H.3.A.i

HIPAA Security Regulations

Title: Unique User Identification Policy

Security Rule: 164.312(a)(1)

Purpose: To ensure the ability to identify, track and monitor individual users that access networks, systems, and applications that contain EPHI.

Requirements:

1. Users who must access any network, system, or application that may access, transmit, receive, or store EPHI must be provided with a unique User Identifier.

2. When logging into any network, system, or application that accesses, transmits, receives, or stores EPHI, users must supply his/her previously assigned unique User Identification in conjunction with a secure password in order to gain access to such networks, systems, or applications.

3. Users must not allow any other individual to use their unique User Identification or Password.

4. Users are responsible for insuring that their User Identification and password are not documented, written, or otherwise exposed in an insecure manner.

5. Users are responsible for insuring that their assigned User Identification is appropriately protected and used only for authorized access to networks, systems, or applications. If a user believes their User Identification has been compromised, he/she is required to report such security incident to the appropriate Security Officer immediately upon learning of the incident.

See: HIPAA Security Regulations: Incident Response and Reporting Policy

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