H.3.C.i

HIPAA Security Regulations

Title: ePHI Integrity and Authentication Policy

Security Rule: 164.312(c)(1)

Purpose: To ensure that appropriate data authentication measures are implemented, based upon the applicable risk assessment, in order to protect the integrity of ePHI by preventing its unauthorized or improper alteration or destruction.

Requirements:

1) Each ePHI system owner must implement a mechanism to corroborate that ePHI is not altered or destroyed in an unauthorized or improper manner.

2) Anti-virus software is the minimum data integrity mechanism required on all ePHI systems.

3) Data Storage - Mechanisms such as error-correcting memory and storage may be utilized to authenticate data storage and retrieval.

4) Data Transmission - For data integrity during transmission, See HIPAA Security Regulations: Transmission Security Policy

5) Data at Rest – When available on ePHI systems, data checksums, cryptographic hashes (e.g. MD5, SHA1), or digital signatures should be used to ensure the integrity of data at rest.

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