RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Facsimile (Fax) Machine Transmittal of Confidential, Sensitive or Protected Health and Other Information					
Section #:	100.1.2	**Section Title:**	HIPAA Policies		**Formerly Book:**	00-01-15-35:00
Approval Authority:	RBHS Chancellor/Executive Vice President for Health Affairs		**Adopted:**	1/23/2003	**Reviewed:**	3/18/2016
Responsible Executive:	Senior Vice President and Chief Enterprise Risk Management, Ethics and Compliance Officer		**Revised:**	10/24/2011, 7/1/2013; 3/18/2016		
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 provides guidance on how to send or receive Restricted or Protected Health Information (PHI) via facsimile in compliance with the Health Information Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act) 2009, the Omnibus Rule of 2013 and the Standards for Privacy of Individually Identifiable Health Information and how to safeguard Restricted, confidential, sensitive and Protected Health Information (PHI) and other information as protected by state law, federal law or University policy. 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 Rutgers University workforce member or any independent contractor, business associate or other vendor providing services and engaged by the Rutgers Covered Entity that works with restricted, confidential, sensitive and Protected Health Information (PHI).

2. Reason for Policy

To provide the rules that should be followed when sending or receiving facsimile (fax) Protected Health Information or University Restricted information to ensure the University's compliance with the Health Information Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act) 2009, the Omnibus Rule of 2013 and the Standards for Privacy of Individually Identifiable Health Information and to safeguard Restricted, confidential, sensitive and Protected Health Information (PHI) and other information as protected by state law, federal law or University policy.

3. Who Should Read This Policy

This policy applies to and should be read by:

I. Within the Rutgers Covered Entity and Components within that Entity, individuals who may send or receive facsimile documents containing Restricted or Protected Health Information (PHI), 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. 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.

IV. Other University departments that assist the Covered Component 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.

V. Any Rutgers University workforce member or any independent contractor, business associate or other vendor providing services and engaged by the Rutgers covered entity that works with restricted data, including PHI.

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 164.524, Title 45, Code of Federal Regulations, Part 164, Section 524, Security and Privacy, Access of Individuals to Protected Health Information

V. Privacy Act, 5 U.S.C. 552a

VI. Rutgers Access of Individuals to Protected Health Information, Policy 100.1.4

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

VIII. Rutgers Accounting of Disclosures of Health Information, Policy 100.1.3

IX. Data Breach Management, Policy 50.3.18

X. Gramm Leach Bliley: http://policies.rutgers.edu/50311-currentpdf

XI. Red Flag Rules: http://policies.rutgers.edu/50312-currentpdf

XII. PCI: Credit Card Acceptance Policy: http://policies.rutgers.edu/40215-currentpdf

XIV FERPA http://compliance.rutgers.edu/ferpa

XV. IT Security Guidelines for Travel https://rusecure.rutgers.edu/content/it-security- guidelines-domestic-and-international-travel

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 (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 be considered active PHI for 50 years after death.

II. Sensitive Protected Health Information: Protected Health Information that pertains to (i) an individual's HIV status or treatment of an individual for an HIV-related illness or AIDS, (ii) an individual's substance abuse condition or the treatment of an individual for a substance abuse disorder or (iii) an individual's mental health condition or treatment of an individual for mental illness.

III. Sensitive Electronic Information (SEI): Includes electronic information that is protected by state or federal regulations. As such, it includes Protected Health Information (PHI) as defined under HIPAA regulations, as well as information governed by Gramm-Leach-Bliley Act (GLBA) and other applicable regulations.

IV. Restricted Information: Restricted Data is the most sensitive information and requires the highest level of protection. See Appendix A of Policy 70.1.2 in Exhibit A of this policy for a detailed description and examples.

V. Secure location: A location that is not accessible to the general public.

VI. Covered Entity (CE): Either A (1) A health care provider, (2) a health plan or (3) a health care clearinghouse that 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. 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. Rutgers Workforce and the Workforce of the Rutgers Covered Entity are committed to safeguarding PHI and other restricted information in order to fulfill its mission to patients and to operate in a manner consistent with applicable federal and state laws and regulations. Consequently, schools and units will exercise special care regarding the location and operation of fax machines.

II. Due care should be exercised when faxing PHI and other Restricted Information. In addition, the faxing of sensitive protected health information, such as dealing with mental health, chemical dependency, sexually transmitted diseases, HIV or other highly personal information, should be avoided whenever possible.

III. Any incidents where incoming or outgoing faxes have compromised a patient's right to privacy must be reported immediately to the University Director of Privacy.

IV. Sending Faxes:

A. Confidential FAX coversheets should be developed by departments utilizing the language in the sample Confidential Fax Cover Sheet (see Exhibit B) and must include the following statement:

This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this information is **STRICTLY PROHIBITED**. If you have received this message in error, please notify the sender immediately and arrange for the return or destruction of these documents.

B. Employees will take reasonable steps to ensure that a fax transmission is sent to and received by the intended recipient. When the fax transmission includes PHI or Restricted information, "reasonable steps" include, but are not limited to, the following:

1. Preprogrammed fax numbers must be verified periodically for validity.

2. When a fax number is entered manually (because it is not one of the pre-programmed numbers) the employee entering the number will visually check the recipient's fax number on the fax machine prior to starting the transmission.

3. The name, business affiliation, telephone number and fax number of the intended recipient as well as the number of pages contained in the transmission must also appear on the cover sheet.

4. Fax confirmation sheets will be checked immediately or as soon as possible after the fax has been transmitted, to confirm the material was faxed to the intended fax number. If the intended recipient notifies the sender that the fax was not received, the sender will use best efforts to determine whether the fax was inadvertently transmitted to another fax number by checking the fax confirmation sheet and/or the fax machine's internal logging system.

5. If an employee becomes aware that a fax with PHI was sent to the wrong fax number, the employee will immediately attempt to contact the recipient by fax or telephone and request that the faxed documents, and any copies of them, be destroyed immediately or returned to the Covered Entity. The employee's supervisor or University Director of Privacy will also be notified of the mis-directed fax. The Director of Privacy will conduct a breach analysis to determine further action.

6. Those recipients who regularly receive PHI via fax will be reminded periodically to notify the Covered Entity of any change to the recipient's fax number.

7. Fax confirmation sheets will be attached to and maintained with all faxed materials.

8. Faxing of sensitive PHI (such as HIV/AIDS results or status or substance abuse and mental health treatment records) should be avoided whenever possible.

9. When faxing PHI or Restricted information, employees will comply with all other Rutgers privacy and security policies and guidelines.

V. Receiving Faxes:

Employees who are intended recipients of faxes that contain PHI or Restricted information will take reasonable steps to minimize the possibility those faxes are viewed or received by someone else. These "reasonable steps" include, but are not limited to, the following:

A. Fax machines that receive such faxes will be located in Secure Areas.

B. If an employee receives such a fax on a fax machine that is not in a Secure Area, the recipient of the fax will promptly advise the sender that the receiving fax machine should not be used for the transmission of such information.

C. Fax machines will be checked on a regular basis to minimize the amount of time incoming faxes that contain PHI or Restricted Information are left on the machines. Employees who monitor the fax machines, or the employee who sees such a fax on the machine, will promptly remove incoming faxes and deliver them to the proper person.

D. If an employee receives a fax addressed to someone other than the employee and the person to whom the fax is addressed is someone at the Covered Entity, the employee will promptly notify the individual to whom the fax was addressed and deliver or make arrangements to deliver the mis-directed fax as directed by the intended recipient.

E. If an employee receives a fax addressed to someone other than the employee and the person to whom the fax is addressed is NOT affiliated with the Covered Entity, the employee will promptly notify the sender, and destroy or return the faxed material as directed by the sender.

F. Employees who routinely receive faxes containing PHI or Restricted Information from other individuals or organizations (either internal or external sources) will promptly advise those regular senders of any changes to the employee's fax number.

G. Faxes with PHI should be placed in a secure/confidential place when they are delivered and not left in a location that is in full view of passers-by.

VI. Sanctions for Non-Compliance

A. Rutgers will apply appropriate sanctions against any member of the Workforce who fails to comply with privacy policies and procedures.

B. The Chancellors, Deans, Vice Presidents and President/CEOs of the Covered Components with the assistance of University Human Resources, will enforce the sanctions appropriately and consistently.

C. The Related Healthcare Entity will document all sanctions that are applied.

VII. Retaliation/Waiver

It is policy that the Related Healthcare Entities may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by

the individual of any privacy right. The Related Healthcare Entities may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

VIII. Exhibits

A. Classification Table

B. Confidential Fax Cover Sheet

Exhibit A

Classification Table

Please see Rutgers Minimum Security Standards for Data Protection, which outlines the minimum level of controls necessary for each category. https://rusecure.rutgers.edu/content/minimum-security-standards-data-protection

Information Classification	Description	Examples
Restricted	Restricted Data is the most sensitive information and requires the highest level of protection. This information is usually described as 'non-public personal information' (NPPI)' about people or critical business, academic or research operations under the purview of the Information Owner (Data Custodian). Restricted data includes, but is not limited to, data that the University is required to protect under regulatory or legal requirements. Unauthorized disclosure or access may 1) subject Rutgers to legal risk, 2) Adversely affect its reputation, 3) jeopardize its mission, and 4) present liabilities to individuals (for example, HIPAA penalties).	• Bank information • Login Credentials (username & password) • Credit/Debit Card Number • Driver's License Number • Human Resources information if it contains SSNs, medical reports, etc. • Passport Number • Protected Health Care Information (PHI)[1] • Protected Data Related to Research[2] • Social Security Number • Student Disciplinary, or Judicial Action Information • Police Records • Student Records (FERPA)
Internal	All other non-public information not included in the Restricted category.	• Licensed Software • Other University Owned Non-Public Data • University Identification Number or Information Number (employee numbers, student ID numbers, etc.)
Public	All public information.	General access data, such as that on unauthenticated portions of any rutgers.edu site.

[1]Protected Health Care Information includes, but is not limited, to the following:

- Protected Health Information (PHI) or Electronic Protected Health Information (EPHI)
- Patient health-care and human subjects research records
- Payment transactions related to health services
- Medical and personal information in research records
- Quality-assurance and peer-review information from patient care units

[2]Protected Data Related to Research

- University proprietary information, including copyrightable and patentable information
- Proprietary information belonging to other individuals or entities, such as under a non-disclosure agreement or contract,
- Library circulation records and any information about use of any library information resource in any format.

Exhibit B

CONFIDENTIAL FAX COVER SHEET

"Confidential Protected Health and Other Information Enclosed"

Protected Health Information is personal and sensitive information related to a person's health care. Other protected or restricted information may include information protected by State or Federal regulations and University policy. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Re-disclosure of PHI without additional patient consent or authorization is by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law.

To:		**From:**	
Location:		**Location:**	
Date Sent:		**Fax Number:**	
Time Sent:		**Phone Number:**	
Fax Number:		**Number of Pages: (Including Cover)**	
Phone Number:			

☐ Urgent ☐ For Review ☐ As Requested ☐ Please Reply ☐ Please Comment

Comments:

IMPORTANT WARNING: This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this information is **STRICTLY PROHIBITED**. If you have received this message in error, please notify the sender immediately and arrange for the return or destruction of these documents.