HIPAA Contingency Planning

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 effectively prepare for and respond to emergencies or disasters in order to protect the confidentiality, integrity and availability of its 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.

3. **Regulations**

3.1. **Contingency Planning (164.308(a)(7))** – ECU’s disaster and emergency response process must reduce the disruption to ECU HIPAA systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes must identify and reduce risks to its HIPAA systems, limit damage caused by disasters and emergencies, and ensure the timely resumption of significant HIPAA systems and processes. These controls and processes must commensurate with the value of the HIPAA systems being protected or recovered. This standard is comprised of five (5) specifications: Data Backup Plan, Disaster Recovery Plan, Emergency Mode Operation Plan, Testing and Revision Procedures, and Applications and Data Criticality Analysis.

3.1.1. **Data Backup Plan (required)** – establish and implement procedures to create and maintain exact retrievable copies of ePHI.

3.1.2. **Disaster Recovery Plan (required)** – establish and implement as needed, procedures to restore any loss of ePHI.

3.1.3. **Emergency Mode Operation Plan (required)** – establish and implement as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

3.1.4. **Testing and Revision Procedures (addressable)** – implement procedures for periodic testing and revision of contingency plans.
3.1.5. **Applications and Data Criticality Analysis (addressable)** - assess the relative criticality of specific applications and data support of other contingency plan components.

4. **Procedure**

4.1. **Data Backup Plan**

4.1.1. It is the responsibility of the HIPAA System Administrator to have formal, documented procedures for creating and maintaining retrievable exact copies of ePHI. At a minimum, these procedures must: identify the HIPAA system(s) to be backed up, provide a backup schedule, identify storage of back up media, parties that may access data, outline the restoration process, and identify who is responsible for ensuring backup of the ePHI.

4.1.2. The criticality of the data will determine the frequency of data backups, retention of data backups, as well as where data backups and restoration procedures will be stored.

4.1.3. Backup copies of ePHI will be stored in a secure location and must be accessible to authorized workforce members for prompt retrieval of the information. The secure location must be geographically distant from the location of the HIPAA system as much as possible.

4.1.4. Restoration procedures for ePHI must be regularly tested as specified in the Testing and Revision Procedures (4.4) section of this policy to ensure that they are effective, and that they can be completed within the time allotted in the Health Care Component’s disaster recovery plan.

4.2. **Disaster Recovery Plan**

4.2.1. It is the responsibility of the HIPAA System Administrator to create and document a Disaster Recovery Plan to recover any ePHI and/or HIPAA system that is impacted by a disaster. The plan must be reviewed and revised on an annual basis or more frequently as needed.
4.2.2. The Disaster Recovery Plan must include at a minimum: identification and definition of workforce member responsibilities, conditions for activating the plan, location of data backups, and restoration procedures.

4.2.3. It is the responsibility of the HIPAA System Administrator to provide workforce members with disaster recovery responsibilities annual training on the disaster recovery plan.

4.2.4. All appropriate workforce members must have access to a current copy of the Disaster Recovery Plan, for the applicable HIPAA system.

4.3. Emergency Mode Operation Plan

4.3.1. It is the responsibility of the HIPAA System Administrator to have a formal, documented Emergency Mode Operation Plan for protecting its HIPAA systems during and immediately after a crisis situation. At a minimum, the plan must: identify and prioritize emergencies that may impact HIPAA systems, define procedures for how the health care component will respond to specific emergencies that impact its HIPAA systems, define procedures for how the health care component (during and immediately after a crisis situation) will maintain the processes and controls that ensure the confidentiality, integrity, and availability of ePHI, and define a procedure that ensures that authorized employees can enter ECU facilities to enable continuation of processes and controls that protect ePHI while ECU is operating in emergency mode.

4.3.2. It is the responsibility of the HIPAA System Administrator to provide workforce members annual training and awareness of the emergency mode operation plan.

4.3.3. All appropriate workforce members must have access to the current copy of the plan.

4.3.4. An appropriate number of current copies of the plan must be kept off-site.

4.4. Testing and Revision Procedures

4.4.1. It is the responsibility of the HIPAA System Administrator to conduct regular testing of its Disaster Recovery and Emergency Mode Operation Plans to ensure they are current
and operative. The criticality of the data and resource availability will determine the frequency of testing. At a minimum, the testing should be conducted on an annual basis.

4.4.2. The results of such tests must be formally documented. The Disaster Recovery and Emergency Mode Operation Plans must be revised as necessary to address issues or gaps identified in the testing process.

4.5. Applications and Data Criticality Analysis

4.5.1. It is the responsibility of the HIPAA System Administrator to have a formal, documented process for defining and identifying the criticality of its HIPAA systems and the data contained within them. At a minimum, the process must include: creating an inventory of interdependent systems and their dependencies, documenting the criticality of HIPAA systems (e.g. impact on patient care), identifying and documenting the impact to health care component services if specific HIPAA systems are unavailable for different periods of time, identifying the maximum time periods that HIPAA systems can be unavailable, and prioritizing HIPAA system components according to their criticality to the Health Care Component’s ability to function at normal levels.

4.5.2. The criticality analysis must be conducted at least annually. The criticality analysis report must be securely maintained.