HIPAA Workstation Use and 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 implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. Physical safeguards for all workstations that access ePHI and strategies to restrict access to HIPAA systems, only authorized users, must also be implemented. 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 covered 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. **Workstation** – an electronic computing device, for example, laptop, desktop computer, tablet, or any other device that performs similar functions, and electronic media stored in its immediate environment. These devices are part of a HIPAA System and thus have access to or store ePHI.

2.7. **Active Directory** - a Windows OS centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

3. **Regulations**

3.1. **Workstation Use (164.310(b))** – Health Care Components are required to specify the proper functions to be performed by workstations used with HIPAA systems. Inappropriate use of workstations can expose a covered entity to risks, such as virus attacks, compromise of HIPAA systems, and breaches of confidentiality. The proper environment for workstations is also covered in this standard. This standard does not have any regulatory specifications, but like all standards must be implemented.

3.2. **Workstation Security (164.310(c))** – Health Care Components will prevent unauthorized access to workstations that store or access ePHI while maintaining the access of authorized employees. Workforce members must not use a health care component workstation to engage in any activity that is either illegal under local, state, federal, or international law, or is in violation of ECU policy. Access to health care component workstations with ePHI must be
controlled and authenticated. This standard does not have any regulatory specifications, but like all standards must be implemented.

4. Procedure

4.1. Workstation Use

4.1.1. Workforce members should be familiar with and follow the guidelines described in ECU’s University Student and Employee Computer Use Regulation and Academic Computer Use Policy.

4.1.2. Workforce members that are granted access to a workstation need to understand how best to use the workstation to maximize the security of its data.

4.1.3. Documentation on applications must be very specific to the function being performed and this documentation must be provided to the health care component.

4.1.4. Each workforce member must log off the applications and/or workstation when leaving the workstation for an extended amount of time.

4.1.5. Workstations residing in Active Directory will be password protected and when left unattended, the automatic workstation lock feature will be activated.

4.1.6. Workstations should be located in secure areas that can be locked when unattended.

4.1.7. If workstations are located in a public area, they should be positioned so as to protect the monitor from being seen by unauthorized person(s) and the automatic workstation lock feature must be activated. If applicable, screen shields can be used to prevent unauthorized viewing of ePHI.

4.2. Workstation Security

4.2.1. Health Care Components must prevent unauthorized physical access to workstations that can access ePHI and ensure that authorized workforce members have appropriate access.

4.2.2. All workforce members who use health care component workstations must take all reasonable precautions to protect the confidentiality, integrity, and availability of ePHI contained on, or accessed by, the workstations. For example, positioning monitors or
shielding workstations so that data shown on the screen is not visible to unauthorized persons.

4.2.3. Unauthorized workforce members must not willfully attempt to gain physical access to workstations that store or access ePHI.

4.2.4. Workforce members must report loss or theft of any access device (such as one card or token) that allows them physical access to areas having workstations that can access ePHI.

4.2.5. Access to all health care component workstations must be authenticated via a process that includes, at a minimum: unique user ID’s that enable users to be identified and tracked, passwords must be masked, suppressed, or otherwise obscured so that unauthorized persons are not able to observe them, initial password(s) issued to a new workforce member must be valid only for the new user’s first logon to the workstation or application and at initial logon the user must be required to change his/her password, and upon termination of a workforce member employment or contracted services, workstation access privileges will be removed.

4.2.6. Workforce members must log out of any application or device that accesses or contains ePHI prior to leaving the application or device unattended.

4.2.7. Workforce members must not share their user accounts or passwords with others. If a workforce member believes that someone else is inappropriately using a user account or password, they must immediately notify their manager.