HIPAA Transmission Security

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 appropriately protect the confidentiality, integrity, and availability of all ePHI that it transmits over electronic communications networks. 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. **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.

3. **Regulations**

3.1. **Transmission Security (164.312(e)(1))** – implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. This standard is comprised of two (2) regulatory specifications: Integrity Controls and Encryption.

3.1.1. **Integrity Controls (addressable)** – implement security measures to ensure that electronically transmitted PHI is not improperly modified without detection until disposed of.

3.1.2. **Encryption (addressable)** – implement a mechanism to encrypt ePHI whenever deemed appropriate.

4. **Procedure**

4.1. **Integrity Controls**

4.1.1. Health Care Components must use integrity controls that are appropriate for protecting the confidentiality, integrity, and availability of ePHI transmitted over electronic communications networks. The appropriateness of controls must be based upon sensitivity of and risks to ePHI. For example, ePHI transmitted over public networks represent a much higher risk than ePHI transmitted over ECU’s campus network. Integrity controls may include, but not limited to: encryption, checksums, point-to-point communications such as Virtual Private Networks (VPN), and switched networks.

4.2. **Encryption**
4.2.1. Health Care Components must consider the following factors, at a minimum, in
determining whether or not encryption must be used when sending specific ePHI over an
electronic communications network: the sensitivity of the ePHI, risks to the ePHI,
expected impact to ECU functionality and work flow if the ePHI is encrypted, and
alternative methods available to protect the confidentiality, integrity, and availability of the
ePHI.