H.3.A.iv

HIPAA Security Regulations

Title: ePHI Data Encryption and Decryption Policy

Security Rule: 164.312(a) (1)

Purpose: To ensure that access to all servers, workstations, and other systems that access, transmit, receive, or store ePHI is appropriately secure and controlled.

Requirements:

1. The ePHI system owner must institute the following access control policies to ensure that access to ePHI and its associated applications, systems, and networks are appropriately secured and controlled:
   See: HIPAA Security Regulations: Unique User Identification Policy
   HIPAA Security Regulations: Logoff/Device Lock Policy

2. Whether encryption of stored ePHI is required as an access control mechanism must be determined by the custodian of the data based upon a risk assessment.

3. Encryption of ePHI may be required in some instances as a transmission control and integrity mechanism.

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