I. PURPOSE

This policy reflects East Carolina University’s commitment to appropriately control healthcare computing systems and their associated electronic media containing EPHI moving into, out of and within its facilities.

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 EPHI located on ECU’s healthcare computing systems and their associated electronic media must be protected against damage, theft, and unauthorized access. EPHI must be consistently protected and managed through its entire life cycle, from origination to destruction.

ECU Health Care Components must regularly conduct a formal, documented process that ensures consistent control of all healthcare computing systems and their associated electronic media containing EPHI that is created, sent, received or destroyed. The

HIPAA Security Rule Language: “Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.”

Regulatory Reference: 45 CFR 164.310(d)(1)
HIPAA Security Policy #0010: Device And Media Controls

destruction of any EPHI should be governed by the university’s Data Retention Policy or the applicable healthcare components’ Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the University Privacy Officer.

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

1. All ECU healthcare computing systems and their associated electronic media containing EPHI must be located and stored in secure environments that are protected by appropriate security barriers and entry controls.

2. As defined in ECU’s Disposal Standard, all healthcare computing systems and their associated electronic media containing EPHI must be disposed of securely and safely when no longer required. The destruction of any EPHI should be governed by the university’s Data Retention Policy or the applicable healthcare components’ Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the University Privacy Officer.

3. As defined in ECU’s Media Re-use Standard, all EPHI on ECU healthcare computing systems and their associated electronic media must be carefully removed before the media or healthcare computing systems are made available for re-use.

4. As defined in ECU’s Accountability Standard, all healthcare computing systems and their associated electronic media containing EPHI that is received by or removed from a sensitive area must be appropriately tracked and logged.

5. As defined in ECU’s Data Backup and Storage Standard, backup copies of all EPHI located on ECU healthcare computing systems or their associated electronic media must be regularly made and stored securely.

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.