H.1.E.iii

HIPAA Security Regulations

Title: Log in Monitoring

Security Rule: 164.308(a)(5)

Purpose: To ensure that access to servers, workstations, and other computer systems containing electronic PHI is appropriately monitored and secured and that questionable data access activities are investigated promptly.

Requirements:

1. All ePHI system owners will develop, implement, and periodically review a documented process for monitoring login attempts and reporting login discrepancies. Each system owner must implement a mechanism to log and document all login attempts on each system containing ePHI. Logs must contain IP address or system name, user account, date, and time. Examples of events to monitor include:
   a. Successful/unsuccessful login and logout of users; denial of service events.
   b. Use of all privileged accounts and utilities.
   c. Changes to user accounts or privileges (creation, modification, deletion).
   d. Automatic logout of a user after exceeding a locally defined time of inactivity or excessive login attempts.
   e. Switching to another user's access or privileges after logging in.
   f. All access to security files, attributes, or parameters; any action to circumvent security controls including access to anti-virus software.

2. Each system owner must review such login activity reports and logs on a periodic basis. The period between reviews must not exceed 7 days.

3. All failed login attempts of a suspicious nature, such as continuous attempts, must be reported immediately to their covered component's HIPAA Security designee or IT Director.

4. Each business unit (i.e., “covered component”) must disseminate and document security reminders to its workforce to make them aware of the preceding log-in monitoring requirements.

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