I. PURPOSE

This standard reflects East Carolina University’s commitment to conduct an annual analysis of the criticality of its healthcare computing systems.

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 have a formal process for defining and identifying the criticality of its healthcare computing systems and the data contained within them. The prioritization of ECU information systems must be based on an analysis of the impact to ECU services, processes, and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time. The criticality analysis must be conducted with significant involvement from the administrators, users, and owners of ECU information systems and business processes. The criticality analysis must be conducted at least annually.

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 have a formal, documented process for defining and identifying the criticality of its information systems and the data contained within them. At a minimum, the process must include:

   - Creating an inventory of interdependent systems and their dependencies.
   - Documenting the criticality of ECU’s information systems (e.g. impact on patient care).
   - Identifying and documenting the impact to Health Care Component services, if specific ECU information systems are unavailable for different periods of time (e.g. 1 hour, 1 day).
   - Identifying the maximum time periods that healthcare computing systems can be unavailable.
   - Prioritizing healthcare computing system components according to their criticality to the Health Care Component’s ability to function at normal levels.

2. The criticality analysis must be conducted at least annually. The criticality analysis report must be securely maintained.

VI. COORDINATING INSTRUCTIONS

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