HIPAA Security Management Process

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 reasonable and appropriate administrative safeguards that establish the foundation for the University’s security program in regard to ePHI. 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 Management Process (164.308(a)(1)) – defines the administrative processes and procedures that ECU will use to implement a security program for all health care components of the University. This standard is comprised of four (4) regulatory specifications: Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review.

3.1.1. Risk Analysis (required) – covered entities must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by ECU.

3.1.2. Risk Management (required) – implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

3.1.3. Sanction Policy (required) – appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with security policies and procedures.

3.1.4. Information System Activity Review (required) – implement procedures to regularly review records of HIPAA system activity, such as audit logs, access reports, and security incident tracking reports. The information system activity review enables ECU to determine if any ePHI is used or disclosed in an inappropriate manner.

4. Procedure

4.1. Risk Analysis

4.1.1. Health Care Components must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its HIPAA systems.

4.1.2. The identification, definition and prioritization of risks to HIPAA systems must be based on a formal, documented risk analysis process. At a minimum, Health Care Components’ risk analysis process must include the following:
4.1.2.1. Identification and prioritization of the threats to HIPAA systems.

4.1.2.2. Identification and prioritization of the vulnerabilities of HIPAA systems.

4.1.2.3. Identification and definition of security measures used to protect the confidentiality, integrity, and availability of HIPAA systems.

4.1.2.4. Identification of the likelihood that a given threat will exploit a specific vulnerability on a HIPAA system.

4.1.2.5. Identification of the potential impacts to the confidentiality, integrity, and availability of HIPAA systems if a given threat exploits a specific vulnerability.

4.1.3. Health Care Components must conduct risk analysis on a regular basis. Such risk analysis must be used in conjunction with ECU’s risk management process to identify, select, and implement security measures to protect the confidentiality, integrity, and availability of HIPAA systems.

4.1.4. Judgements used in Health Care Components’ risk analysis, such as assumptions, defaults, and uncertainties should be explicitly stated and documented.

4.1.5. In addition to regular risk analysis, Health Care Components must conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity, or availability of specific HIPAA systems.

4.1.6. Each Health Care Components’ risk analysis process must be based on the following steps: inventory, threat identification, vulnerability identification, security control analysis, risk likelihood determination, impact analysis, and risk determination. The process shall be formally documented and securely maintained.

4.2. Risk Management

4.2.1. Security measures must be implemented to reduce the risks to HIPAA systems. Selection and implementation of such security measures must be based on a formal, documented risk management process. At a minimum, the risk management process must include the following:
4.2.1.1. Assessment and prioritization of risks to HIPAA systems.

4.2.1.2. Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage, mitigate, or accept identified risks.

4.2.1.3. Workforce member training and awareness on implemented security measures.

4.2.1.4. Regular evaluation and revision, as necessary, of existing security measures.

4.2.2. Health Care Components must manage risk on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity, and availability of HIPAA systems. Strategies for managing risk should be commensurate with the risk prioritization as described below to such systems, using one or more of the following methods to manage risk: risk acceptance, risk avoidance, risk limitation, or risk transference.

4.2.3. Health Care Components’ risk management process must be based on the following steps: inventory, risk prioritization, method selection, security method selection, assignment of responsibility, security method implementation, and security method evaluation. The process shall be formally documented and securely maintained.

4.3. Sanction Policy

4.3.1. ECU must have a formal, documented process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.

4.3.2. The identification and definition of such sanctions are defined in the applicable ECU policies to include but are not limited to: ECU Academic Computer Use Policy, University Student and Employee Computer Use Regulation, and the HIPAA Sanctions Regulation.
4.3.3. Sanctions can include but are not limited to: suspension, required retraining, written warning, and/or dismissal. Please reference the University’s HIPAA Sanctions Regulation located on the ECU Privacy Policies webpage.

4.4. Information System Activity Review

4.4.1. Health Care Components must regularly review records of activity on HIPAA systems. Records of activity may include but are not limited to: audit logs, access reports, and security incident tracking reports.

4.4.2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on HIPAA systems. At a minimum, such mechanisms must provide the following information if feasible: date and time of activity, origin of activity, identification of user performing activity, and description of attempted or completed activity.

4.4.3. Such reviews must be via a formal documented process. At a minimum, the process must include the following: 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.

4.4.4. Health Care Components must maintain the documentation of the review of such systems for a minimum of six (6) years.

4.4.5. Whenever possible, workforce members should not monitor or review activity related to their own user account.