I. PURPOSE

This policy reflects East Carolina University’s commitment to use appropriate audit controls on its information systems that contain or use 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. POLICY

ECU Health Care Components must record and examine significant activity on its information systems that contain or use EPHI. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on ECU information systems that contain or use EPHI.

IV. APPLICABILITY

This policy 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

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. ECU Health Care Components must record and examine significant activity on its information systems that contain or use EPHI. ECU Health Care Components must identify, define, and document what constitutes “significant activity” on a specific information system. Such activity might include:
   - User access to EPHI and user account activity
   - Use of certain software programs or utilities
   - Use of a privileged account
   - Healthcare computing system anomalies, such as unplanned system shutdown or application errors
   - Failed and successful authentication attempts

2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on ECU healthcare systems that contain or use EPHI. At a minimum, such mechanisms must provide the following information:
   - Date and time of activity
   - Origin of activity
   - Identification of user performing activity
   - Description of attempted or completed activity

3. ECU Health Care Components must develop and implement a formal process for audit log review. At a minimum, the process must include:
   - Definition of which workforce members will review records of activity
   - Definition of what activity is significant
   - Procedures defining how significant activity will be identified and reported
   - Procedures for preserving records of significant activity

4. When possible, ECU Health Care Components workforce members should not review audit logs that pertain to their own system activity. In addition, workforce members should not have the ability to alter or delete log entries that pertain to their own system activity. If it is not possible to limit this access, management should ensure that appropriate compensating controls are documented and implemented.

VI. COORDINATING INSTRUCTIONS

All section policies, standards and procedures will be reviewed annually. Every section policy, standard 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.
HIPAA Security Policy # 0012: Audit Controls

Other East Carolina University, University of North Carolina system, or state of North Carolina requirements may stipulate a longer retention period.