H.2.A

HIPAA Security Regulations

Title: Facility Access Control Policy

Security Rule: 164.310(a) (1)

Purpose: To ensure that access to facilities used to house systems or media containing ePHI is appropriately controlled.

Requirements:

1. ePHI system owners must establish and maintain a Facility Security Plan that outlines and documents the procedures necessary to safeguard all facilities, systems, and equipment that contain ePHI against unauthorized physical access, tampering, or theft. The Facility Security Plan must include the following components:
   
   a. Access Control and Validation – procedures to control and validate a workforce member’s access to facilities based on their role or function, including the methods for controlling and validating employees’ and visitors’ access to facilities.
   
   b. Physical Access Records – procedures to log physical access to any facility containing medium and high risk ePHI-based systems. Examples of facilities requiring physical access records are computer and system rooms, data centers, etc.
   
   c. Physical Access Controls – procedures to ensure that only authorized individuals have access to facilities and equipment that contain ePHI, and to prevent tampering and theft of ePHI related equipment.
   
   d. Contingency Operations – procedures that allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan.
   
   e. Maintenance Records – procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.
   
   f. Environmental Controls – Procedures and safeguards to ensure that temperature and humidity are properly controlled, and that appropriate fire suppression systems are in place and properly maintained.

2. Procedures must be established and implemented to control, validate, and document visitor access to any facility used to house ePHI based systems.
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:** August 20, 2015

**Review Date:** August 20, 2015