H.2.C

HIPAA Security Regulations

Title: Workstation Security Policy

Security Rule: 164.310(c)

Purpose: To ensure that all workstations (e.g., desktop systems) used to access, transmit, receive or store ePHI are appropriately secured.

Requirements:

1. All system administrator or root accounts must be password protected.
2. A User Identification and Password authentication mechanism must be implemented to control user access to the system.
3. All relevant security patches and updates must be applied.
4. A virus detection system must be implemented, including a procedure to ensure that the virus detection software is maintained and up-to-date.
5. A host-based firewall that denies all unsolicited inbound requests from unauthorized systems should be implemented on each workstation within the covered component.
6. Laptops storing any ePHI and desktop workstations storing significant volumes of ePHI (more than 500 records) must utilize an Emory approved whole disk encryption solution to protect the ePHI stored on the device.
7. All unused or unnecessary services must be disabled.
8. In addition to the above measures, workstations that are located in open, common, or otherwise insecure areas must also implement the following:
   a. An inactivity timeout or automatic logoff mechanism. The inactivity timeout period may not exceed 30 minutes.
   b. The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.
   c. If any of the measures outlined in this Paragraph 6 are not feasible for certain workstations, e.g. thin clients, all measures that are relevant to that workstation must be implemented.

This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness.
Non-compliance with this policy may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

See: HIPAA Security Regulations: Sanction Policy

Recommended By: Emory HIPAA Security Working Group

Effective Date: April 20, 2005

Authorized By: Emory HIPAA Security Steering Committee

Date of Last Edit: April 21, 2011

Review Date: April 21, 2011