HIPAA Security Incident Procedures

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 quickly and effectively detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of the University’s 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. **Security incident** – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

3. **Regulations**

3.1. **Security Incident Procedures (164.308(a)(6)** - ECU Health Care Components must have a formal, documented process for quickly and effectively detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of the University’s information systems. There is one (1) regulatory specification for this standard: Response and Reporting.

3.1.1. **Response and Reporting (required)** – ensure procedures are in place to report a security incident in a timely manner to reduce the impact of the incident.

4. **Procedure**

4.1. It is the responsibility of the HIPAA System Administrator to have a process for detecting security incidents. This may include, but is not limited to: regular review of data access logs, system alert messages, and other application anomalies.

4.2. Workforce members must report suspected security incidents to the ECU ITCS Help Desk and the affected HIPAA system responsible parties immediately.

4.3. It is the responsibility of the HIPAA System Administrator, along with ITCS, to document the security incident, to include at a minimum: name of person(s) conducting the incident response.
investigation, description of the data and the computing system affected by the incident, time and date of the incident, damage to the data and the computing system(s), suspected cause of the incident, actions taken to mitigate damage and restore the data and/or computing system, and recommendations for further actions to enhance security of ePHI.

4.4. Upon completion of the incident investigation, the incident response investigator(s) will submit the documentation to the ITCS Security Officer and provide a copy to the HIPAA Security Office.