HIPAA Device and Media Controls

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 policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facilities, and the movement of these items within its facilities. 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. **Electronic media** – any form of electronic storage device, to include but not limited to: computers (desktops, laptops, mobile devices), floppy disks, backup tapes, CD/DVD’s, zip drives, portable hard drives, and flash memory devices.

3. Regulations

3.1. **Device and Media Controls (164.310(d)(1))** – Health Care Components must ensure ePHI located on HIPAA systems and their associated electronic media must be protected against damage, theft, and unauthorized access. ePHI must be consistently protected and managed through its entire life cycle, from origination to destruction. Health Care Components must regularly conduct a formal, documented process that ensures consistent control of all HIPAA systems and their associated electronic media containing ePHI that is created, received, transmitted, maintained, or destroyed. The destruction of any ePHI should be governed by the university’s Data Retention Policy or the applicable Health Care Components’ Data Retention Policy. Questions concerning the destruction of ePHI should be directed to the ITCS Helpdesk. This standard is comprised of four (4) regulatory specifications: Disposal, Media Re-Use, Accountability, and Data Backup and Storage.

3.1.1. **Disposal (required)** – implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
3.1.2. **Media Re-Use (required)** – implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

3.1.3. **Accountability (addressable)** – maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3.1.4. **Data Backup and Storage (addressable)** – create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

4. **Procedure**

4.1. **Disposal**

4.1.1. All HIPAA systems and/or associated electronic media containing ePHI must be disposed of properly when no longer needed for legitimate use. The destruction of any ePHI should be governed by the university’s Data Retention Policy or the applicable Health Care Component’s Data Retention Policy. Questions concerning the destruction of ePHI should be directed to the ITCS Helpdesk.

4.1.2. To dispose of a HIPAA system or electronic media containing ePHI, the data must be completely removed with data sanitization tool (s) that erase or overwrite media in a manner that prevents the data from being recovered. “Deleting” typically does not destroy data and may enable unauthorized persons to recover ePHI from the media.

4.1.3. An alternative to data sanitization of electronic media is physical destruction. The physical destruction of electronic media may be feasible where the media is inexpensive and the destruction methods are easy and safe. For example, CD’s and DVD’s are relatively inexpensive and can be easily destroyed with a pair of scissors, if handled carefully or shredded.

4.2. **Media Re-Use**

4.2.1. All ePHI on HIPAA systems and/or associated electronic media must be removed before the systems and/or media can be re-used.
4.2.2. ePHI must be removed from HIPAA systems and/or associated electronic media using data sanitation tool(s) which erase or overwrite media, in accordance with Materials Management’s Guidelines for Surplus and Disposal, in a manner that prevents the data from being recovered. “Deleting” typically does not destroy data and may enable unauthorized persons to recover ePHI from the system hardware or media.

4.3. Accountability

4.3.1. HIPAA System Administrators must maintain an inventory of all HIPAA systems and/or associated electronic media. The inventory must also identify the persons responsible for the devices containing ePHI.

4.3.2. Health Care Components must maintain a record of the movement of HIPAA systems and/or associated electronic media as it moves into and out of the facility.

4.3.3. Before HIPAA systems and/or associated electronic media are moved / stored to a location outside of ECU’s premises (ECU owned, leased, or controlled), the move must be approved by the Health Care Component, notification of the move given to the HIPAA Security Office, and the move must be tracked and documented.

4.3.4. Workforce members who move HIPAA systems and/or associated electronic media are responsible for the subsequent use of such items and must take all appropriate and reasonable actions to protect them against damage, theft, and/or unauthorized access.

4.4. Data Backup and Storage

4.4.1. Backup copies of all ePHI on HIPAA systems and/or associated electronic media must be made regularly and stored in a secure location.

4.4.2. HIPAA System Administrators, and when applicable ITCS, must regularly test backup and restoration procedures for HIPAA systems and/or associated electronic media to ensure that they are effective and can be completed within a reasonable amount of time.
4.4.3. Health Care Component’s backup media containing ePHI at a remote backup storage site must be given an appropriate level of physical and environmental protection consistent with the standards applied to the protection of ePHI at ECU.

4.4.4. The retention period for backup of ePHI on HIPAA systems and/or associated electronic media must be defined and documented.