

## BUSINESS ASSOCIATE AGREEMENT

**THIS BUSINESS ASSOCIATE AGREEMENT (“BAA”)** is entered into between:

**[Insert Name and Address of Business Associate Here]** (hereinafter referred to as “Covered Entity”),

and

**Rutgers, The State University of New Jersey (“Rutgers”)**, an instrumentality of the State of New Jersey, a public entity, with offices at Winants Hall, 7 College Avenue, New Brunswick, NJ 08901, for itself and on behalf of its organizational unit, **Rutgers Biomedical and Health Sciences (“RBHS”)**, and the unincorporated constituent units therein. Individually and together, Rutgers and RBHS, and all of their other present and future Affiliates, are collectively, “Business Associate”,

(The Covered Entity and Business Associate hereinafter each a “Party” and collectively the “Parties”).

- A. **WHEREAS**, Covered Entity and Business Associate have entered into the Services Agreement (as defined below) under which Business Associate has been engaged to perform a function or service for or on behalf of Covered Entity;
- B. **WHEREAS**, in connection with the Services Agreement, the Covered Entity discloses to Business Associate certain Protected Health Information (“PHI”) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act (Title XIII of the American Recovery and Reinvestment Act of 2009) (the “HITECH Act”), and regulations promulgated by the U.S. Department of Health and Human Services (the “HHS”) (hereinafter the “HIPAA Regulations” and the “HITECH Regulations,” respectively) and/or applicable state and/or local laws and regulations;
- C. **WHEREAS**, in connection with the Services Agreement, Business Associate accesses, uses and/or discloses individually identifiable health information, including PHI, as part of performing said services, or otherwise performs a function that is subject to protection under HIPAA, the HITECH Act, the HIPAA regulations and/or the HITECH regulations;
- D. **WHEREAS**, HIPAA requires that Covered Entity receive adequate assurances that Business Associate will appropriately safeguard PHI that has been or will be used or disclosed in the course of providing services to or on behalf of Covered Entity; and

E. **WHEREAS**, the purpose of this BAA is to comply with the requirements of HIPAA, the HITECH Act, the HIPAA regulations and/or the HITECH regulations;

**NOW THEREFORE**, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Definitions. Terms used in this BAA but not otherwise defined herein shall have the meaning ascribed to those terms in HIPAA, the HITECH Act, and any current or future regulations promulgated under HIPAA and/or the HITECH Act. *See* 45 C.F.R. §§ 160.103, 164.402 and 164.501.
  - 1.1. “Services Agreement” means any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to Covered Entity which involve the use or disclosure of PHI, and all such agreements shall be collectively referred to as the “Services Agreement.” Each Services Agreement is amended by and incorporates the terms of this BAA.
2. Permitted Uses and Disclosures of PHI by Business Associate.
  - 2.1. Except as otherwise limited in this BAA or in the Services Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Services Agreement, provided that such uses and/or further disclosures (i) do not violate the requirements of HIPAA’s Business Associate contract standard at 45 C.F.R. § 164.504(e)(1) and/or the HITECH Act, if done by the Covered Entity, (ii) are the minimum necessary PHI to accomplish the intended purpose, or (iii) are Required By Law.
  - 2.2. Except as otherwise limited in this BAA or in the Services Agreement, Business Associate may use or disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate, provided, however, that any such uses or disclosures are Required By Law, or Business Associate obtains reasonable written assurances from the person to whom the information is disclosed that (i) the PHI 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 (ii) the person immediately notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been the subject of a Breach.
  - 2.3. Except as otherwise limited in this BAA or in the Services Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity, consistent with 45 C.F.R. § 164.504(e)(2)(i)(B).
  - 2.4. Business Associate may use PHI to report violations of law to appropriate federal and state authorities as required under HIPAA and/or other federal and state laws, consistent

with 45 C.F.R. § 164.502(j)(1), provided that Business Associate gives Covered Entity prior written notice of its intention to report any such violation of law and the facts or circumstances related thereto, to the extent legally permissible.

3. Duties and Obligations of Business Associate Related to PHI.

- 3.1. Business Associate shall not use or disclose PHI other than as permitted or required by the Services Agreement, this BAA, and/or as Required By Law. Business Associate shall comply with the provisions of this BAA relating to privacy and security of PHI and all present and future provisions of HIPAA, the HITECH Act and HIPAA Regulations that relate to the privacy and security of PHI and that are applicable to Covered Entity and/or Business Associate.
- 3.2. Business Associate shall use and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PHI and/or Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity, including implementing requirements of 45 C.F.R. Part 164 Subpart C with regard to Electronic PHI.
- 3.3. Business Associate agrees to promptly report in writing to Covered Entity any use or disclosure of PHI not permitted by this BAA, as well any Security Incident, of which Business Associate becomes aware. The Parties agree that this paragraph constitutes notice by Business Associate to Covered Entity, and no further notice shall be required with respect to the ongoing occurrence of attempted but unsuccessful Security Incidents including, but not limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, attempts to log on a system or enter a database with an invalid password or username, and denial-of-services attacks that do not result in a server being taken off-line, provided that such do not result in actual unauthorized access, use, disclosure, modification or destruction of PHI or interference with an information system.
  - 3.3.1. Notwithstanding the foregoing, Business Associate shall maintain and make available to Covered Entity upon reasonable request an accounting of unsuccessful Security Incidents, including the dates the unsuccessful Security Incident occurred and was discovered; the nature of the unsuccessful Security Incident; an explanation as to why the unsuccessful Security Incident was unsuccessful; and, a description of any improvements or safeguards implemented as a result of the unsuccessful Security Incident.
- 3.4. Business Associate agrees to promptly, without unreasonable delay, and in no event more than three (3) business days after discovery, notify Covered Entity following the discovery of a Breach of Unsecured PHI. A Breach is considered "discovered" as of the first day on which the Breach is known, or reasonably should have been known, to Business Associate or any employee, officer, Subcontractor, or agent of Business Associate, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured PHI shall include (to the extent reasonably known) the

identification of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Security Incident or Breach as well as any other information that the Covered Entity is required to include in the notice to affected Individuals under 45 C.F.R. § 164.404(c), either at the time of notice of Breach to the Covered Entity or as promptly thereafter as information becomes available.

- 3.5. Business Associate is subject to the same legal requirements to cure, terminate or report violations to the Secretary of HHS, and in the same manner, as Covered Entity.
- 3.6. Business Associate shall not 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 unless otherwise approved in writing in advance by the Covered Entity. Business Associate shall ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such PHI.
  - 3.6.1. 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.
- 3.7. Business Associate agrees to mitigate, to the extent practicable, any harmful effect to Covered Entity that is known to Business Associate of a Breach of PHI by Business Associate or its employees, officers, Subcontractors, or agents in violation of the requirements of this BAA (including, without limitation, any Security Incident or Breach of Unsecured PHI). Business Associate agrees to reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this BAA and/or any Security Incident or Breach. Business Associate shall also reasonably cooperate and coordinate with Covered Entity in the preparation of any reports or notices to the Individual, a regulatory body or any third party required to be made under HIPAA, HIPAA Regulations, the HITECH Act, or any other federal or state laws, rules or regulations, provided that any such reports or notices shall remain the obligation of Covered Entity.
- 3.8. Business Associate shall ensure that any agent, including a Subcontractor, to whom it provides PHI (i) received from, or (ii) created or received by Business Associate on behalf of, a Covered Entity agrees, in writing, to the same restrictions, conditions and requirements that apply through this BAA to Business Associate with respect to such PHI 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 Covered Entity.

- 3.9. Upon reasonable request, Business Associate shall provide Covered Entity access to its premises for a review and demonstration of its internal practices and procedures for safeguarding PHI and Electronic PHI.
- 3.10. Within three (3) business days following request, Business Associate shall provide Covered Entity with an accounting of uses and disclosures of PHI provided to it by Covered Entity.
- 3.11. To the extent that Business Associate possesses or maintains PHI in a Designated Record Set, Business Associate agrees to provide access, at the reasonable request of Covered Entity, and in the time and manner designated by the Covered Entity during normal business hours, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under the HIPAA Regulations. If an Individual makes a request for access to PHI directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act (42 U.S.C. § 17935(e)).
- 3.12. To the extent that Business Associate possesses or maintains PHI in a Designated Record Set, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to HIPAA Regulations at the request of Covered Entity or an Individual. If an Individual makes a request for an amendment to PHI directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.
- 3.13. Business Associate agrees to use, disclose and request (i) only the minimum necessary PHI to carry out the intended purpose of the use or disclosure, as defined by law, and (ii) to the extent practicable, only the limited data set of PHI excluding direct identifiers, as defined in 45 C.F.R. § 164.514(e)(2).
- 3.14. Business Associate shall document disclosures of PHI 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 PHI (45 C.F.R. § 164.528). Should Covered Entity request an accounting of disclosures of PHI pursuant to 45 C.F.R. § 164.528, Business Associate agrees to promptly provide Covered Entity with information in a format and manner sufficient to respond no later than ten (10) days after receipt of such request, subject to specific statutory exceptions, 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 of the individual, if and to the extent that such accounting is required under the HITECH or HITECH Regulations. In the event any Individual or Personal Representative requests

access to the Individual's PHI directly from Business Associate, Business Associate shall, within ten (10) business days, forward that request to Covered Entity. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a Personal Representative, and compliance with the requirements applicable to an Individual's right to obtain access to PHI, shall be the sole responsibility of the Covered Entity.

- 3.15. Business Associate shall make its internal practices, books and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, available to Covered Entity at the request of Covered Entity, or the Secretary of HHS, for purposes of the Secretary determining Covered Entity's compliance with HIPAA and/or the HITECH Act in the time, manner and place designated by the Covered Entity and/or the Secretary.
- 3.16. Business Associate agrees to abide by the limitations on marketing communications to Individuals regarding the purchase and use of products or services, which are set forth in the HITECH Act and the HITECH Regulations.
- 3.17. Business Associate agrees and acknowledges that the administrative rules governing, and the civil and criminal penalties for violating, HIPAA, the HITECH Act, the HIPAA Regulations and the HITECH Regulations, apply to it in the same manner as they apply to Covered Entity.
- 3.18. To the extent, if any, that Business Associate agrees to carry out one or more of Covered Entity's obligation(s) under 45 CFR Part 164, Subpart E, then Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
- 3.19. Except as necessitated by occasional travel outside of the United States by Business Associate's employees, Business Associate agrees not to share, store, or in any way allow the transmission of PHI outside of the United States without the express advance written permission of Covered Entity or otherwise permit a Subcontractor to do so.
- 3.20. To the extent that Business Associate's workforce will have access to Covered Entity's PHI, Business Associate shall appropriately train such workforce members in HIPAA and related responsibilities and obligations with respect to accessing and using Covered Entity's PHI under this Agreement.

#### 4. Term and Termination.

- 4.1. Term. The term of this BAA shall be effective as of the effective date of the Services Agreement 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 of this Section 4.

4.2. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- 4.2.1. Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this BAA and the Services Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
- 4.2.2. Immediately terminate this BAA and/or the Services Agreement if Business Associate has breached a material term of this BAA and cure is not possible; or
- 4.2.3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of HHS.

4.3. Effect of Termination.

- 4.3.1. Except as provided in Section 4.3.3, upon termination of this BAA, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of PHI.
- 4.3.2. Except as provided in Section 4.3.3, if Covered Entity, in its sole discretion, requires that Business Associate destroy any or all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, either due to the termination of this BAA or otherwise, Business Associate shall certify, in writing, to Covered Entity that the PHI has been destroyed and rendered indecipherable, pursuant to HIPAA and the HITECH Act. This provision also shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate.
- 4.3.3. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible within thirty (30) calendar days of such request. In such case, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. This provision also shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate.
- 4.3.4. Should the Business Associate make a disclosure of PHI in violation of this BAA, Covered Entity shall have, in addition to all other legal and equitable remedies

available to Covered Entity, the right to immediately terminate any contract, other than this BAA, then in force between the Parties, including the Services Agreement.

4.3.5. The provisions of this Section 4.3 shall survive the termination of this BAA and the Services Agreement for any reason.

## 5. Remedies.

5.1. Business Associate shall defend, indemnify and hold Covered Entity and its trustees, directors, officers, employees, students, faculty and agents (collectively, the “Covered Entity Parties”) harmless from and against any and all claims, demands, losses, obligations, damages, liabilities, expenses, costs and fines (including costs of investigation, notification and remediation), 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 or to any failure by Business Associate or a Subcontractor to perform any of its or their covenants, duties, obligations and assurances under this BAA. The obligations of Business Associate under this Section shall survive termination of this BAA.

5.2. Business Associate agrees and acknowledges that irreparable harm will result to Covered Entity and to its business in the event of any Breach or which result from or relate to any failure by Business Associate or a Subcontractor to perform any of its or their covenants, duties, obligations and assurances under this BAA (individually and collectively, “breach”) and further agrees that remedy at law for any such breach shall be inadequate and that damages resulting therefrom are not susceptible to being measured in monetary terms. In the event of any such breach or threatened breach by Business Associate, Covered Entity shall be entitled to (i) immediately enjoin and restrain Business Associate from any continuing violations and (ii) reimbursement for reasonable attorneys’ fees, costs and expenses incurred as a proximate result of the breach. The remedies in this Section 5 shall be in addition to any action for damages and/or other remedy available to Covered Entity for such breach.

5.3. Business Associate agrees to carry insurance covering Breach response, investigation, notification and remediation in an amount of not less than five million dollars (\$5,000,000).

5.4. Covered Entity shall not be liable to Business Associate for any claim, loss, or damage relating to Business Associate’s use or disclosure of any information received from Covered Entity or from any other source.

6. Electronic Transaction Standards. To the extent that Business Associate or its products perform all or part of any transaction for which the Secretary has adopted a standard under HIPAA (“Covered Transactions”) on the Covered Entity’s behalf, the following shall apply:



- 6.1. Compliance with HIPAA Standards. When providing its services and/or products, Business Associate shall comply with all applicable HIPAA standards and requirements (including, without limitation, those specified in 45 CFR Part 162) with respect to the transmission of health information in electronic form in connection with any Covered Transactions. Business Associate will make its services and/or products compliant with HIPAA's standards and requirements no less than thirty (30) days prior to the applicable compliance dates under HIPAA. Business Associate represents and warrants that it is aware of all current HIPAA standards and requirements regarding Covered Transactions, and Business Associate shall comply with any modifications to HIPAA standards and requirements which become effective from time to time. Business Associate agrees that such compliance shall be at its sole cost and expense, which expense shall not be passed on to Covered Entity in any form, including, but not limited to, increased fees.
- 6.2. Agents and Subcontractors. Business Associate shall require all of its agents and Subcontractors (if any) who assist Business Associate in providing its services and/or products to comply with all applicable requirements of HIPAA, including without limitation, compliance with 45 CFR Part 162.
7. Miscellaneous.
- 7.1. Independent Contractor. None of the provisions of this BAA and/or the Services Agreement are intended to create nor shall be deemed or construed to have created any relationship between the Parties other than that of independent entities contracting with each other unless otherwise explicitly stated in this BAA or the Services Agreement.
- 7.2. Detrimental Reliance by Covered Entity. Business Associate agrees and acknowledges that its covenants, duties, obligations and assurances herein shall be detrimentally relied upon by Covered Entity in choosing to commence or continue a business relationship with Business Associate.
- 7.3. Regulatory References. Any reference herein to law means the law as in effect or as amended.
- 7.4. Construction. The BAA shall be construed broadly and any ambiguity shall be resolved in favor of a meaning that complies and is consistent with applicable law.
- 7.5. Severability. In the event that any provision of this BAA violates any applicable statute, ordinance or rule of law in any jurisdiction that governs this BAA, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this BAA.
- 7.6. Authority. The signatories below have the right and authority to execute this BAA for their respective entities and no further approvals are necessary to create a binding agreement.

- 7.7. Compliance with State Law. Business Associate acknowledges and agrees that as the holder of individually identifiable health information received from or created for Covered Entity, Business Associate is subject to New Jersey law. In the event of any conflict between HIPAA and New Jersey law, Business Associate shall comply with the more restrictive provision.
- 7.8. Choice of Law and Venue. This BAA, and all claims or causes of action that may be based upon, arise out of or relate to this BAA, shall be governed by and enforced in accordance with the internal laws of the State of New Jersey, including its statutes of limitations and without reference to its conflicts of laws principles. The Parties further agree that any and all claims arising under this BAA, or related thereto, shall be heard and determined either in the courts of the State of New Jersey with venue in the Middlesex County vicinage or in the federal courts located in New Jersey.
- 7.9. Conflict Among Contracts. Should there be conflict between the terms of this BAA and any other agreement between the Parties (either previous or subsequent to the date of this BAA), the terms of this BAA shall control.
- 7.10. Modification. This BAA may only be modified by a writing signed by the Parties. The Parties agree to take such action subsequent to this BAA as necessary to amend the BAA from time to time as necessary for the Parties to comply with the requirements of any applicable law.
- 7.11. Assignment. Neither Party shall directly or indirectly assign or otherwise transfer this Agreement, or any interest herein or obligation hereunder, without the prior written consent of the other party. Notwithstanding the foregoing, a corporate reorganization of the clinical operations of Rutgers, which results in the clinical operations of Rutgers being transferred to an affiliate, or an entity controlled by or under common control with, or in an organized health care arrangement with Rutgers, shall not require approval of Business Associate.
- 7.12. No Third Party Beneficiaries. Except as expressly provided in Section 3.6.1 above, this BAA is made solely for the benefit of the Parties and their affiliates, successors and assigns and no other person or entity shall have any right, benefit or interest under or because of this BAA.
- 7.13. Notices to Parties. All notices, requests, approvals, demands, and other communications required or permitted to be given under this BAA will be in writing and will be deemed to have been duly given when (a) delivered personally or (b) if sent via USPS/FedEx/UPS (or similar courier service) then as evidenced by a delivery receipt or tracking report, addressed as follows or to such other address as either Party may designate by notice to the other Party:

To the Covered Entity:

[Insert name/address here]

To the Business Associate:

Rutgers Procurement Services

With a copy to:

Director of Procurement  
33 Knightsbridge Road, East Wing  
Piscataway, NJ 08854  
With a copy to:

Rutgers University Ethics and Compliance  
Director of Privacy  
335 George Street, Suite 2100  
New Brunswick, NJ 08901

*Remainder of page intentionally left blank.  
Signature page follows.*

**IN WITNESS WHEREOF**, the Parties have executed this Business Associate Agreement as of the last date written below.

**[INSERT NAME HERE]  
[COVERED ENTITY]**

**RUTGERS, THE STATE UNIVERSITY  
OF NEW JERSEY  
[BUSINESS ASSOCIATE]**

\_\_\_\_\_  
Name:  
Title:  
  
Date: \_\_\_\_\_

\_\_\_\_\_  
Name:  
Title:  
  
Date: \_\_\_\_\_

*Signature Page for Business Associate Agreement*