RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.2.3

Section Title: Legacy UMDNJ policies associated with Information Technology

Policy Name: Information Security: Mobile Computing and Removable Media

Formerly Book: N/A

Approval Authority: Senior Vice President for Administration

Responsible Executive: Vice President for Information Technology and Chief Information Officer

Responsible Office: Office of Information Technology (OIT)

Originally Issued: July 1, 2013

Revisions: Originally 00-01-95-20:05 at UMDNJ; 10/10/2013 (Updated title)

Errors or changes? oitpolicy@rutgers.edu

1. **Policy Statement**
   To establish the requirements for the physical and technical protection and access control of Mobile Computing Devices and Removable Media that connect to Rutgers, The State University of New Jersey, information systems.

2. **Reason for Policy**
   The purpose of this policy is to establish requirements and procedures regarding the proper use of mobile computing devices and removable media.

3. **Who Should Read This Policy**
   This policy applies to any individual responsible for the management, operation, and/or maintenance of the legacy UMDNJ information technology services and/or environment. If you are uncertain whether this policy applies to you, please contact your direct supervisor.

4. **Related Documents**
   Federal Information Security Management (FISMA) Act
   http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

5. **Contacts**
   oithelp@rutgers.edu

6. **The Policy**

70.2.3 INFORMATION SECURITY: MOBILE COMPUTING AND REMOVABLE MEDIA

All members of the University community have a responsibility to protect the Confidentiality, Integrity, and Availability of University information collected, processed, transmitted, stored, or transmitted on mobile computing devices and removable media.

- Confidentiality – the expectation that only authorized individuals, processes, and systems will have access to Rutgers' information.
- Integrity – the expectation that Rutgers' information will be protected from intentional, unauthorized, or accidental changes.
- Availability – the expectation that information is accessible by Rutgers when needed.

Because the use of such devices and media presents an information risk to the University, each business unit must establish departmental procedures governing their use, including whether the use of personal devices and media are permitted for the conduct of sound University business.

If a business unit approves the use of mobile computing devices and removable media (whether University-owned or personal) to facilitate the execution of its business processes and functions, they must be secured according to the University's security standards and requirements.

Sharing of electronic information related to "treatment, payment or operations of health care business" (TPO) is not to be impeded by the controls stipulated in this policy. See the Exhibit for an extended definition of TPOs.

I. Requirements:

A. Each business unit must document and communicate to their members whether the business unit permits the use of mobile computing and removable media (whether University-owned or personal) for University business. If the business unit allows the use of such devices and media, they must develop, document, and communicate procedures for their use.

Procedures must:

1. Reflect the value and importance of the information the business generates, processes, and handles.

2. Stipulate the business unit's record retention and e-discovery requirements, if any.

3. Stipulate the business unit's and University's security expectations and requirements.

4. Reflect the expectations of third parties and partners for which the business unit acts as information custodian.

5. Communicate that University information stored or transmitted on personally owned devices and media remain the property of the University.

Business units must periodically conduct policy and procedures training and awareness for their members.

B. All mobile computing devices and removable media used for University business must be secured against unauthorized access, loss, or theft. This is regardless of whether it is owned or leased by the University or a personally owned device or media. Contractual partners who keep Rutgers confidential information on their mobile computing devices or media must also adhere to these requirements.

C. The security of mobile computing devices and removable media used for University business must be managed by OIT and, at minimum, must be password protected and encrypted. Departments should evaluate their need for additional safeguards based on their specific security and business requirements.

D. Technical controls must comply with the University's security standards as defined by Office of Information Technology.

E. Shipments of devices or media containing Confidential or Private or other sensitive information must be done using a courier that can track shipments and provide proof of receipt. Lost or stolen shipments must be reported to the Information Owner and the Department of Risk Management and Insurance.

II. Responsibilities:

A. All members of the University community must protect the Confidentiality, Integrity, and Availability of University information on mobile computing devices and removable media, whether they are personally owned or owned or leased by the University.

B. Business units must establish procedures governing the use of mobile computing and removable media by their members and periodically conduct training and awareness for its members.

C. OIT must define the technical standards that meet the information security requirements of the University, its departments, and its regulatory bodies.

III. Incident Reporting

Loss or theft of a Mobile Computing Device and Removable Media must be reported immediately. The following steps must be taken:

A. Immediately report the loss or theft to the OIT Help Desk.

B. Immediately report loss, theft, or unauthorized access to a manager. If the information is electronic patient health information, Compliance must be notified.

C. Report loss or theft of physical assets to Department of Risk Management and Insurance.

IV. 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.

V. Exhibit – Treatment, Payment, and Health Care Operations (TPO)

These definitions are from the U.S. Department of Health & Human Services document, "Uses and Disclosures for Treatment, Payment, and Health Care Operations." The document can be downloaded from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf.

Guidance on aspects of the HIPAA Privacy Rule can be found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/privacyguidance.html

Treatment, Payment, and Health Care Operations

What are Treatment, Payment, and Health Care Operations? The core health care activities of "Treatment," "Payment," and "Health Care Operations" are defined in the Privacy Rule at 45 CFR 164.501.

- "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care

provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

- "Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

  In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:
  - Determining eligibility or coverage under a plan and adjudicating claims;
  - Risk adjustments;
  - Billing and collection activities;
  - Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
  - Utilization review activities; and
  - Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

- "Health care operations" are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, include:
  - Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
  - Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
  - Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
  - Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Frequently Asked Questions

To see Privacy Rule FAQs, go to
http://www.hhs.gov/ocr/privacy/hipaa/faq/privacy_rule_general_topics/index.html.