premises, promises and mutual covenants contained herein and other good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually covenanted and agreed by and between Covered Entity and Business Associate as follows:

1. Definitions.

(a) General. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, PHI, Required By Law, Secretary, Security Incident, Subcontractor, and Unsecured PHI. Terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms are given when defined in the HIPAA Rules.

(b) Specific Definitions.

(i) Business Associate. Business Associate” shall generally have the same meaning as the term “business associate” at 45 C.F.R. §160.103, and in reference to the party to this Agreement, shall mean the Business Associate as first defined above.

(ii) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “the Covered Entity” at 45 C.F.R. §160.103, and in reference to the party to this Agreement, shall mean the Covered Entity as first defined above; provided, however, that in the event that same is otherwise a hybrid entity under the HIPAA Rules, that entity may appropriately designate a health care component of the entity, pursuant to 45 C.F.R. §164.105(a), as the Covered Entity for purposes of this Agreement.

(iii) HIPAA Rules: “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164.

(iv) Security Incident: 45 CFR § 164.304 defines “security incident” as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(v) Breach: “Breach” shall mean an impermissible use or disclosure which compromises the security or privacy of the Protected Health Information. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA Covered Entities and their Business Associates to provide notification of breach of Protected Health Information which has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology.

2. Obligations and Activities of Business Associate.

The Business Associate agrees to:

(a) Not use or disclose PHI other than as permitted or required by this Agreement or as Required By Law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

(c) Immediately report to the Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, but in no case later than three (3) business days, including Breaches of Unsecured PHI as required at 45 C.F.R. §164.410, and any Security Incident of which it becomes aware;

(ii) Upon discovery a Breach of Protected Health Information, Business Associate shall provide immediate verbal notification of the Breach to an appropriate representative of the Covered Entity such as the Covered Entity’s signatory to this agreement or to the Rutgers University Director of Privacy within the Office of Enterprise Risk Management, Ethics and Compliance. Business Associate shall also provide written notification of the Breach to the Covered Entity no later than five (5) days after discovery of the Breach, and the content of

such notice shall be consistent with 45 CFR § 164.410. If Business Associate has been requested orally or in writing by law enforcement officials that notification of affected individuals may impede a criminal investigation, Business Associate shall so inform the Covered Entity. Notwithstanding any other provision of this Agreement, Business Associate agrees to reimburse the Covered Entity for any and all reasonable expenses (e.g., cost of mailing, media, credit monitoring, etc.) incurred by the Covered Entity in carrying out the obligations of the Covered Entity under the HIPAA Rules to notify individuals affected by a Breach of Business Associate or its Subcontractor. In the alternative and upon agreement of the Parties, Business Associate may directly undertake all or parts of such obligations and expenses in lieu of the herein provided reimbursement.

(ii) Upon discovery of a Security Incident, Business Associate shall provide immediate verbal notification of the Security Incident to an appropriate representative of the Covered Entity such as the Covered Entity's signatory to this agreement or to the Rutgers University Director of Privacy within the Office of Enterprise Risk Management, Ethics and Compliance. Business Associate shall also provide written notification of the Security Incident to the Covered Entity no later than five (5) days after discovery of the Security Incident, and the content of such notice shall be consistent with that of breach notification at 45 CFR § 164.410. Notwithstanding any other provision of this Agreement, Business Associate agrees to reimburse the Covered Entity for any and all reasonable expenses (e.g., cost of mailing, media, credit monitoring, etc.) incurred by the Covered Entity in carrying out the obligations of the Covered Entity under the HIPAA Rules to notify individuals affected by a Security Incident of Business Associate or its Subcontractor. In the alternative and upon agreement of the Parties, Business Associate may directly undertake all or part of such obligations and expenses in lieu of the herein provided reimbursement.

(iii) Business Associate agrees to report to the Covered Entity within ten (10) days, any use or disclosure of PHI by the Business Associate or its Subcontractors not provided for by this Agreement of which it becomes aware.

(d) Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate, or a Subcontractor of Business Associate, in violation of the requirements of this Agreement;

(e) In accordance with 45 C.F.R. §§164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors (including, without limitation, independent contractors or agents, ("Subcontractor")) that create, receive, maintain, or transmit PHI on behalf of the Business Associate to agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such PHI. The Business Associate shall only be permitted to engage the use of a Subcontractor to perform or assist in the performance of the Services that involves use or disclosure of PHI to the Subcontractor or creation of PHI by the Subcontractor if approved in writing by the Covered Entity;

(i) Such agreement shall identify the Covered Entity as a third-party beneficiary with rights of enforcement in the event of any violations. If Business Associate discovers a material breach or violation of the agreement between itself and any Subcontractor, Business Associate must require the Subcontractor to correct the violation, or terminate said agreement.

(ii) With respect to electronic Protected Health Information, Business Associate shall ensure that any Subcontractor of Business Associate that creates, receives, maintains, or transmits electronic protected health information on behalf of 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.

(f) Make available PHI in a Designated Record Set to the Covered Entity or, as directed by the Covered Entity, to an individual as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. §164.524;

(i) Business Associate agrees to provide access to such PHI no later than thirty (30) days from the date on which the Covered Entity makes the request. Business Associate agrees to allow individuals to access PHI at Business Associate's offices, if directed to do so by the Covered Entity.

(ii) Business Associate agrees, upon the request of the individual, to provide such individual with a copy of his or her Electronic Health Record in electronic format.

(g) Make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. §164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. §164.526;

(i) Except for good cause shown in writing to the Covered Entity, Business Associate shall act upon the Covered Entity's request for an amendment within fifteen (15) days of receipt of the Covered Entity's request.

(h) Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. §164.528;

(i) To the extent the Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s);

(j) Make its internal practices, books, and records available to the Secretary of DHHS for purposes of determining compliance with the HIPAA Rules;

(k) In the event the Business Associate receives a request from an Individual in connection with any of such Individual's PHI (whether a request for access, amendment, accounting of disclosures or any other request of any nature or description), the Business Associate shall immediately notify the Covered Entity of such request and cooperate with the Covered Entity's instructions in responding to such request;

(l) The Business Associate shall immediately cooperate with the Covered Entity to amend, restrict or change any use or disclosure of any Individual's PHI in the Business Associate's control or within the control of a Subcontractor; and

(m) That it will, at such time and in such manner as directed by the Covered Entity, implement and use such technologies and methodologies, including without limitation, Encryption and

Destruction, which the Secretary of DHHS identifies from time to time as rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

3. Permitted Uses and Disclosures by Business Associate.

(a) Since the Business Associate is or shall provide services as necessary to perform its obligations to the Covered Entity [as set forth in _____ (the “Services Agreement”)] (“Services”) that may involve the receipt, creation, or other uses of any nature or description of PHI, the Business Associate agrees, except as otherwise provided in this Agreement, only to use or disclose PHI as necessary to perform the Services for the Covered Entity.

(b) The Business Associate may use or disclose PHI as Required by Law.

(c) The Business Associate agrees to make uses and disclosures and requests for PHI consistent with the Covered Entity’s Minimum Necessary policies and/or procedures.

(d) The Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity except for the specific uses and disclosures set forth below in subsection (e).

(e) The Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are Required By Law, or the Business Associate obtains the following: (i) written approval from the Covered Entity; and (ii) reasonable assurances from the person to whom the PHI is disclosed that (A) the PHI 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 (B) the person will immediately notify the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been Breached.

(f) Business Associate may provide Data Aggregation services relating to the Health Care Operations of the Covered Entity if requested by the Covered Entity in writing.

(g) The Business Associate shall not use de-identified PHI in any manner without the express written authorization of the Covered Entity.

4. Indemnification. Business Associate shall defend, indemnify and hold Covered Entity and Covered Entity's owners, governors, trustees, shareholders, members, partners, directors, managers, officers, employees, agents, representatives, successors and assigns (collectively, the "Covered Entity Parties") harmless from and against any and all claims, demands, losses, expenses, costs, obligations, damages, liabilities, of any nature or description including, without limitation, interest, penalties and reasonable attorney’s fees which the Covered Entity Parties may incur, suffer or sustain, which arise, result from or relate to any breach of or failure by Business Associate or a Subcontractor to perform any of such party’s representations, warranties, covenants or agreements under this Agreement. The obligations of Business Associate under this Section shall survive termination of this Agreement.

5. Term and Termination.

(a) Term. The term of this Agreement shall be effective as of the date first written above, 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 the termination provisions in this Section 5..

(b) Termination by Covered Entity. The Business Associate authorizes termination of this Agreement by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of this Agreement and the Business Associate has not immediately cured the breach and ended the violation.

(c) Termination by Business Associate. Business Associate may terminate this Agreement without penalty provided that: (i) it knows of a pattern of activity or practice of Covered Entity that constitutes a material breach or violation of this Agreement; (ii) it notifies Covered Entity in writing of the material breach or violation; (iii) within forty-five (45) days after receipt of such notice, Covered Entity does not cure the breach or end the violation; and (iv) the parties mutually agree in writing that termination of this Agreement is feasible in light of relevant factors such as the nature and scope of Business Associate's obligations. If the parties determine that termination is not feasible pursuant to the foregoing, then Business Associate may report the material breach or violation to the Secretary in writing, provided that no less than fifteen (15) days before such notification is given, Business Associate furnishes Covered Entity with a copy of the proposed report, and if Covered Entity elects to prepare a written explanation or statement, Business Associate encloses same as part of its submission to the Secretary.

(d) Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, the Business Associate, with respect to PHI received from the Covered Entity, or created, maintained, or received by the Business Associate on behalf of the Covered Entity, shall:

(i) Retain only that PHI which is necessary for the Business Associate to continue its proper management and administration or to carry out its legal responsibilities as approved by the Covered Entity in writing after the Covered Entity has an opportunity to consider whether any PHI must be reasonably retained by the Business Associate for such purposes;

(ii) Return to the Covered Entity or, if agreed to by the Covered Entity in writing, destroy the remaining PHI that the Business Associate and/or any Subcontractors still maintain in any form;

(iii) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as the Business Associate retains any PHI as approved by the Covered Entity in writing;

(iv) Not use or disclose the PHI retained by the Business Associate (and ensure that any Subcontractors agree to also not use or disclose) other than for the purposes for which such PHI was retained and subject to the same conditions set forth above in subsection (i) above

and in accordance with all protections and restrictions on the use and disclosure of PHI as contained in this Agreement; and

(v) Return to the Covered Entity (or, if agreed to by the Covered Entity in writing, destroy the PHI) retained by the Business Associate when it is no longer needed by the Business Associate for its proper management and administration or to carry out its legal responsibilities.

(vi) Notwithstanding any other provisions contained in this Agreement to the contrary, the Business Associate agrees to transmit the PHI to another business associate of the Covered Entity at termination.

(vii) The Business Associate further agrees that any permitted Subcontractor complies with all of the Business Associate's obligations set forth in this Agreement, including, without limitation, the obligations contained in this Section 5.

(e) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

6. No Third Party Rights.

Except as expressly provided in Section 2(e)(i) above, nothing in this Agreement, expressed or implied, is intended or shall be construed to confer upon or give to any person, firm, corporation, association, or legal entity other than the parties, any rights, remedies or other benefits under or by reason of the Agreement. Accordingly, no third party shall have the right to enforce the provisions of the Agreement or any other document relating to this Agreement.

7. Miscellaneous.

(a) Amendment. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event a party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Rules, such party so shall notify the other party in writing. For a period of up to thirty (30) days, the parties shall address in good faith such concern and shall amend the terms of this Agreement if necessary to bring it into compliance. If after such thirty (30) day period the terms and conditions of this Agreement fail to comply with the HIPAA Rules with respect to the concern(s) raised pursuant to this Agreement, then either party has the right to terminate this Agreement upon written notice to the other party.

(b) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

(d) Notices. Any notice to be given under this Agreement to a party shall be made via U.S. Mail, commercial courier or hand delivery to such party at its address given above, or to such

other address, as shall hereafter be specified by notice from the party. Any such notice shall be deemed given when so delivered to or received at the proper address.

(e) Assignment. This Agreement applies to the Services being provided by Business Associate and may not be assigned without the written consent of Covered Entity. An agreement with a Subcontractor that complies with the requirements of this Agreement shall not be an assignment for the purposes of this Agreement.

(f) Governing Law; Venue. This Agreement shall be governed by, construed, interpreted and enforced under the laws of the State of New Jersey, without regard to its choice of law provisions. The parties hereby consent to the jurisdiction and venue of the state and federal courts located in Middlesex County, New Jersey.

The parties hereto have set their hands and seals the day and year written above.

COVERED ENTITY: _____

Signature

Print Name: _____

Title: _____

Contact Phone Number: _____

BUSINESS ASSOCIATE: _____

Signature

Print Name: _____

Title: _____

Contact Phone Number: _____