H.1.D

HIPAA Security Regulations

Title: Information Access Management Policy

Security Rule: 164.308(a) (4)

Purpose: To ensure that access to ePHI is authorized and managed in a manner commensurate with the role of each workforce member and that access to ePHI is consistent with the HIPAA Privacy and Security Rules,

Requirements: In order to implement the purpose of this policy, the following procedures must be observed:

1. Each ePHI system owner must implement procedures to establish, document, review, and modify each workforce member’s authorization to access ePHI. These procedures must comply with the following:
   a. It is the responsibility of supervisors/and or managers to ensure that a background check has been successfully completed before authorizing users to access systems containing ePHI for each of their subordinates.
   b. It is the responsibility of supervisors/and or managers to ensure that a statement of adherence to security policies and procedures has been signed and is being kept on file before authorizing users to access systems and networks containing ePHI for each of their subordinates.
   c. It is the responsibility of supervisors and/or managers to authorize access to systems and networks containing ePHI for each of their subordinates. Workforce members are not permitted to authorize their own access to ePHI or be granted authorization by another workforce member’s supervisor.
   d. It is the responsibility of each supervisor or manager to ensure that the access granted for each of their subordinates to ePHI meets the minimum requirements for their roles, but does not exceed the level of authorization necessary to perform legitimate job functions.
   e. It is the responsibility of supervisors and/or managers to regularly review the scope of access granted to ePHI for each of their subordinates, adjusting their access rights as their roles change.
   f. It is the responsibility of supervisors/and or managers to ensure that only unique non-generic userids are authorized to access to systems and networks containing ePHI for each of their subordinates.

2. If a workforce member’s employment is terminated or if a workforce member leaves the Covered Component:
a. The workforce member's supervisor or manager must ensure that the workforce member's authorization to access ePHI is terminated within 2 business days.

b. The workforce member's supervisor or manager must ensure that access to all facilities housing ePHI also has been terminated. This includes, but is not limited to, card access, keys, codes, and other facility access control mechanisms. Codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.

c. Human Resources should be notified and the termination of authorization should be processed in a timely and appropriate manner.

3. If a workforce member transfers to another department or workgroup:
   a. The workforce member's existing/former supervisor or manager must ensure that all authorization to access accounts containing ePHI is terminated.
   b. The workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the workforce member's new role.

4. Under no circumstances will access to ePHI be extended to workforce members beyond the final date of their employment unless an approved Business Associates Agreement is executed and on file in the appropriate departmental office.

5. Each ePHI system owner must periodically perform account reviews and cleanups of active user accounts to ensure that only those users whose access levels are appropriate are active within their system(s). The time interval between reviews may not exceed 90 days.

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