UNIVERSITY OF MAINE SYSTEM
HIPAA POLICY #41
SECURITY OF PHI – GENERAL RULES

I. General Requirements

Covered Components must do the following:

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

II. Security Measures

Covered Components may use any security measures that allow the Covered Component to reasonably and appropriately implement the standards and implementation specifications as specified in the Security Rule. In deciding which security measures to use, a Covered Component must take into account the following factors:

A. The size, complexity, and capabilities of the Covered Component.
B. The Covered Component's technical infrastructure, hardware, and software security capabilities.
C. The costs of security measures.
D. The probability and criticality of potential risks to electronic PHI.

III. Implementation specifications

HIPAA Security implementation specifications set forth in these policies are identified as either required or addressable. If an implementation specification is required, the word “Required” appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word “Addressable” appears in parentheses after the title of the implementation specification.

When an implementation specification is identified as “Required,” a Covered Component must implement the implementation specification.

When an implementation specification is identified as “Addressable,” a Covered Component must--

A. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the Component's electronic PHI; and
B. As applicable to the Component--
  1. Implement the implementation specification if reasonable and appropriate; or
  2. If implementing the implementation specification is not reasonable and appropriate--
    a. Document why it would not be reasonable and appropriate to implement the implementation specification; and
    b. Implement an equivalent alternative measure if reasonable and appropriate.

IV. Maintenance

Security measures implemented to comply with standards and implementation specifications adopted under the Security Rule and these policies must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic PHI.

Revised 02/09/2010