H.3.D

HIPAA Security Regulations

Title: Person or Entity Authentication

Security Rule: 164.312(d)

Purpose: All entities must authenticate all persons or entities seeking access to ePHI systems before access is granted.

Requirements:

1) All owners of system with ePHI must create and implement a formal, documented process for verifying the identity of a person or entity before granting them access. The process must be regularly reviewed and revised as necessary.

2) At a minimum, authentication processes must include the following:

   a) Formal documented procedure(s) for granting a person or entity an authentication method (e.g. password, biometrics, or token) as well as changing an existing authentication method.

   b) All authentication identifiers used for access to ePHI system must be uniquely identifiable so activities using the identifier can be traced to an individual person or entity (see Audit Control policy).

   c) Formal documented procedure for detecting and responding to unusual or suspicious authentication activity (see Login Monitoring policy).

3) Appropriate and reasonable system(s) must be used to ensure that only properly authenticated persons and entities access its ePHI. Such systems can include but are not limited to:

   a) Biometric identification systems

   b) Password systems

   c) Telephone callback systems

   d) Security token systems

4) When applicable, such authentication system(s) must include, at a minimum:

   a) Unique user identifiers (user IDs) that enable persons and entities to be uniquely identified. User IDs must not give any indication of the user’s privilege level.

   b) A secret identifier (password or PIN)

   c) The removal or disabling of authentication methods for persons and entities that no longer need access to an ePHI system within 2 business days.
d) Verification that redundant or duplicate user identifiers are not issued.

5) All authentication data, such as passwords and PINs, must be encrypted and protected with appropriate access controls to prevent unauthorized access.

6) All password and PIN based authentication systems must mask, suppress, or otherwise obscure the passwords and PINs so that unauthorized persons are not able to observe them.

7) Methods (e.g. password or PIN) for authentication to ePHI systems must not be built into logon scripts.

8) Workforce members must not share or reveal their authentication methods to others. Workforce members are accountable for all actions another party performs with a shared authentication method (e.g. password, pin, token). Any workforce member who believes that their authentication method is being inappropriately used must immediately notify his or her manager.

9) Workforce members must immediately report the loss or theft of an access method (e.g. key card or security token) to appropriate management.

10) Authentication attempts to all ePHI systems must be limited to no more than 5 attempts within 30 minutes.

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