UNIVERSITY OF MAINE SYSTEM
HIPAA POLICY #42
SECURITY OF PHI – ADMINISTRATIVE SAFEGUARDS

I. Security Management Process

Each Covered Component must implement policies and procedures to prevent, detect, contain, and correct security violations, which shall include at a minimum:

A. Risk analysis (Required). The Covered Component shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the Covered Component.

B. Risk management (Required). The Covered Component shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI the Covered Component creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
4. Ensure compliance with the Security Rule by its workforce.

C. Sanction policy (Required). The Covered Component shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Covered Component.

D. Information system activity review (Required). The Covered Component shall implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

II. Assigned Security Responsibility

The Covered Component shall identify the security official within the Covered Component who is responsible for the development and implementation of the policies and procedures required by this policy.

III. Workforce Security

The Covered Component shall implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, as provided under its information access management policies and procedures, and to prevent those workforce members who do not have access under its information access management policies and procedures from obtaining access to electronic PHI.

A. Authorization and/or Supervision (Addressable). The Covered Component shall implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.

B. Workforce clearance procedure (Addressable). The Covered Component shall implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.

C. Termination procedures (Addressable). The Covered Component shall implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by determinations made under the workforce clearance procedures.

VI. Information Access Management

The Covered Component shall implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the Privacy Rule.

A. Isolating health care clearinghouse functions (Required). If the Covered Component contains a health care clearinghouse, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization.

B. Access authorization (Addressable). The Covered Component shall implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

C. Access establishment and modification (Addressable). The Covered Component shall implement policies and procedures that, based upon the component's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

V. Security Awareness and Training

The Covered Component shall implement a security awareness and training program for all members of its workforce (including management).

A. Security reminders (Addressable). The Covered Component shall issue periodic security updates.

B. Protection from malicious software (Addressable). The Covered Component shall implement procedures for guarding against, detecting, and reporting malicious software.

C. Log-in monitoring (Addressable). The Covered Component shall implement procedures for monitoring log-in attempts and reporting discrepancies.

D. Password management (Addressable). The Covered Component shall implement procedures for creating, changing, and safeguarding passwords.

VI. Security Incident Procedures

The Covered Component shall implement policies and procedures to address security incidents.

A. Response and Reporting (Required). The Covered Component shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Covered Component; and document security incidents and their outcomes.

VII. Contingency Plan

The Covered Component shall establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI.

A. Data backup plan (Required). The Covered Component shall establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.

B. Disaster recovery plan (Required). The Covered Component shall establish (and implement as needed) procedures to restore any loss of data.

C. Emergency mode operation plan (Required). The Covered Component shall establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.

D. Testing and revision procedures (Addressable). The Covered Component shall implement procedures for periodic testing and revision of contingency plans.

E. Applications and data criticality analysis (Addressable). The Covered Component shall assess the relative criticality of specific applications and data in support of other contingency plan components.

VIII. Evaluation

The Covered Component shall perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this policy, and subsequently in response to environmental or operational changes affecting the security of electronic PHI, that establishes the extent to which the Covered Component's security policies and procedures meet the requirements of the Security Rule.

IX. Business Associates

A Covered Component may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the Covered Component’s behalf only if the Covered Component obtains satisfactory assurances in the form of a written business associate contract, that the business associate will appropriately safeguard the information.

Revised 05/10/2013