H.1.E.iv

HIPAA Security Regulations

Title: HIPAA Security Password Management Policy

Security Rule: 164.308(a)(5)

Purpose: To ensure that passwords created and used by the Emory University workforce to access any network, system, or application used to access, transmit, receive, or store ePHI are properly safeguarded and that Emory’s workforce is kept apprised of all password related policies.

Requirements:

1. Access to networks, systems, or applications used to transmit, receive, or store ePHI must be accomplished through the use of a Unique User Identification and password in order to access the ePHI.

2. Any password used to gain access to any network, system, or application used to access, transmit, receive, or store ePHI must be of sufficient complexity to ensure that it is not easily guessable.

3. Managers of networks, systems, or applications used to access, transmit, receive, or store ePHI must ensure that passwords set by workforce members meet the following minimum requirements if technically feasible:
   a. Passwords must be between 8 and 30 characters in length
   b. Passwords must contain at least 1 uppercase and 1 lowercase character along with at least 1 number or special character.
   c. Passwords must be changed periodically. The interval between password changes must not exceed 365 days.
   d. New passwords must be chosen at each password change. Reusing previous passwords is prohibited. Systems capable of enforcing this requirement via “password history” settings should use a password history of 30 or greater.

4. Managers of networks, systems, or applications used to access, transmit, receive, or store ePHI are responsible for making workforce members aware of all password related policies and procedures, and any changes to those policies and procedures.

5. Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
a. Passwords are only to be used for legitimate access to networks, systems, or applications.

b. Passwords must not be disclosed to other workforce members or other individuals.

c. Workforce members must not allow other workforce members or other individuals to use their password.

d. Passwords must be committed to memory and not be written down, posted, or exposed in an insecure manner (e.g., written on a notepad that may be read by others, posted on the workstation, stored in an unencrypted computer file, etc.).

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