HIPAA Workforce Security

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 allow HIPAA systems access only to workforce members who have been appropriately authorized. The type and extent of access authorized to HIPAA systems must be based on review by the system stewards/owners (or their designated delegates). 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. 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.

3. Regulations

3.1. Workforce Security (164.308(a)(3)) – Access to HIPAA systems must be granted only to
properly trained ECU workforce members who have a need for ePHI in order to accomplish a
legitimate task. This standard is comprised of three (3) regulatory specifications: Authorization
and/or Supervision, Workforce Clearance Procedure, and Termination Procedures.

3.1.1. Authorization and/or Supervision (addressable) - ECU departments must ensure
only authorized and properly trained users access ePHI located on ECU computing
systems and their associated electronic media; the level of access must be limited to the
minimum required to perform business function; users must be adequately trained to
perform required business functions and complete HIPAA privacy and/or security
requirements as determined.

3.1.2. Workforce Clearance Procedure (addressable) - Implement procedures to determine
that the access of a workforce member to ePHI is appropriate.

3.1.3. Termination Procedures (addressable) - Implement procedures for terminating access
to ePHI when the employment of a workforce member ends or as required by
determinations made as specified in the Workforce Clearance Procedure (4.2) section of
this policy.

4. Procedure

4.1. Authorization and/or Supervision

4.1.1. Appropriate HIPAA system stewards/owners, or their chosen delegates, must define and
authorize all access to HIPAA systems.

4.1.2. Appropriate HIPAA system stewards/ owners, or their chosen delegates, must specify the
type and extent of access granted to users on HIPAA systems.
4.1.3. Before third party persons are granted access to HIPAA systems or ECU locations where ePHI can be accessed, review and approval by the system stewards/owners, or their designated delegates, is required. At a minimum, the review must consider the following factors: type of access required, sensitivity of the ePHI on the HIPAA system, security controls on the HIPAA system, and security controls used by the third party.

4.1.4. Access by third party persons to HIPAA systems 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, and ECU’s right to monitor and revoke third party persons’ access and activity.

4.1.5. Where appropriate, third party persons should be supervised by an appropriate ECU employee when they are accessing HIPAA systems or in an ECU location where ePHI might be accessed.

4.2. **Workforce Clearance Procedure**

4.2.1. Health Care Components must identify the appropriate level of access required by all workforce members who access HIPAA systems. Such access must be formally documented and securely maintained.

4.2.2. The background of all ECU workforce members must be adequately reviewed during the hiring process. Verification checks include, but are not limited to character references and criminal background checks.

4.2.3. When defining a position, the Health Care Component and the hiring manager must identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of HIPAA systems or processes containing ePHI.
4.3. Termination Procedures

4.3.1. Health Care Components must create and implement a formal, documented process for terminating or editing access to ePHI when the employment or job responsibility of a workforce member ends or changes.

4.3.2. When the employment of Health Care Component workforce members ends, his/her HIPAA systems privileges, both internal and remote, must be disabled or removed by the time of departure. Consideration should also be given to physical access to areas where ePHI is located.

4.3.3. When workforce members depart from ECU, they must return all ECU supplied equipment (PCs, Mobile/Portable Devices, OneCard, Keys, etc.) by the time of departure. The return of all such equipment must be tracked and logged.

4.3.4. If a departing workforce member has used cryptography on ECU data, they must make the cryptographic keys available to appropriate management by the time of departure.

4.3.5. As appropriate, all physical security access codes (PIN, FOB) used to protect HIPAA systems that are known by a departing workforce member must be deactivated or changed. For example, the PIN to a keypad lock that restricts entry to an ECU facility containing HIPAA systems must be changed if a workforce member who knows the PIN departs.

4.3.6. A workforce member who departs from ECU must not retain, give away, or remove from ECU premises any HIPAA information (ePHI).

4.3.7. Prior to the departure of a terminating ECU Health Care Component workforce member, his/her computers’ resident files must be promptly reviewed by his/her immediate supervisors to determine the appropriate transfer or disposal of any confidential information.

4.3.8. If a workforce member is to be terminated immediately, his/her HIPAA system privileges must be removed or disabled just before they are notified of the termination.
4.3.9. Health Care Components or their designees must periodically review HIPAA system access privileges to ensure that this policy is being adhered to and that existing procedures are effective.