East Carolina University
HIPAA Security Standards

Subject: Risk Management  Coverage: ECU Health Care Components
Standard #: Security-0001b  Page: 1 of 3
Supersedes:  Approved:
Effective Date: April 21, 2005  Revised: December 9, 2010,

HIPAA Security Rule Language: “Implement security measures sufficient to reduce risks and
vulnerabilities to a reasonable and appropriate level to comply with
Sec.164.306 (a).”
Regulatory Reference: 45 CFR 164.308(a)(1)(ii)(B)
Required specification

I. PURPOSE

This standard reflects East Carolina University’s commitment to select and implement
security measures to reduce the risks to its information systems containing EPHI to a
reasonable and appropriate level.

II. AUTHORIZATION AND ENFORCEMENT

Health Care component management and/or administrator(s) are responsible for
monitoring and enforcing this policy, in consultation with the ECU IT Security Officer,
ECU HIPAA Security Officer, and ECU HIPAA Privacy Officer.

III. STANDARD

East Carolina University must implement security measures that reduce the risks to its
information systems containing EPHI to reasonable and appropriate levels. Selection and
implementation of such security measures must be based on a formal, documented risk
management process.

ECU Health Care Components must conduct risk management on a continuous basis and
all selected and implemented security measures must ensure the confidentiality, integrity
and availability of information systems containing EPHI and be commensurate with the
risks to such systems.
IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

1. Security measures must be implemented to reduce the risks to information systems containing EPHI to reasonable and appropriate levels. Selection and implementation of such security measures must be based on a formal, documented risk management process. At a minimum, the risk management process must include the following:

   a. Assessment and prioritization of risks to information systems containing EPHI.
   b. Selection and implementation of reasonable, appropriate and cost-effective security measures to manage, mitigate, or accept identified risks.
   c. Workforce member training and awareness on implemented security measures.
   d. Regular evaluation and revision, as necessary, of existing security measures.

2. ECU Health Care Components must manage risk on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity and availability of information systems containing EPHI. Strategies for managing risk should be commensurate with the risk prioritization as described below to such systems, using one or more of the following methods to manage risk: risk acceptance, risk avoidance, risk limitation, or risk transference.

3. ECU Health Care Components’ risk management process must be based on the following steps, which shall be formally documented and securely maintained:

   a. **Inventory.** ECU Health Care Components must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems. ECU Health Care Components must be able to identify its information systems and the relative value and importance of those systems.
   b. **Risk prioritization.** Based on the risks defined by ECU Health Care Components’ risk analysis, risks must be prioritized on a scale from high to low based on the potential impact to information systems containing EPHI and the probability of occurrence. When deciding what ECU resources should be allocated to identified risks, highest priority must be given to those risks with unacceptably high risk rankings.
   c. **Method selection.** ECU Health Care Components must select the most appropriate security methods to minimize or eliminate identified risks to information systems containing EPHI. Such selections must be based on the nature of a specific risk and the feasibility and effectiveness of a specific method.
d. **Security method selection.** ECU Health Care Components must determine the most appropriate, reasonable and cost-effective security method(s) for reducing identified risks to information systems containing EPHI.

e. **Assignment of responsibility.** ECU workforce members who have the appropriate expertise must be identified and assigned responsibility for implementing selected security method(s).

f. **Security method implementation.** Selected security method(s) must be correctly implemented.

g. **Security method evaluation.** Selected security method(s) must be regularly evaluated and revised as necessary.

### VI. COORDINATING INSTRUCTION

1. All section policies, standards and procedures will be reviewed annually. Every section policy, standards and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other East Carolina University, University of North Carolina system, or state of North Carolina requirements may stipulate a longer retention.