I. PURPOSE

This policy reflects East Carolina University’s commitment to ensure the confidentiality, integrity, and availability of its information systems containing electronic protected health information (EPHI) by implementing policies and procedures to prevent, detect, mitigate, and correct security violations.

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 ensure the confidentiality, integrity and availability of its information systems containing EPHI by implementing appropriate and reasonable policies, procedures and controls to a) prevent, b) detect, c) mitigate, and d) correct security violations.

ECU Health Care Components’ security management programs must be based on formal and regular processes for risk analysis and management, sanction policies for non-compliance, information system activity review, and training and awareness of workforce members regarding security policies, procedures, and controls.
All ECU workforce members are responsible for appropriately protecting EPHI maintained on ECU information systems from unauthorized access, modification, destruction, and disclosure.

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 within a Health Care Component 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 regularly identify, define and prioritize risks with respect to the confidentiality, integrity, and availability of its information systems containing EPHI, as specified in the Risk Analysis Standard.

2. ECU Health Care Components must implement security measures that reduce the risks to its information systems containing EPHI to reasonable and appropriate levels, as specified in the Risk Management Standard.

3. ECU Health Care Components must apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures, as specified in the Sanction Standard.

4. ECU Health Care Components must regularly review records of activity on information systems containing EPHI, as specified in the Information System Activity Review Standard.

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.