RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Disclosures of Personally Identifiable Health Information to Business Associates					
Section #:	100.1.10	**Section Title:**	HIPAA Policies		**Formerly Book:**	00-01-15-40:00
Approval Authority:	RBHS Chancellor/Executive Vice President for Health Affairs		**Adopted:**	3/8/2016	**Reviewed:**	3/8/2016
Responsible Executive:	Senior Vice President and Chief Enterprise Risk Management, Ethics and Compliance Officer		**Revised:**			
Responsible Office:	Office of Enterprise Risk Management, Ethics and Compliance		**Contact:**	Office of Enterprise Risk Management, Ethics and Compliance: 973-972-8093		

1. **Policy Statement**
   To ensure compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA), including the HITECH Act (2009), the Omnibus Rule (2013) and related state and federal law, in relation to disclosures of Protected Health Information (PHI) and to entering into contracts with Business Associates**.**

2. **Reason for Policy**
   This policy shall apply to disclosures to Business Associates of Protected Health Information (PHI) generated during provision of health care, healthcare payment or treatment to patients in:

   I. The Rutgers Covered Entity and Covered Components within that entity, including faculty, employees, students, volunteers, trainees, and other persons whose conduct, in the performance of work for Rutgers and/or its units, is under the direct control of the Rutgers Covered Entity, whether or not they are paid by Rutgers.

   II. Any Rutgers University workforce member of any Rutgers school, unit or department that bills federal and/or state programs for the provision of medical care to patients, or engages in human subject research sponsored by federal, state or private programs.

   III. Other University departments that assist the Rutgers Covered Entity in certain activities including, but not limited to, the Office of Enterprise Risk Management, Ethics and Compliance, the Office of Information Technology and the Office of the Senior Vice President and General Counsel.

3. **Who Should Read this Policy**
   Those responsible for engaging the services of a Business Associate and/or the negotiation, approval and/or oversight of agreements between the University and Business Associates, as defined by this policy.

4. **Resources**

   I. 45 CFR 160.103(a), Code of Federal Regulations, Title 45, Part 164, Section 103, Subpart A, General Administrative Requirements, General Provisions, Definitions

II. 45 CFR 164.501(e), Code of Federal Regulations, Title 45, Part 164, Section 501, Subpart E, Security and Privacy, Definitions, Privacy of Individually Identifiable Health Information

III. 45 CFR 164.502(e), Code of Federal Regulations, Title 45, Part 164, Section 502, Subpart E, Security and Privacy, Uses and Disclosures of Protected Health Information: General Rules, Privacy of Individually Identifiable Health Information

IV. 45 CFR 164.504(e), Code of Federal Regulations, Title 45, Part 164, Section 504, Subpart E, Security and Privacy, Uses and Disclosures: Organizational Requirements, Privacy of Individually Identifiable Health Information

V. 45 CFR 164.532 (d) and (e), Code of Federal Regulations, Title 45, Part 164, Section 532, Subpart E, Security and Privacy, Uses and disclosures: Organizational requirements, Privacy of Individually Identifiable Health Information and (d) Standard: Effect of Prior Contracts or Other Arrangements with Business Associates

VI. 45 CFR 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule January 25, 2013

VII. Uses and Disclosures of Health Information With and Without an Authorization 100.1.1

VIII. The following policy provides additional and related information: Standards for Privacy of Individually Identifiable Health Information 100.1.9

IX. OCR HIPAA breach definition: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

5. **Definitions**

I. Protected Health Information (PHI): Protected health information means individually identifiable health information that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual and identifies or could reasonably be used to identify the individual.

A. Except as provided in paragraph two (2) of this definition that is: a) transmitted by electronic media; b) maintained in electronic media; or c) transmitted or maintained in any other form or medium.

B. Protected health information excludes individually identifiable health information in: a) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; b) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and c) Employment records held by a covered entity in its role as employer.

C. Relevant individually identifiable health information of deceased individuals should be considered active PHI for 50 years after death.

II. Business Associate: A business associate is any organization (an individual person can be an organization, e.g. an independent consultant) that creates, receives, maintains, or transmits PHI on behalf of a covered entity (CE), including but limited to the following:

A. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing; or

B. Any other function or activity regulated by HIPAA regulations; or

C. Provides legal, actuarial, accounting, auditing, consulting, data aggregation (as defined in CFR § 164.501), management, administrative, accreditation, or financial services to or for Rutgers and/or its units, or to and/or for an organized health care arrangement in which Rutgers and or its units participate, where the provision of the service involves the disclosure of individually identifiable health information from such entities or arrangement, or from another Business Associate of such entities or arrangement, to the person.

III. Workforce: Faculty, employees, students, volunteers, trainees, and other persons whose conduct, in the performance of work for Rutgers and/or its units, is under the direct control of the Rutgers Covered Entity, whether or not they are paid by Rutgers.

IV. HITECH ACT (2009): Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was enacted on February 17, 2009.

V. HIPAA Omnibus Rule (2013): Enhancements to the HIPAA Privacy, Security, Enforcement and breach notification rules under HITECH and GINA. 45 CFR parts 160 and 164. See Federal Register, Vol 78 (17), Friday, January 25, 2013.

VI. Covered Entity (CE): Either A (1) A health care provider, (2) a health plan or (3) a health care clearinghouse who transmits any health information in electronic form in connection with a transaction covered by 45 CFR 160.103. Covered Entities must comply with the HIPAA regulation, including the HITECH Act (2009), the Omnibus Rule (2013) and related state and federal law.

VII. Rutgers Covered Entity: The collective term referring to all units, schools or departments that meet the definition of a Covered Entity as put under 45 CFR 160.103 and are required to follow HIPAA regulation, including the HITECH Act (2009), the Omnibus Rule (2013) and related state and federal law.

VIII. Rutgers Covered Component: Refers to a single unit, school or department within the Rutgers Covered Entity.

IX. HIPAA Breach: An impermissible use or disclosure that 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 that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology.

6. **The Policy**

I. Requirements:

A. Rutgers and/or its units may only allow an individual or entity that is not part of its workforce that provides certain services to Rutgers and/or its units, or performs a function or activity on its behalf, to create or receive PHI without an authorization if the individual or entity:

1. Meets the definition of a business associate as described above, and
2. Enters into a written business associate contract with Rutgers that meets the elements in 45 CFR 164.504(e).

B. To determine whether the person or entity is required to enter into a business associate contract, use the following guidelines with the attached flowchart (EXHIBIT B):

1. No contract is needed with members of the workforce as defined in the definition. An independent contractor may be considered a member of the workforce if Rutgers exercises

supervision and control over the person as it would if the independent contractor was an employee.

2. A contract is necessary with persons who meet the definition of a business associate. (Since business associates access PHI without obtaining authorizations from the individuals to whom the PHI pertain, it is important that units do not inappropriately classify a person as a business associate and therefore fail to obtain the required authorization).

3. A business associate is someone who does the following:

   a. Performs or assists in the performance of a function or activity on behalf of Rutgers and/or its units including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, re-pricing, and any other function regulated by 45 CFR 164.504.

      For examples see EXHIBIT A for a list of specific types of persons, entities, and services that may qualify as a business associate provided that they meet all the elements discussed in this policy and procedure (i.e. the person will perform a function on behalf of Rutgers that is not for the purposes of treatment only, etc.).

   b. Provides legal, auditing, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, paper recycling, shredder companies, transcription services, record copy services, offsite storage, information technology (IT) services where confidentiality, integrity or availability of ePHI is at risk, including software/hardware support of computing medical devices, and/or application services such as email, web or database services or financial services for Rutgers.

4. Under the Final Rule, include Health information organizations, Health information exchanges, e-prescribing gateways and vendors of personal health records

   a. Researchers - When outside researchers receive PHI for research purposes and in accordance with Rutgers policies, a BAA is not required. Certain disclosures, even if made solely in the general context of research, may nonetheless require a BAA if the recipient of the information is using or disclosing the information to perform a function or activity regulated by the privacy rule.

   b. Financial Transactions - No business associate agreement is required with a financial institution if it only processes consumer-conducted financial transactions in payment for health care.

      For example, a bank that processes credit or debit card transactions or clears checks for a faculty practice plan would not be considered a business associate. Although some PHI of the patient is disclosed to a financial institution in this example, such as the patient's identity and perhaps some health information (e.g., the procedure performed), these facts do not create a business associate relationship because the bank is not acting on behalf of the faculty practice plan in performing its functions. The faculty practice plan is not in the business of directly processing credit card transactions or cashing checks.

   c. No contract is needed when the person or entity's function or service does not involve the use and disclosure of PHI, and where access to PHI by such persons would be *de minimus* or incidental, if at all.

      For example, it is not required that Rutgers enter into a contract with janitorial services, waste disposal of sealed materials, or equipment repair because the performance of such services does not involve the use and disclosure of PHI. I n this case, any incidental contacts or disclosures are permitted under the federal privacy laws as an incidental disclosure, provided that reasonable safeguards are in place to prevent such disclosures.

d. No contract is needed with another healthcare provider when the use or disclosure of the PHI is for treatment purposes.

i. If the relationship between the healthcare providers also includes involvement of PHI for operational or payment purposes, then a contract is necessary.

Examples: A physician, outside the workforce, serves as a medical director, or provides quality assurance or utilization management services through participation in hospital committees.

ii. For the definition and examples of the term treatment, payment, operations see EXHIBIT C.

No contract is needed when another entity serves as conduits of PHI/EPHI (ie. Post offices, Package delivery companies, and internet service providers)

e. If it is unclear as to whether the business associate definition has been met or if it is met, whether a contract is necessary, contact the Office of General Counsel for assistance. Generally, if it continues to be unclear as to whether there is a business associate relationship, no information should be shared with the person or entity without the patient's authorization.

II. Responsibilities

A. Documentation of Business Associate Agreement

Rutgers and its units will document the satisfactory assurances of protecting health information by the business associate through a written contract that meets the applicable requirements of the Health Insurance and Portability and Accountability Act (HIPAA), 45 CFR 164.504(e) and 164.308(b).

All Rutgers units must assure that the individuals and entities identified above agree in writing to the provisions in the attached business associate contract prior to engaging their services or allowing them to encounter any PHI. See EXHIBIT D. Exceptions have to be negotiated with and approved by the Office of Enterprise Risk Management, Ethics and Compliance.

B. Disclosure of Protected Health Information

Rutgers and its units may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf, if satisfactory assurances are obtained that the business associate will appropriately safeguard the information.

C. Responsibility of Individuals Authorized to Contract for Rutgers

Any individual authorized to contract for Rutgers, or who enters into any form of relationship on behalf of Rutgers in which PHI is exchanged or in which another entity has access to PHI other than a relationship with another treating provider relating to the treatment of patients, is responsible to obtain satisfactory assurances of protecting health information through the approved business associate contracting process and with the approved business associate contract. Failure to meet this responsibility is subject to disciplinary action up to and including termination and/or dismissal.

Rutgers and its units must require business associates to return or destroy all PHI in its possession at the termination of the contract when feasible and permitted by law.

For purposes of internal monitoring of compliance with this policy, all units must maintain a log of all arrangements with parties providing business associate services. The above log must be kept at the unit and a copy provided to the Rutgers' Privacy Officer. The log shall include, but not be limited to:

1. The name of the business associate and the name of any subcontractor(s) utilized by the business associate to provide the service.

2. The type of services provided to Rutgers, or the function or activity performed on behalf of Rutgers.

3. The date the business associate provisions were entered into.

4. The date the performance or services begin and ends.

5. The type of PHI that will be shared with the business associate.

6. Whether any of the PHI will be shared through electronic means. Business associates may only use and disclose PHI to the extent that Rutgers would be allowed to use and disclose the information. See University policy, Uses and Disclosures of Health Information With and Without an Authorization, 100.1.1. Only the information minimally necessary to complete the purpose of the service or function may be shared.

III. EXHIBITS

A. Is a Person or Entity a "Business Associate" and Required to Enter Into a Written Business Associate Contract?

B. Examples of Potential Business Associates

C. Treatment, Payment and Health Care Operations

D. Business Associates Agreement Involving the Access to Protected Health Information

EXHIBIT A

Examples of Potential Business Associates

(This is not an all-inclusive list, nor is every arrangement listed necessarily a business associate. Use the attached flowchart and policy and procedure to analyze whether the relationship is a business associate relationship under HIPAA. Contact Office of General Counsel for assistance in the analysis.)

Accountants
Accounting services and firms
Accreditation services
Actuarial services
Actuarial specialists
Adjudication services
Administrative services
Advertisers
Architects, builders, and contractors
Asset-based lenders to healthcare facilities
Attorneys
Auditors
Billing service companies
Bulk mailing services
Care management programs
Civic groups and other local groups help out on ad hoc basis with patients who are hospitalized for a traumatic event or complicated illness (e.g., Shrine Temples, Ronald McDonald House)
Coding providers and experts
Community health management information systems
Computer maintenance services and companies
Consulting services
Contract Research Organization – An entity used by pharmaceutical and device manufactures to monitor clinical research trials
Copy services
Data aggregation services
Device manufactures
Document storage and destruction vendors
Financial service companies
Government health data systems
Hardware vendors
Healthcare consultants (e.g., risk management, information technology, billing, coding and management)
Hospital associations (National and State)
HVAC vendors
Independent contractors

EXHIBIT A (continued)

Examples of Potential Business Associates

Independent service organizations (ISO) offering clinical/biomedical engineering services
Insurance brokers
Interpreter services (both deaf and foreign language)
Janitorial services; waste disposal and recycling services and companies
Law firms, its staff and employees
Lobbyists
Mailing houses
Maintenance contractors
Management services
Marketing services or firms
Medical equipment testing/ repair services
Medical or Physician associations (National and State)
Medical record moving companies
Medical record storage companies
Medical record transcription services
Medical software vendors
Microfilm conversion providers
Organ and Tissue Banks
Organ procurement organization
Outsourced document shredders
Patient advocates
Pharmaceutical companies
Pharmaceutical manufacturers
Pharmaceutical representatives
Plasma Donor Centers
Printing companies (ID cards and other member materials)
Private health data systems
Professional liability insurance carriers
Recycling services and companies
Software vendors
Sperm Banks
Temporary Staffing Companies
Third-party administrators
Trade associations
Utilization management vendors
Value added networks
Vendors to business associates if involving the disclosure of independently identifiable health information
Waste disposal services and companies

EXHIBIT B

Is a Person or Entity a "Business Associate" and Required to Enter Into a Written Business Associate Contract?

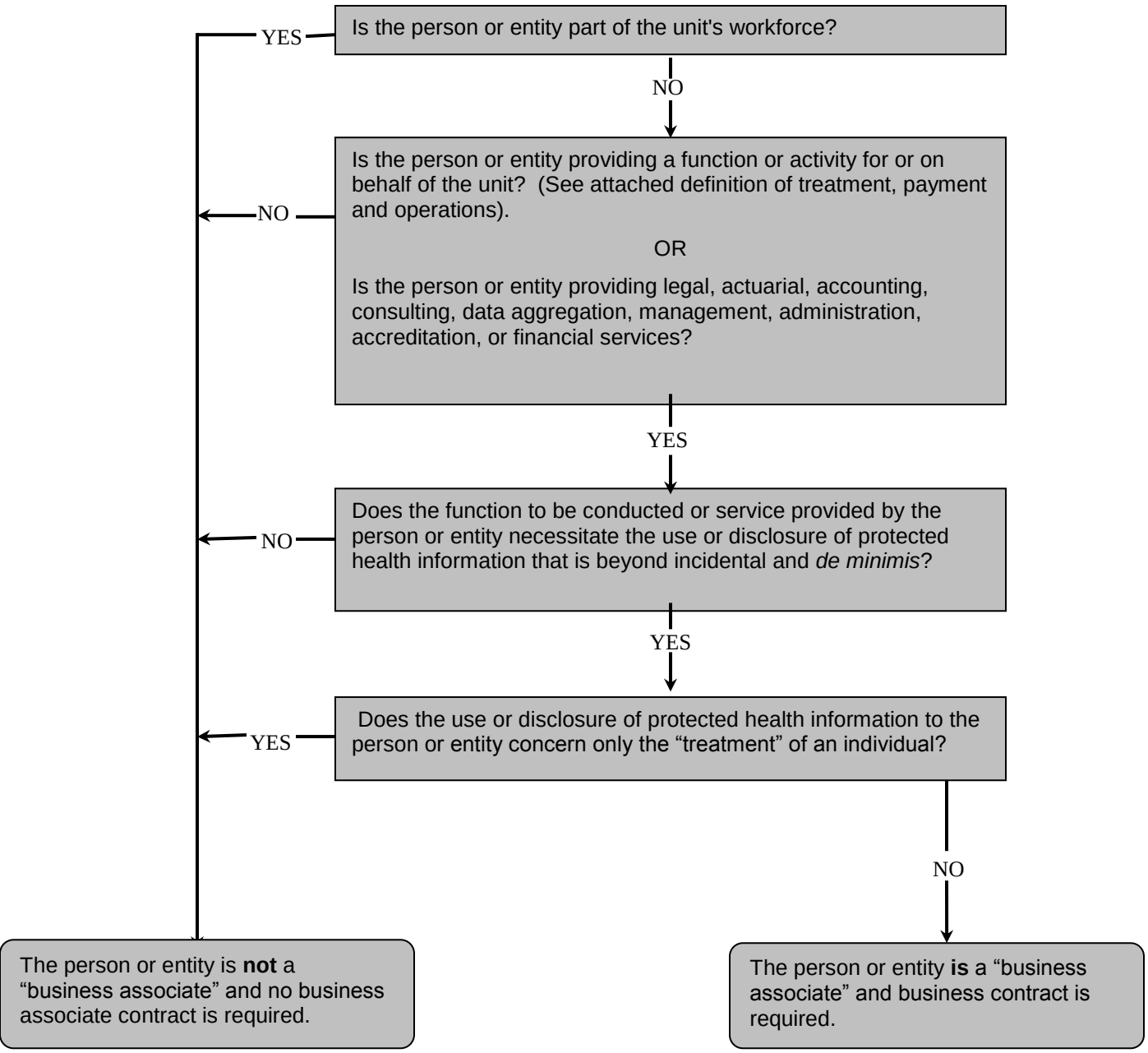

EXHIBIT C

Treatment, Payment and Health Care Operations

A. "Treatment" - the provision, coordination, or management of health care and related services by one or more health care providers, including:

1. The coordination or management of health care by a health care provider with a third party;

2. Consultation between health care providers relating to a patient; or

3. The referral of a patient for health care from one health care provider to another.

B. "Payment" - the activities undertaken to obtain payment for the provision of healthcare; and relates to the individual to whom health care is provided and includes, but is not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

2. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

    a. Obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable, and, therefore, would constitute a payment activity.

    b. Debt collection is recognized as a payment activity.

3. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

4. Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and

5. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of reimbursement:

    a. Name and address;
    b. Date of Birth;
    c. Social Security Number;
    d. Payment history;
    e. Account number; and
    f. Name and address of the health care provider and/or health plan.

C. "Health Care Operations" - any of the following activities:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contracting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care providers, accreditation, certification, licensing, or credentialing activities;

3. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

4. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

5. Business management and general administrative activities of Rutgers, including, but not limited to:

    a. Resolution of internal grievances;

    b. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity.

EXHIBIT D

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

Page 12 of 18

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 that 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 that 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;

Page 14 of 18

(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

Page 15 of 18

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 that the Covered Entity Parties may incur, suffer or sustain, that 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 that 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

Page 16 of 18

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;

(i) 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;
(ii) 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;
(iii) 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
(iv) 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.
(v) 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.

Page 17 of 18

(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.

IN WITNESS WHEREOF, 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: _____

Page 18 of 18