HIPAA Facility Access Controls

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 to limit physical access to HIPAA systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. 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.

2.6. **Facility** – the physical premises and the interior and exterior of a building(s).

3. **Regulations**

3.1. **Facility Access Controls (164.310(a)(1))** – Health Care Components must appropriately limit physical access to the HIPAA systems contained within its facilities while ensuring that properly authorized workforce members can physically access such systems. HIPAA systems must be physically located in such a manner as to minimize the risk that unauthorized persons can gain access to them. The level of protection must be commensurate with that of identified risks. This standard is comprised of four (4) regulatory specifications: Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, and Maintenance Records.

3.1.1. **Contingency Operations (addressable)** – establish and implement as needed, procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operation Plan in the event of a disaster or emergency.

3.1.2. **Facility Security Plan (addressable)** – implement policies and procedures to safeguard the facility and the HIPAA systems from unauthorized physical access, tampering, and theft.

3.1.3. **Access Control and Validation Procedures (addressable)** – implement procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision.
3.1.4. **Maintenance Records (addressable)** – implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

4. **Procedure**

4.1. **Contingency Operations**

4.1.1. Health Care Components must ensure that, in the event of a disaster or emergency, appropriate persons can enter its facility to take necessary actions defined in its Disaster Recovery and Business Continuity Plans.

4.1.2. Based on its Disaster Recovery and Business Continuity Plans, Health Care Components must develop, implement, and regularly review a formal, documented procedure that ensures that authorized employees can enter the facility to enable continuation of processes and controls that protect ePHI (HIPAA systems) while the Health Care Component is operating in emergency mode.

4.1.3. In the event of an emergency, only authorized ECU employees may administer or modify processes and controls which protect ePHI (HIPAA systems). Such employees or roles must be defined in the Health Care Components’ Disaster Recovery and/or Business Continuity Plans.

4.2. **Facility Security Plan**

4.2.1. Health Care Components must maintain, and regularly review, a formal documented facility security plan that describes how its facilities and HIPAA systems within them will be appropriately protected. The plan must be revised as necessary.

4.2.2. At a minimum, Health Care Components’ facility security plan must address the following:

4.2.2.1. Identification of HIPAA systems to be protected from unauthorized physical access, tampering, and/or theft.
4.2.2.2. Identification of processes and controls used to protect HIPAA systems from unauthorized physical access, tampering, and/or theft.

4.2.2.3. Actions to be taken if unauthorized physical access, tampering, and/or theft attempts are made against HIPAA systems.

4.2.2.4. A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

4.3. Access Control and Validation Procedures

4.3.1. Health Care Components will identify and document all organizational or functional areas considered sensitive due to the nature of the ePHI that is stored or available within them.

4.3.2. After documenting sensitive areas, access rights to such areas should be given only to workforce members who have a need for specific physical access in order to accomplish a legitimate task.

4.3.3. All visitors to sensitive facilities where HIPAA systems are located must show proper identification, state reason for need to access, and sign in prior to gaining access.

4.3.4. Workforce members must immediately report to appropriate management the loss or theft of any device (e.g. one card or token) that enables them to gain physical access to such sensitive facilities.

4.3.5. Workforce members must wear an identification badge (one card) when at ECU facilities where HIPAA systems are located and should be encouraged to report unknown persons not wearing such identification to the appropriate authority.

4.3.6. All access rights to ECU facilities where HIPAA systems are located or software programs that can access HIPAA systems must be regularly reviewed and revised as necessary.

4.4. Maintenance Records
4.4.1. Health Care Components must document all repairs and modifications to the physical components of its facilities where HIPAA systems are located. Physical components include, but are not limited to: electronic card access systems, locks, doors, and walls.

4.4.2. Health Care Components must conduct an inventory of all the physical components within its facilities that are related to the protection of HIPAA systems on an annual basis at a minimum. Inventory results must be documented and stored in a secure manner.

4.4.3. Repairs or modifications to any ECU physical component listed in the above inventory must be documented. At a minimum, the documentation must include: date and time of repair or modification, reason for repair or modification, person(s) performing the repair or modification, and outcome of repair or modification.