I. PURPOSE

This policy reflects East Carolina University’s commitment to inform ECU Health Care Components and ECU workforce members of their responsibilities to protect the confidentiality, integrity and availability of the University’s electronic protected health information (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 workforce members are responsible for taking all reasonable precautions to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI) for which they have access. In addition, ECU workforce members must receive appropriate security training before accessing EPHI on any ECU healthcare computing system, workstation, or other electronic device. Non-compliance with this policy can lead to the application of the health care components’ and / or university’s sanctions policies.
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 purposes. This policy’s scope includes all protected health information in electronic form.

V. PROCEDURE

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

1. Your Role in Protecting EPHI: You are responsible for taking all reasonable precautions to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI) for which you have access. At a minimum these precautions require that you:
   - Must not share your account or your password: All activities associated with your assigned user account are your responsibility
   - Must report any suspicious activity involving your account or other systems with access to EPHI
   - Must not circumvent or otherwise bypass existing security measures: For example, do not disable anti-virus or firewall software

2. HIPAA Security Training: You must receive training on HIPAA security issues before accessing your computer accounts or ECU information systems containing EPHI. In addition, you must attend training on an annual basis or more frequently as needed. Such training will consist of, but is not limited to:
   - Responsibilities of workforce members for protecting EPHI
   - Security best practices (e.g. how to choose a good password, how to report a security incident).
   - ECU information security policies and standards

3. Protecting Your Workstation: You must protect your workstation and the EPHI for which you have access from unauthorized access. Workstations are defined in this policy as desktop computers, laptops, personal digital assistants (PDA), and other electronic devices that you may use to access EPHI. At a minimum, you:
   - Must not open email attachments without verifying with the sender
   - Must not download or install any software not required for official job duties
   - Must ensure anti-virus software is installed and regularly updated
   - Must ensure that your workstation is physically located in a manner that minimizes the risk that unauthorized individuals can gain access: In addition, be sure that your monitor or display screen is positioned to prevent viewing by unauthorized individuals
   - Must log off from your workstation when your shift is complete.
   - Must ensure that your workstation is locked when unattended: This may be done manually or by automated screen locking software
• Must store all media (e.g., diskettes, zip disks, and flash drives) that contain EPHI in a secure location: When disposing of media with EPHI, the data must be removed with data sanitizing software or the media must be physically destroyed.

4. Storing EPHI on your workstation: If possible, do not store EPHI on your workstation. Use other alternatives, such as storing the EPHI on a secure server or a secure network storage device. However, if you store EPHI on your workstation, the following requirements apply to you:

- You must obtain approval from your department head prior to storing EPHI on your workstation.
  - Your departmental management must inventory and document the EPHI stored on your workstation at least on an annual basis.
  - Your departmental management must review and document the security safeguards for protecting the EPHI stored on your workstation.
- You must encrypt the data files containing EPHI wherever possible.
  - If encryption is not possible, you must obtain a review by the HIPAA Security and Privacy Officer prior to storage.
- If you are storing EPHI on a portable device, such as a laptop or PDA, you must encrypt the data to protect it from unauthorized disclosure in the event that the device is lost or stolen. Refer to the HIPAA Portable Device Security Policy # 0017 for additional information.

5. Email and EPHI: Do not send EPHI over email unless you take reasonable precautions to protect the EPHI. At a minimum you must (a) you send the email from your ECU email account on the university’s enterprise email system to another ECU email account on the university’s enterprise email system and implemented the appropriate privacy controls or (b) you send email from your ECU email account to locations outside of the enterprise email system, implemented the appropriate privacy controls and encrypted the email with an ITCS recommended encryption solution. Refer to HIPAA Privacy Policies, or contact the HIPAA Privacy Officer if you have questions concerning privacy requirements. Refer to the IT Security Data Encryption web page or contact ITCS @ 328-9866 if you have questions concerning email encryption. NOTE: Vidant Health is considered outside of the university enterprise email system.

6. Wireless Networking and EPHI: Do not access or send EPHI over a wireless network, unless the data is encrypted prior to transmission. Logging into the secure ECU Buccaneer wireless network while on campus will provide the required encryption. 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). Data sent over a unencrypted wireless network can be captured by unauthorized persons in nearby buildings, parking lots, and streets.

7. Non-compliance with this policy can lead to the application of the health care components’ and / or university’s sanctions policies.
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.