I. PURPOSE

This policy reflects East Carolina University’s commitment to assign a single employee overall final responsibility for the confidentiality, integrity, and availability of its 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’s Information Security Officer is responsible for the development and implementation of all policies and procedures necessary to appropriately protect the confidentiality, integrity, and availability of ECU information systems and EPHI.

IV. APPLICABILITY

This policy is applicable for ECU Administration. This policy’s scope includes all protected health information in electronic form.

V. PROCEDURE

The ECU Information Security Officer’s responsibilities include, but are not limited to:
HIPAA Security Policy # 0002: Assigned Security Responsibility

1. Ensure that ECU information systems comply with all applicable federal, state, and local laws and regulations.
2. Ensure that no ECU information system compromises the confidentiality, integrity, or availability of any other ECU information system.
3. Develop, document, and ensure dissemination of appropriate security policies, procedures, and standards for the users and administrators of ECU information systems and the data contained within them.
4. Ensure that newly acquired ECU information systems have features that support required and/or addressable security Implementation Specifications.
5. Coordinate the selection, implementation, and administration of significant ECU security controls.
6. Ensure ECU workforce members receive regular security awareness and training.
8. Develop and implement an effective risk management program.
9. Regularly monitor and evaluate threats and risks to ECU information systems.
10. Develop and monitor/audit records of ECU information systems’ activity to identify inappropriate activity.
11. Maintain an inventory of all ECU information systems that contain EPHI.
12. Create an effective security incident response policy and related procedures.
13. Ensure adequate physical security controls exist to protect ECU’s EPHI.
14. Coordinate with ECU’s Privacy Officer to ensure that security policies, procedures and controls support compliance with the HIPAA Privacy Rule.
15. Evaluate new security technologies that may be appropriate for protecting ECU’s information systems.

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.