RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Standards for Privacy of Individually Identifiable Health Information					
Section #:	100.1.9	**Section Title:**	HIPAA Policies		**Formerly Book:**	00-01-15-05:00
Approval Authority:	RBHS Chancellor/Executive Vice President for Health Affairs.		**Adopted:**	01/27/2003	**Reviewed:**	3/11/2016
Responsible Executive:	Senior Vice President and Chief Enterprise Risk Management, Ethics and Compliance Officer		**Revised:**	04/20/2012; 7/1/2013; 3/11/2016		
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**
   This policy covers the standards for privacy of individually identifiable health information. This policy applies to:

   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 such 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. Any Business Associate, independent contractor or other vendor providing services engaged by the Rutgers Covered Entity.

   IV. 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, Office of Information Technology and the Office of the Senior Vice President

2. **Reason for Policy**
   To establish guidelines ensuring the Workforce of the Rutgers Covered Entity and the Rutgers Covered Entity's Business Associates and other independent contractors engaged in the handling or creation of individually identifiable health information understand the standards established under HIPAA regulation, including the HITECH Act (2009), the Omnibus Rule (2013) or other applicable federal law, state law, and University policy.

3. **Who Should Read This Policy**
   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 such 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. Any Rutgers University workforce member of any Rutgers school, unit or department that is engaged in the provision, coordination, or management of health care and related services among providers, including third parties, and involving consultations regarding a patient.

IV. Any Business Associate, independent contractor or other vendor providing services engaged by the Rutgers Covered Entity.

V. 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.

4. **Related Documents**

I. 45 CFR, 160, Code of Federal Regulations, Title 45, Part 160, Subpart C, General Administrative Requirements, Compliance and Enforcement

II. 45 CFR, 164.514(e), Code of Federal Regulations, Title 45, Part 164, Subpart E, Security and Privacy, Privacy of Individually Identifiable Health Information

III. 45 CFR, 164.530, Code of Federal Regulation, Security and Privacy, Administrative Requirements

IV. 45 CFR, 164.501(b), Code of Federal Regulation, Privacy Rule, Marketing

V. 45 CFR, 164.514(f), Code of Federal Regulation, Privacy Rule, Fundraising

VI. 45 CFR, 164.508, Code of Federal Regulation, Privacy Rule, Sale of PHI

VII. Records Management and Record Retention Schedules

VIII. 100.1.3 Accounting of Disclosures of Health Information Policy

IX. 100.1.X Disclosures of Personally Identifiable Health Information to Business Associates Policy

X. 50.3.18 Data Breach Notification Policy

5. **Definitions**

I. Individually Identifiable Health Information ("IIHI"): individually identifiable is a subset of health information, including demographic information collected from an individual, and created or received by a health care provider, health plan, employer, or health care clearinghouse; and

A. 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

B. That identifies the individual; or

C. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

For purposes of the Privacy Rule, genetic information is considered to be health information if

the genetic information can be identified PHI.

II. 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 (B) 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 considered active PHI for 50 years after death.

II. Business Associates: 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 not 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 Components or arrangement, or from another Business Associate of such Components or arrangement, to the person.

III. 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.

IV. Rutgers Covered Entity: The collective term referring to all units, schools or departments which 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.

V. Rutgers Covered Component(s): Refers to a single unit, school or department within the Rutgers Covered Entity.

VI. 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.

6. **The Policy**

I. The Rutgers Covered Entity and its Workforce will implement and maintain a Privacy Program to ensure compliance with state law, federal law, and Rutgers policies protecting the confidentiality of individually identifiable health information of its patients and/or Human Subjects. The Rutgers Privacy Program will complement the Rutgers Information Security policies.

II. Each individual within the Rutgers Covered Entity Workforce will conduct his or her activities in a manner so as to protect the confidentiality of patients' individually identifiable health information as required by state law, federal law, and in conformance with Rutgers University policies.

III. The Privacy Program for the Rutgers Covered Entity will consist of the following elements:

A. Rutgers Office of Enterprise Risk Management, Ethics, and Compliance

1. The Rutgers University Director of Privacy with the support of the Chief Healthcare Officer and Health Care Compliance Officers will oversee the development, implementation and maintenance of the Privacy Program for the Rutgers Covered Entity. The Privacy Program will complement the Information Security policies of the University.

2. The Rutgers Covered Entity Compliance Officer(s) will act as a privacy liaison; assist the Rutgers University Privacy Officer in implementing the Privacy Program and University-wide policies and procedures within Rutgers Covered Components. Such Compliance Officers will also oversee the development, implementation and maintenance of any school, unit or departmental policies and procedures related to privacy as appropriate.

3. Rutgers Institutional Review Boards (IRBs) will ensure that informed consents include appropriate authorizations for disclosure or that the authorization for disclosure has been appropriately waived.

4. School and Healthcare Unit Custodian of Medical Records

a. Presidents/CEOs and Deans of the Rutgers Covered Entities maintaining Protected Health Information (PHI) will appoint a Custodian of Medical Records.

b. It will be the responsibility of the Custodian of Medical Records to ensure that processes are in place within their healthcare unit or school, and subordinate work units to implement and monitor compliance with the elements detailed in Section 5 below.

5. The Rutgers University Director of Privacy, with assistance from the Chief ERM, Ethics & Compliance Officer, Healthcare Compliance Officer(s), and the Custodians of Medical Records will direct and support each Rutgers Covered Component to ensure the following elements are developed, implemented and maintained in conformance with state and federal requirements, and are reflected in the University policies and procedures accordingly:

a. Protecting the confidentiality of uses and disclosures of PHI, including requiring appropriate authorizations, and/or allowing a patient the opportunity to agree or object to uses and disclosures of PHI when mandated by law;

b. Implementing appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of PHI from unauthorized use or disclosure;

c. Ensuring that a written process is in place to allow individuals to restrict uses and disclosures of their health information. The Rutgers Covered Entity, however, is not required to agree to such requests;

d. Ensuring patients can receive communications of their health information by alternate means or alternate locations, if requested;

e. Implementing a written process for maintaining an accounting of the Rutgers Covered Entity's uses and disclosures of PHI and providing such accounting to requesting individuals to whom the information pertains;

f. Ensuring that a written process is in place to allow individuals to access, inspect and/or obtain a copy their health information;

g. Ensuring that a process is in place to allow individuals to request their medical record be amended. The Rutgers Covered Entity, however, may deny requests under specified circumstances;

h. Ensuring a process is in place for Rutgers Covered Components that desire to market or sell PHI to receive authorization from affected patients;

i. Ensuring a process is in place to enable patients of the Rutgers Covered Entity to opt out of fundraising activities and requests;

j. Ensuring the Rutgers Covered Entity provides a process for a patients/individuals to make complaints concerning the Rutgers Covered Entity privacy policies and procedures.

6. The Rutgers University Director of Privacy will be the designated contact person for individuals seeking further information or clarification on the Rutgers Covered Entity's health information policies, privacy rights and patient rights requirements. The Rutgers University Director of Privacy will be designated to receive complaints concerning Rutgers Covered Components alleged non-compliance with health information privacy and patient rights requirements.

7. All existing or new unit, school, or departmental policies and procedures addressing any of the items within this policy, or concerning the use or disclosure of PHI, and all consent/authorization forms used for the disclosure of PHI must be presented to the Rutgers University Director of Privacy for review to ensure compliance with University policies, federal law and state law.

8. The Director of Privacy will communicate periodically with the Presidents/CEOs and Deans of the Rutgers Covered Components on the status of all policies and procedures concerning PHI and the Privacy Program, including its implementation, the training of the Workforce of the Rutgers Covered Entity, and any recommended changes or amendments to the University's privacy program or policies

9. Rutgers Covered Components will promptly revise policies and procedures related to the Privacy Program as discussed above as necessary and appropriate to comply with changes in the law. All policies and procedures will be reviewed periodically by the Rutgers University Director of Privacy to ensure compliance and operational effectiveness. If changes in federal or state privacy law materially affect privacy practices as stated in the Rutgers Notice of Privacy Practices ("NPP"), the NPP must also be changed in a timely manner.

10. Rutgers Covered Components will provide notice of the Rutgers Covered Entity privacy practices by making public and distributing the Rutgers Covered Entity's Notice of Privacy Practices according to federal standard.

11. All notices to patients concerning the Rutgers Covered Entity's privacy practices must state the Rutgers Covered Entity reserves the right to make changes in its privacy practices at any time.

B. Education and Training

1. The Rutgers University Director of Privacy will establish training requirements and recommend refresher training to the Rutgers Covered Entity's Workforce relevant to the Rutgers Privacy Program, University privacy policies and procedures, and federal and state regulatory requirements, as appropriate.

2. The Rutgers Office of Enterprise Risk Management, Ethics, and Compliance, in conjunction with Human Resources or other appropriately assigned departments/divisions, will ensure the necessary efforts will be taken to provide new members of the Rutgers Covered Entity's Workforce privacy training appropriate to the position employed within 30 days of hire or transfer to a new position.

3. As necessary, the Rutgers University Director of Privacy will coordinate additional training of the Workforce whose functions are affected by material change in the privacy policies and procedures within a reasonable period of time after the change becomes effective.

4. Training, attendance and completion will be appropriately documented and the documentation will be maintained by the University Director of Privacy for a minimum of six (6) years or as specified by the Records Management Policy and the attendant Record Retention Schedules, whichever is longer.

C. Non-retaliation for exercise of Patient Rights

1. Rutgers Covered Entity Workforce is prohibited from threatening, coercing, discriminating or taking other retaliatory action against the following: :

a. Patients for exercising any right established by HIPAA privacy guidelines, 45 CFR 164, subpart E;

b. Individuals and others for filing a complaint with the Secretary of Health and Human Services under 45 CFR 160, subpart C;

c. Individuals and others for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

d. Individuals or others for opposing any act or practice made unlawful by 45 CFR 164, subpart E, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of 45 CFR 164, subpart E.

IV. The Rutgers University Director of Privacy or designee shall be responsible for communicating and enforcing the above policy as it relates to all University employees.

V. The Medical Directors, President/CEOs of the Rutgers Covered Components and Research Deans shall be responsible for communicating and enforcing the above policy as it relates to persons involved in patient and human subject contact.

VI. The Executive Director of University Procurement Services or his or her designee shall be responsible for communicating and enforcing the above policy as it relates to vendors,

independent contractors, Business Associates or other contracted services provider engaging with the Rutgers Covered Entity through the Procurement Process.

VII. The Rutgers Covered Entity may not require individuals to waive their rights to file a complaint with the Secretary of Health and Human Services or any other right under CFR 164, subpart E, including 164.500 through 164.530, as a condition of the provision of treatment, payment, and enrollment in a health plan or eligibility for benefits.

VIII. Monitoring and Evaluation

A. The Rutgers Compliance Committee is the governing body for the evaluation and monitoring of the Rutgers Privacy Program and will review compliance issues as appropriate.

B. The IRB, the University's Research Compliance Officer, and other appointed research or research compliance personnel will monitor compliance with requirements for research related disclosures.

C. The Rutgers University Director of Privacy will periodically request external or internal audits to be conducted to ensure compliance with this policy.

D. The Rutgers University Director of Privacy is responsible for investigating and reporting on allegations of non-compliance with the privacy policies applicable to the Rutgers Covered Entity.

IX. Sanctions for Non-Compliance

A. The Rutgers Covered Entity will apply appropriate sanctions against any member of the Workforce who fails to comply with the University's privacy policies and procedures, and applicable state and federal laws.

B. The Rutgers University Director of Privacy, with the assistance of University Human Resources and designees of The Deans and President/CEOs of affected Rutgers Covered Components, will determine and enforce the sanctions appropriately and consistently.

C. The Rutgers Covered Components will document all sanctions that are applied.

D. Documentation

X. Documentation evidencing implementation of the privacy program applicable to the Rutgers Covered Entity, including complaints, training, sanctions, auditing, etc., will be maintained for a minimum of six (6) years or the time period specified by the Records Management Policy and attendant Record Retention Schedules, whichever is longer.