I. PURPOSE

This standard reflects East Carolina University’s commitment to ensure that all workforce members who can access ECU information systems containing EPHI are appropriately authorized or supervised.

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. STANDARD

ECU Healthcare Components must ensure that all workforce members who can access ECU information systems containing EPHI are appropriately authorized and/or supervised.

ECU Healthcare Components must have a formal documented process for granting authorization to access to ECU information systems containing EPHI. The type and extent of access granted to ECU information systems containing EPHI must be based on review by the system owners/stewards or their designated delegates. Access to ECU information systems containing EPHI must be authorized only for ECU workforce members having a need for specific information in order to accomplish their respective job responsibilities.
Before third-party persons are granted access to ECU information systems containing EPHI or ECU locations where EPHI can be accessed, a review by the system owners/stewards or their designated delegates must be conducted. Access by third-party persons to ECU information systems containing EPHI or ECU locations where EPHI can be accessed, must be allowed only after appropriate security controls have been implemented and an agreement has been signed defining the terms for access. Whenever appropriate, third-party persons should be supervised by an appropriate ECU employee.

IV. APPLICABILITY

This standard 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

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

1. Appropriate ECU information system stewards/owners or their chosen delegates must define and authorize all access to ECU information systems containing EPHI. Such information system owners and delegates must be formally designated and documented as specified in the Access Authorization Standard.

2. The type and extent of access granted to ECU information systems containing EPHI must be based on specifications in the Access Establishment and Modification Standard.

3. Before third party persons are granted access to ECU information systems containing EPHI or ECU locations where EPHI can be accessed; review by the system owners/stewards or their designated delegates must be performed. At a minimum, the review must consider the following factors:

   - Type of access required
   - Sensitivity of the EPHI on the information system
   - Security controls on the information system
   - Security controls used by the third party

4. Access by third party persons to ECU information systems containing EPHI or ECU locations where EPHI can be accessed must be allowed only after appropriate security controls have been implemented and an agreement has been signed defining the terms for access. The agreement must define the following:

   - The security processes and controls necessary to ensure compliance with ECU’s security policies.
Restrictions regarding the use and disclosure of ECU data.
ECU’s right to monitor and revoke third party persons’ access and activity.

5. Where appropriate, third party persons should be supervised by an appropriate ECU employee when they are accessing ECU information systems containing EPHI or in an ECU location where EPHI might be accessed.

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 systems, or state of North Carolina requirements may stipulate a longer retention.