H.3.A.iii

HIPAA Security Regulations

Title: Logoff/Device Lock Policy

Security Rule: 164.312(a)(1)

Purpose: To ensure that access to all servers and workstations that access, transmit, receive, or store ePHI is appropriately controlled.

Requirements:

1. When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the system’s Automatic Logoff Mechanism (e.g., CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.

2. Servers, workstations, or other computer systems containing ePHI repositories must employ an inactivity timeout or automatic logoff mechanism (e.g., password protected screen savers that black out screen activity). The inactivity timeout period may not exceed 30 minutes.

3. Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas that access, transmit, receive, or store ePHI must employ an inactivity timeout or automatic logoff mechanism. The inactivity timeout period may not exceed 30 minutes.

4. Applications and databases using ePHI, such as Electronic Medical Records (EMR), must employ an inactivity timeout or automatic session logoff mechanism. The inactivity timeout period may not exceed 30 minutes.

5. If a system requires the use of an inactivity timer or automatic logoff mechanism as detailed above, but does not support such mechanisms, at least one of the following procedures must be implemented:
   a. The system must be moved into a locked or secure physical environment.
   b. All ePHI must be removed and relocated to a system that supports the minimum HIPAA Security Automatic Logoff procedures.
   c. The system must be upgraded or moved to support the minimum HIPAA Security Automatic Logoff procedures.

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: January 14, 2009

Review Date: April 21, 2011