HIPAA Security Awareness and Training

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 provide regular security awareness and training to its workforce members. 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. Security Awareness and Training (164.308(a)(5)) – ECU must develop, implement, and regularly review a formal, documented program for providing appropriate HIPAA security awareness and training to its workforce members. All Health Care Components’ workforce members must be provided with sufficient training and supporting reference materials to enable them to appropriately protect ePHI on HIPAA systems. ECU’s HIPAA Business Associates must adhere to the HIPAA security rule per the regulations. This standard is comprised of four (4) regulatory specifications: Security Reminders, Protection from Malicious Software, Log-in Monitoring, and Password Management.

3.1.1. Security Reminders (addressable) – covered entities must provide periodic security updates to remind the workforce of current policies and procedures as well as a formal retraining on security policies and procedures.

3.1.2. Protection from Malicious Software (addressable) – implement procedures for guarding against, detecting, and reporting malicious software.

3.1.3. Log-in Monitoring (addressable) – implement procedures for monitoring log-in attempts and reporting discrepancies.

3.1.4. Password Management (addressable) – implement procedures for creating, changing, and safeguarding passwords.

4. Procedure

4.1. Security Reminders

4.1.1. ECU must periodically distribute security reminders to all of its workforce members.

4.1.2. Security reminders will address security topics that include, but are not limited to, the following: information security policies, information security controls and processes, risks
to HIPAA systems and ePHI, security best practices, or ECU’s information security legal and business responsibilities.

4.1.3. In addition to providing regular security reminders, ECU must provide security information and awareness to all of its workforce members when any of the following events occur: revisions to ECU’s information security policies or procedures, new information security controls are implemented at ECU, changes to information security controls, changes in legal or business responsibilities, or new threats or risks to ePHI.

4.2. Protection from Malicious Software

4.2.1. ECU will provide guidance and awareness education to workforce members on following procedures for guarding against, detecting, and reporting on malicious software.

4.2.2. Guidance and awareness education topics should cover items such as: how to identify and handle potential scams and hoaxes, explanation of how university anti-virus and malware protection software operates, how to use anti-virus and malware protection software, good security practices for web browsing, file sharing and opening email attachments, risks of installing unsupported software, security updates for workstations and software applications, and what to do when anti-virus and malware protection software detects an infection or intrusion.

4.3. Log-in Monitoring

4.3.1. ITCS, in collaboration with the HIPAA Security Office, will train workforce members on following procedures for monitoring log-in attempts and reporting discrepancies.

4.3.2. Training and awareness must cover the following topics at a minimum: how to effectively use ECU’s secure log-in processes, how to detect log-in discrepancies, and how to report log-in discrepancies.

4.4. Password Management

4.4.1. ECU must train workforce members on following procedures for creating, changing, and safeguarding passwords.
4.4.2. Training and awareness must cover the following topics at a minimum: ECU’s passphrase (password) requirements, good password practices, and ensuring that ECU Health Care Component workforce members understand that all activities involving their user identification and password will be attributed to them.