HIPAA Access Control

Authority: Chancellor

History:

Contact for Info: Office of Institutional Integrity, 252-744-5200

1. Purpose

1.1. This policy reflects East Carolina University’s commitment to implement policies and procedures for HIPAA Systems to allow access only to those persons or software programs that have been granted access rights. Compliance of this policy is in accordance with the Security Rule of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). All University units that have been designated as “Health Care Components” must comply with the requirements set forth in this policy as outlined by the final HIPAA Security Rule.

2. Definitions

2.1. HIPAA Security Rule - establishes national standards to protect individuals’ electronic Protected Health Information (ePHI) that is created, received, transmitted, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

2.2. electronic Protected Health Information (ePHI) – individually identifiable health information which is created, received, transmitted, or maintained in electronic form.

2.3. Health Care Component – a component of a covered entity designated by the entity that functions as a health care provider, as defined by HIPAA.

2.4. HIPAA System – defines any hardware, software, server, workstation, or mobile device that a Health Care Component uses in the course of its daily functions to create, receive, transmit, or maintain ePHI.
2.5. **HIPAA System Administrator** – a full time ECU faculty or staff member that oversees a device or system (HIPAA system) that creates, receives, transmits or maintains ePHI. This person has been designated by his/her department or clinic as the system administrator for the HIPAA system.

2.6. **Workforce** – employees, volunteers, trainees, learners, faculty, students, and other persons whose conduct in the performance of work for an ECU Health Care Component, is under the direct control of such ECU Health Care Component, whether or not they are paid by the ECU Health Care Component.

2.7. **Access** – the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource, as defined by the HIPAA Security Rule for this subpart.

3. **Regulations**

3.1. **Access Control (164.312(a)(1))** – implement technical policies and procedures for HIPAA Systems to allow access only to those persons or software programs that have been granted access rights as specified in the HIPAA Information Access Management Policy. This standard is comprised of four (4) regulatory specifications: Unique User Identification, Emergency Access Procedure, Automatic Logoff, and Encryption and Decryption.

3.1.1. **Unique User Identification (required)** – assign a unique name and/or number for identifying and tracking user identity.

3.1.2. **Emergency Access Procedure (required)** – establish and implement as needed, procedures for obtaining necessary ePHI during an emergency.

3.1.3. **Automatic Logoff (addressable)** – implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

3.1.4. **Encryption and Decryption (addressable)** – implement a mechanism to encrypt and decrypt ePHI.

4. **Procedure**
4.1. Unique User Identity

4.1.1. HIPAA System Administrators must grant users access to HIPAA Systems via unique identifiers that identify workforce members or users and allow activities performed on HIPAA Systems to be traced back to a particular individual through tracking of unique identifiers.

4.1.2. Unique identifiers must not give any indication of the user’s privilege level.

4.1.3. All Health Care Component users must authenticate their identity by providing something they know or have, such as a password, personal identification number (PIN), token, or biometric feature.

4.1.4. Where Health Care Components cannot implement unique user IDs for specific HIPAA Systems, they must implement appropriate compensating controls, such as maintaining a list of personnel with access to and knowledge of the credentials used to access the HIPAA System, and the changing of the “generic” credentials used to access the specific HIPAA System whenever a person with knowledge of the credentials transfers or is no longer employed.

4.2. Emergency Access Procedure

4.2.1. Health Care Components must have a formal, documented emergency access procedure enabling authorized workforce members to obtain required ePHI during an emergency.

4.2.2. At a minimum the procedure must: identify and define manual and automated methods to be used by authorized workforce members to access ePHI during an emergency and identify and define appropriate logging and auditing that must occur when authorized workforce members access ePHI during an emergency.

4.3. Automatic Logoff

4.3.1. Where possible Health Care Components must implement a method to perform an automatic logoff for inactive HIPAA System sessions.
4.3.2. Where Health Care Components cannot implement a method to perform an automatic logoff for inactive HIPAA Systems, they must implement automatic locking on all workstations used to access those systems.

4.3.3. Where Health Care Components utilize a shared workstation for clinical operations, there will be an automatic time-out for the application.

4.4. Encryption and Decryption

4.4.1. Health Care Components must consider the following factors, at a minimum, in determining whether or not specific ePHI must be encrypted on a HIPAA System: the sensitivity of the ePHI, the risks to the ePHI, the expected impact to ECU functionality and work flow if the ePHI is encrypted, and alternative methods available to protect the confidentiality, integrity, and availability of the ePHI.