HIPAA Audit 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 use appropriate audit controls on 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. 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.

2.8. **Significant Activity** – successful log-ins, failed log-in attempts, after-hours log-ins and administrative actions to HIPAA Systems.

3. **Regulations**

3.1. **Audit Controls (164.312(b))** – implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. The Audit Controls standard does not have any regulatory specifications, but like all standards must be implemented.

4. **Procedure**

4.1. **Audit Controls**

4.1.1. HIPAA System Administrators, in collaboration with ITCS, must record and examine significant activity on its HIPAA Systems.

4.1.2. Where appropriately identified, hardware, software, or procedural auditing mechanisms must be implemented on HIPAA Systems. At a minimum, such mechanisms must provide the following information: date and time of activity, origin of activity, identification of user performing the activity, and description of attempted or completed activity.

4.1.3. Health Care Components, in collaboration with ITCS, must develop and implement a formal process for audit log review. At a minimum, the process must include: definition of which workforce members will review records of activity, definition of what activity is
significant, procedures defining how significant activity will be identified and reported, and procedures for preserving records of significant activity.

4.1.4. Workforce members should not review audit logs that pertain to their own system activity. In addition, workforce members should not have the ability to alter or delete log entries that pertain to their own system activity. If it is not possible to limit this access, management should ensure that appropriate compensating controls are documented and implemented.