I. PURPOSE

This standard reflects East Carolina University’s commitment to regularly conduct accurate and thorough analysis of the potential risks to the confidentiality, integrity, and availability of its information systems containing EPHI.

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

ECU Health Care Components must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI. The identification, definition and prioritization of risks to information systems containing EPHI must be based on a formal, documented risk analysis process. ECU Health Care Components must conduct a risk analysis of its information systems on a regular basis. Such risk analysis must be used in conjunction with ECU’s risk management process. ECU Health Care Components must also conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing EPHI.
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. ECU Health Care Components must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI.

2. The identification, definition and prioritization of risks to information systems containing EPHI must be based on a formal, documented risk analysis process. At a minimum, ECU Health Care Components’ risk analysis process must include the following:
   a. Identification and prioritization of the threats to information systems containing EPHI.
   b. Identification and prioritization of the vulnerabilities of information systems containing EPHI.
   c. Identification and definition of security measures used to protect the confidentiality, integrity, and availability of information systems containing EPHI.
   d. Identification of the likelihood that a given threat will exploit a specific vulnerability on an ECU information system containing EPHI.
   e. Identification of the potential impacts to the confidentiality, integrity, and availability of information systems containing EPHI if a given threat exploits a specific vulnerability.

3. ECU Health Care Components must conduct risk analysis on a regular basis. Such risk analysis must be used in conjunction with ECU’s risk management process to identify, select and implement security measures to protect the confidentiality, integrity, and availability of information systems containing EPHI.

4. Judgments used in ECU Health Care Components’ risk analysis, such as assumptions, defaults, and uncertainties, should be explicitly stated and documented.

5. In addition to regular risk analysis, ECU Health Care Components must conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing EPHI. Such changes include but are not limited to:
   a. Significant security incidents to specific information systems containing EPHI.
   b. Significant new threats or risks to specific information systems containing EPHI.
c. Significant changes to the organizational or technical infrastructure of ECU which affect specific information systems containing EPHI.

d. Significant changes to ECU information security requirements or responsibilities which affect specific information systems containing EPHI.

6. ECU’s risk analysis 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.

b. **Threat identification.** ECU Health Care Components must identify all potential threats to its information systems containing EPHI. Such threats may be natural, human or environmental.

c. **Vulnerability identification.** ECU Health Care Components must identify all vulnerabilities on its information systems containing EPHI. This should be done by regularly reviewing vulnerability sources and performing security assessments.

d. **Security control analysis.** ECU Health Care Components must analyze the security measures that have been implemented or will be implemented to protect its information systems containing EPHI; this includes both preventive and detective controls.

e. **Risk likelihood determination.** ECU Health Care Components must assign a rating to each specific risk which indicates the probability that a vulnerability will be exploited by a particular threat. Three factors should be considered: 1) threat motivation and capability, 2) type of vulnerability, and 3) existence and effectiveness of current security controls.

f. **Impact analysis.** ECU Health Care Components must determine the impact to confidentiality, integrity or availability of EPHI which would result if a threat were to successfully exploit a vulnerability on an ECU information system containing EPHI.

g. **Risk Determination.** ECU Health Care Components must use the information obtained in the above six steps to identify the level of risk to specific information systems containing EPHI. For each vulnerability and associated possible threat, ECU Health Care Components must make a risk determination based on:

- The likelihood a certain threat will attempt to exploit a specific vulnerability.
- The level of impact should the threat successfully exploit the vulnerability.
- The adequacy of planned or existing security controls.

**VI. COORDINATING INSTRUCTIONS**

1. All section policies and procedures will be reviewed annually. Every section policy 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.