I. PURPOSE

This policy reflects East Carolina University’s commitment to the protection of portable devices and all electronic protected health information (EPHI) that is stored or accessed by such devices.

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 implement appropriate controls to ensure the protection of portable devices that store or access EPHI.
IV. APPLICABILITY

This policy is applicable to all workforce members, departments, and health care components that use or disclose electronic protected health information for any purpose. This policy’s scope includes all protected health information in electronic form. This policy applies to all handheld devices whether University owned or personal that are used to access, transmit or store EPHI. It includes but is not limited to: 1) Digital Organizers 2) Personal Digital Assistants (PDA) 3) Smart Phones 4) Wireless E-mail Devices 5) USB Drives 6) Laptops and any other portable device used to store or access protected health information.

V. VIOLATIONS

1. Violators of this policy are subject to the sanctions as defined in the ECU HIPAA Privacy Policy, Sanctions - #0002, HIPAA Security Policy, STD0001c-SANPOL, Academic Computer Use Policy, University Student and Employee Computer Use Policy and all other applicable University sanctions.

2. Sanctions can include but are not limited to:
   a. Suspension
   b. Required retraining
   c. Letter of reprimand
   d. Termination

VI. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

As defined in ECU’s EPHI Portable Device Security Standard #0017, ECU Health Care Components must ensure all workforce members follow the appropriate portable device security guidelines that describe who can use the devices, purpose of use, how it is to be used and appropriate security measures that must be implemented. Health Care Components who can not implement the safeguards recommended in EPHI Portable Device Security Standard #0017 must provide other compensating controls. All compensating controls must be reviewed and approved by the HIPAA Privacy and Security Officers in advance of implementation.

VII. 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.