HIPAA Information Access Management

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 have a formal documented process for authorizing appropriate access to its HIPAA systems. 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. **Information Access Management (164.308(a)(4))** – ECU Health Care Components must have a formal, documented process for establishing, documenting, reviewing, and modifying access to its HIPAA systems. This standard is comprised of two (2) regulatory specifications: Access Authorization and Access Establishment and Modification.

3.1.1. **Access Authorization (addressable)** - Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

3.1.2. **Access Establishment and Modification (addressable)** - Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

4. Procedure

4.1. Access Authorization

4.1.1. Health Care Components must have a formal documented process for granting access to HIPAA systems. At a minimum, the process must include:

4.1.1.1. Procedure for granting access to HIPAA systems.

4.1.1.2. Procedure for tracking and logging authorization of access to HIPAA systems.

4.1.1.3. Procedure for regularly reviewing and revising, as necessary, authorization of access to HIPAA systems.

4.1.2. HIPAA system stewards/owners or their chosen delegates must define and authorize all access to HIPAA systems that are entrusted to them. Such HIPAA system stewards/owners and delegates must be formally designated and documented.
4.1.3. Access to HIPAA systems must be authorized only for workforce members having a need for specific information in order to accomplish a legitimate task for their job. Access must not be allowed until properly authorized. All such access must be defined and documented as specified in the Access Establishment and Modification (4.2) section of this policy. Such access must also be regularly reviewed and revised as necessary.

4.1.4. Workforce members must not willfully attempt to gain access to HIPAA systems for which they have not been given proper authorization.

4.2. Access Establishment and Modification

4.2.1. Health Care Components must have a formal, documented process for establishing, documenting, reviewing, and modifying access to HIPAA systems.

4.2.2. Only properly authorized and trained workforce members may access HIPAA systems. Such access must be established via a formal, documented process.

4.2.3. Where appropriate, security controls or methods that allow access to be established to HIPAA systems must include, at a minimum: unique user identifiers (user IDs), prompt removal or disabling of access methods for persons and entities that no longer need access to ePHI, and verification that redundant user identifiers are not issued.

4.2.4. Access to HIPAA systems must be limited to workforce members who have a need for specific ePHI in order to perform their job responsibilities.

4.2.5. Appropriate HIPAA system owners/stewards, or their designated delegates, must regularly review workforce member access rights to HIPAA systems to ensure that they are provided only to those who have a need for specific ePHI in order to accomplish a legitimate task. Such rights must be revised as necessary.

4.2.6. All revisions to workforce member access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information: date and time of revision, identification of workforce member whose access is being revised, brief
description of revised access right(s), and reason for the revision. This information must be securely maintained.