RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Data Breach Management					
Section #:	50.3.18	**Section Title:**	Legal Matters		**Formerly Book:**	n/a
Approval Authority:	Senior Vice President and Chief Enterprise Risk Management, Ethics and Compliance Officer, and Senior Vice President of Administration		**Adopted:**	7/6/2015	**Reviewed:**	7/6/2015
Responsible Executives:	Associate Vice President and Deputy Chief Enterprise Risk Management and Compliance Officer, and Vice President for Information Technology and Chief Information Officer		**Revised:**			
Responsible Offices:	Office of Enterprise Risk Management, Ethics and Compliance and Office of Information Technology		**Contact:**	Information Protection and Security, OIT 732-445-8011 Office of Enterprise Risk Management, Ethics and Compliance (ERM) 973-972-8093 http://www.rutgers-compliance-hotline.com		

1. **Policy Statement**
   The university collects information about individuals only if permissible by law and university policy and when it meets appropriate business purposes. It is the university's policy to protect information it receives, handles, and stores in all instances, and to comply with laws pertaining to the safeguarding of Restricted information, including the New Jersey Identity Theft Prevention Act and HIPAA.

   In accordance with this policy and implementing guidelines, the university community must be educated and vigilant about requirements for collecting, retaining and restricting access to information classified as Restricted and identifying potential security breaches (i.e. incidences where information may have been accessed by unauthorized persons), and reporting such security breaches to appropriate university personnel for immediate evaluation and action. The university shall be committed to carefully and expeditiously investigating potential security breaches. In situations where notification to potential victims of security breaches is determined to be required by law or otherwise appropriate, the university shall do so in the most expedient time possible and without unreasonable delay.

2. **Reason for Policy**
   To establish a uniform data breach management and notification process and to ensure University-wide compliance with state(s) and federal regulatory breach notification obligations.

3. **Who Should Read this Policy**
   All members of the University community.

4. **Resources**

I. Policies.rutgers.edu: Information Technology - Section 70
II. Policies.rutgers.edu: Clinical, Compliance, Ethics & Corporate Integrity - Section 100
III. RU Secure Website: http://rusecure.rutgers.edu/
IV. OCR HIPAA breach definition:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

5. **Definitions**

I. Restricted Data: Restricted Information: Restricted Data is the most sensitive information and requires the highest level of protection. See Exhibit A of this policy for a detailed description and examples. (The Exhibit of the Classification Table is also referenced in the Appendix of Policy 70.1.2).

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

III. Covered Entity: Either (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 Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

6. **The Policy**

I. Reporting Security Breaches

Any unit or individual aware of a potential breach of security containing Restricted information must immediately report the potential breach of security to their supervisor or unit head and the Office of Enterprise Risk Management, Ethics and Compliance at 973-972-8093. To report anonymously, contact the Rutgers Compliance Hotline at 1-800-215-9664 or http://www.rutgers-compliance-hotline.com

II. Investigation of Reported Security Breaches:

Without undue delay, upon receiving notification of a report, the Office of Enterprise Risk Management, Ethics and Compliance shall invoke incident response procedures commensurate with the potential breach of security. The Office of Enterprise Risk Management, Ethics and Compliance shall make an initial evaluation and determination if the potential breach of security can be investigated and managed by a single responder. Even when a potential breach of security is investigated by a single responder, all applicable law, regulation and policy will be complied with, including any notice required under Section D hereunder. If the Office of Enterprise Risk Management, Ethics and Compliance determines a significant breach is possible, the breach shall be referred expeditiously to the Information Protection Evaluation Team (IPET). IPET shall be comprised of the following individuals and representatives of the following offices:

- Director of the Office of Information Protection & Security (Co-Chair)
- Director of Privacy (Co-Chair)
- Office of the Senior Vice President and General Counsel
- Department of Risk Management & Insurance
- Chancellor Designee from the effected campus
- Office of Information Technology Designee

The IPET also may be advised by or seek advice from representatives of the following units as needed:

- University Human Resources
- Office of the Registrar
- Office of Student Affairs
- Rutgers University Police Department
- Unit in which the incident occurred
- University Communications and Marketing
- Any other unit or department that the IPET determines may provide assistance

Without undue delay a Chair of IPET shall convene a meeting to expeditiously conduct a fact-finding investigation concerning the possible breach of security or compromise of systems. All members of IPET are required to participate in the meeting, but the excused absence of any members should not delay the meeting or the investigation. The IPET is encouraged to speak directly to persons who may have information regarding the matter being investigated (e.g., data owners). The investigation shall conclude without undue delay.

In conducting its investigation, members of IPET and any others assisting the IPET, may be required to obtain and review Restricted information in electronic or hardcopy format related to the incident. Extreme care and caution should be used to ensure that such information is protected and that there are no further security breaches resulting from the investigation.

During the course of an investigation, the IPET has the authority to provision additional internal or external resources, such as computer forensics, to help determine whether it was possible that an exploit of a vulnerability led to the exposure of Restricted information.

III. Report of IPET and Recommendation:

A. Without undue delay, upon the conclusion of an investigation, a Chair of IPET shall oversee the preparation and retention of a written report based on the criteria of the regulatory requirements.

B. A Chair of IPET shall forthwith submit the written report and recommendation to the Senior Vice President and Chief Enterprise Risk Management, Ethics and Compliance Officer, Senior Vice President for Academic Affairs, and Senior Vice President for Administration. The members of IPET shall make themselves available to answer any questions about the investigation and report. A copy of the report will be made available to the Chancellor and unit head from where the breach occurred, the Chief Audit Executive, and the IPET members.

C. The Senior Vice President and Chief Enterprise Risk Management, Ethics and Compliance Officer, Senior Vice President for Academic Affairs, and Senior Vice President for Administration shall make a written final determination regarding notification without undue delay.

IV. Notification:

A. Notifications shall meet the breach notification requirements of the applicable federal and state(s) regulations.

1. HIPAA

A log of all breaches involving less than 500 individuals will be maintained and annually submitted to the Secretary of HHS.

For breaches involving 500 or more individuals, notice shall be provided to the Secretary of HHS at the same time notice is made to the individuals. Notice shall be provided to prominent media outlets serving the state(s) and regional area where affected patients/individuals are likely to reside.

2. New Jersey Identity Theft Prevention Act

   Prior to effecting any notification and without undue delay, the IPET with the assistance of Rutgers Police shall report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigating and handling, which may include dissemination or referral to other appropriate law enforcement entities.

   In cases where notification of more than 1,000 persons at a time is required, the Chair of IPET in conjunction with the appropriate Rutgers supportive staff shall also provide notification to all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis as defined by the federal "Fair Credit Reporting Act".

3. Units where a potential security breach has been substantiated shall be responsible with other supportive units (e.g. Registrar, Alumni Relations, and Human Resources) for providing the Office of Enterprise Risk Management, Ethics and Compliance with a list of affected individuals and their current contact information. The Office of Enterprise Risk Management, Ethics and Compliance will create breach notification letters, which shall be signed by a representative of the Office of Enterprise Risk Management, Ethics and Compliance and the department head for the unit where the incident occurred. The Office of Enterprise Risk Management, Ethics and Compliance shall make notifications within the regulatory requirements and without undue delay. The cost of the breach remediation shall be borne by the department where the incident occurred.

4. In the case of potential breaches referred to IPET, whether notification is required or not, the Internal Audit Department will review or consult with the unit head to determine whether or not any material weaknesses existed in the controls and processes leading to the breach, and suggest improvements to minimize future events.

V. Records Management:

The Office of Enterprise Risk Management, Ethics and Compliance shall maintain the records pertaining to each reported incident for a period defined by applicable regulatory requirements. Those records shall include all requirements defined by each applicable regulation.

VI. Non-Compliance and Sanctions:

Failure to comply with this policy may result in denial or removal of access privileges to the university's electronic systems, disciplinary action under applicable university policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable state and federal statutes.

VII. 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 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.