I. PURPOSE

This policy reflects East Carolina University’s commitment to appropriately protect the confidentiality, integrity, and availability of all EPHI that it transmits over electronic communications networks.

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 appropriately protect the confidentiality, integrity, and availability of all EPHI it transmits over electronic communications networks.

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 that is accessed remotely by healthcare workers.
V. PROCEDURE

1. As defined in ECU’s Integrity Controls Standard, ECU Health Care Components must use integrity controls where appropriate to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

2. As defined in ECU’s Encryption Standard, ECU Health Care Components must use encryption where appropriate to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

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.