I. PURPOSE

This standard reflects East Carolina University’s commitment to the protection of portable devices and all electronic protected health information (EPHI) 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. 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

IV. STANDARD

ECU Health Care Components must implement appropriate controls to ensure the protection of portable devices that store or access EPHI.

V. APPLICABILITY

This Standard is applicable to all workforce members within any ECU Health Care Component who use or disclose EPHI for any purpose. This Standard’s scope includes all protected health information in electronic form. The safeguards in this Standard apply to all handheld devices whether University-owned or individually-owned and that are used to access, transmit or store EPHI which include but are not limited to: Digital Organizers, Personal Digital Assistants (PDA), Smart Phones, Wireless E-mail Devices, USB Drives Laptops, and any other portable device used to store or access EPHI.

VI. PROCEDURE

The following safeguards must be implemented to satisfy the requirements of this standard:

1. ECU Health Care Components who cannot implement the safeguards recommended in this Standard must provide other acceptable compensating controls. All compensating controls must be reviewed and approved by the HIPAA Privacy and Security Officers in advance of implementation.

2. All EPHI stored on handheld computing or portable storage devices must be encrypted as required by ECU HIPAA Security Policy # Security-0016, Healthcare Workforce Acceptable Use Policy.

3. EPHI shall remain on the device only as long as necessary.

4. Whenever possible, EPHI shall be discarded or transferred to a designated secure storage area.

5. Whenever possible, any health information stored on handheld computing or portable storage device shall be in a de-identified form. Information such as names, date of birth, social security numbers, medical record numbers or other individual identifiable information as outlined in the ECU HIPAA Privacy policy, De-Identified Information, #0013.
6. Software applications used to access EPHI which will be loaded onto any portable device that houses, transmits, or accesses EPHI must be approved in advance by the HIPAA Workgroup Committee.

7. Syncing of the device will be restricted to ECU desktops authorized and configured to access EPHI on campus.

8. ECU Healthcare Components must implement appropriate physical security safeguards to prevent the loss or theft of portable devices. Such safeguards should include but are not limited to:
   a. Activate locking software when device is unattended
   b. Keep the device with you at all times when traveling
   c. Keep the device in a locked location when not in use

9. Infrared and Bluetooth communication must be disabled while the device is established in a network which allows access to EPHI.

10. At a minimum the following safeguards must be implemented when accessing EPHI over a wireless network:
   a. Wireless users must authenticate through the secure ECU Buccaneer wireless network prior to accessing network resources.
   b. Wireless communications must be encrypted when accessing EPHI. Two possible encryption alternatives for on campus or remote connectivity include the university’s Citrix system for access to Centricity EMR and the university’s Virtual Private Network (VPN).

11. Any loss, theft or suspected unauthorized use of the device must be reported immediately to the ITCS Help Desk and ECU Police.

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.