

MONMOUTH UNIVERSITY POLICIES AND PROCEDURES

Policy Name: Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Policy

Original

Issue Date: Unknown

Revision Date: February 18, 2011

Approved By: President and Cabinet

Issued By: Patricia Swannack
Vice President for
Administrative Services

I. Purpose

Monmouth University, pursuant to the Health Insurance Portability and Accountability Act (HIPAA) law and regulations, is required to take reasonable steps to ensure the privacy of your Electronic Protected Health Information (ePHI). Protected Health Information (PHI) is individually identifiable health information related to the past, present or future physical or mental health or condition of an individual; provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. ePHI is any PHI that is created, accessed, transmitted or received electronically. The HIPAA Security rule provides for administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of all ePHI data that a covered component creates, receives, maintains or transmits, and that such data is protected from unauthorized access.

II. Scope of Policy

This policy is specific to the HIPAA Security Rule and applies only to those HIPAA covered components identified in the Privacy Policy. Other laws or University rules regarding privacy are addressed in separate University policies and procedures. Employees are expected to adhere to State and Federal laws and regulations, and to the University's policies and procedures. Employees who disregard University policies and procedures, and/or related State or Federal laws and regulations will be subject to disciplinary action up to and including termination.

III. Administrative Safeguards

A. Risk Analysis

A yearly risk analysis will be performed on all covered components to identify the potential risks and vulnerabilities of ePHI maintained or transmitted electronically. This will include documentation of all repositories of ePHI as well as allowed users of each repository. The risk analysis is to be presented to the Security Official who will identify remedial steps for any identified risks.

B. Risk Management

Each covered component will implement security measures and safeguards for each ePHI repository to reduce risks and vulnerabilities to a reasonable level.

C. Sanctions

Any employee who fails to comply with HIPAA laws and regulations or University policies and procedures will be subject to disciplinary action and sanctions commensurate with the gravity of the violation and shall include, but are not limited to, re-training, verbal and written warnings, and termination. The University will investigate any potential HIPAA security violation or incident in a timely manner. The University will not intimidate, threaten, coerce, discriminate against or take any retaliation against any employee who reports a HIPAA security violation or incident.

D. Information System Activity Review

The University will implement internal audit procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to ensure that its security controls are effective and that ePHI has not been potentially compromised.

E. Assigned Security Responsibility

The University has appointed a Security Official (the Vice President for Information Management) to ensure compliance with the HIPAA Security rule for all covered components included in this policy. The Security Official is responsible for the development and implementation of policies, procedures and training programs that will ensure compliance with the HIPAA Security rule. The Security Official may delegate some or all of the responsibilities in carrying out the requirements of this policy.

F. Workforce Security

Each covered component will establish procedures that ensure only authorized personnel have access to systems that manage ePHI and that such access is only provided when necessary to carry out job responsibilities. Documentation will be maintained regarding the levels of access granted to each individual and program.

G. Information Access Management

Each covered component will establish procedures to assign, implement, revoke and modify access to ePHI.

H. Security Awareness and Training

All covered components will ensure that employees with access to ePHI receive HIPAA Security Training and periodic security updates.

I. Security Incident Procedures

The Security Official will be the University's contact person for receiving information related to suspected or known incidents of unauthorized access to ePHI. The Security Official will investigate and mitigate, to the extent practicable, any harmful effects of security incidents that are known, and will document any known security incidents and their outcomes.

J. Contingency Plan

The University will maintain a Contingency Plan for responding to system emergencies, which will include procedures for creating and maintaining backups of ePHI and restoring any data lost due to such an emergency. Each covered component will identify any critical business processes necessary and maintain its own procedures for enabling such processes to continue if essential.

K. Evaluation

The Security Official will perform periodic evaluations, at least annually, to determine compliance with the HIPAA Security Rule and to assure continued viability in light of environmental or operational changes that could affect the security of ePHI.

L. Business Associate Contracts and Other Arrangements

The University will enter into business associate agreements with any third party vendor ("business associate") it permits to create, receive, maintain or transmit ePHI on the University's behalf to ensure that the business associate will appropriately safeguard the information. Such contracts will provide that the business associate will (1) implement administrative, physical and technical safeguards to reasonably protect the confidentiality, integrity, and availability of ePHI it has access to; (2) ensure that agents, including subcontractors, agree to implement reasonable and appropriate safeguards to protect ePHI; (3) report to the University any security incidents of which it becomes aware; and (4) terminate such contract upon request by the University and return or destroy all ePHI it maintains.

IV. Physical Safeguards

A. Facility Access Controls

The University will ensure that access to facilities housing ePHI is appropriately safeguarded against unauthorized physical access, tampering or theft, while ensuring that properly authorized access is allowed.

B. Workstation Use

Any University employee with authorized access to ePHI will be assigned a specific workstation in which he/she is allowed to access such ePHI. These workstations will have appropriate security controls in place to prevent unauthorized access to ePHI.

C. Workstation Security

Any University employee with authorized access to ePHI will have his/her workstation location set to eliminate or minimize the possibility of unauthorized access to ePHI. Workstations will be set with inactivity timeouts and use password protected screen savers.

D. Device and Media Controls

Laptop workstations will not be utilized for accessing ePHI without proper security and firewall protection, and only when permission has been granted by the Security Official

to access ePHI from such a workstation. ePHI should not be stored on any computer hard drive or other storage unit such as CD ROMs or thumb drives without the approval of the Security Official and appropriate steps taken to ensure data has been properly protected. Any medium used to store ePHI, such as for backup and recovery, if being disposed of, must be discarded or reused in a manner that prevents data recovery.

V. Technical Safeguards

A. Access Control

Security controls will be established to ensure that access to systems containing ePHI will be allowed only to those employees that have been granted access rights. A unique user name will be used by each individual provided access to systems to enable identifying and tracking user identity. Emergency access procedures will be established to allow emergency access to systems necessary to continue business operations when needed. Workstations and applications will be programmed to automatically log out when inactivity has exceeded a set period of time established by each covered component, not to exceed fifteen (15) minutes. A mechanism for encrypting and decrypting data will be implemented when ePHI is transferred to/from systems not controlled by the University.

B. Audit Controls

An audit process will be established to examine logged information to assist in identifying suspicious data access activities. Audit logs will capture information on systems managing ePHI including user access and activity, exception reports, dormant account reports, failed login reports and unauthorized user access attempts.

C. Integrity

Data will be protected from improper alteration or destruction through encryption and proper backup storage.

D. Person or Entity Authentication

Controls will be established to verify that a person seeking access to systems containing ePHI is the actual individual authorized.

E. Transmission Security

Controls will be implemented to ensure that data transmitted over electronic communication systems will be safeguarded.