HIPAA Security Regulations

Title: HIPAA Security Data Backup Policy

Security Rule: 164.308(a)(7)

Purpose: To ensure the availability of all ePHI in accordance with its designated level of criticality.

Requirements:

1. Each ePHI system owner must establish and implement a data backup procedure to create and maintain retrievable, exact copies of all ePHI.

2. Data backup procedures must be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved and made available. Testing of backup procedures must be conducted at least annually, and immediately after any modification to backup procedures that may affect the integrity of the backups.

3. All media used for backing up ePHI must be transported in a secure manner and stored in a secure location with a properly controlled environment.

4. If using a 3rd party vendor for off-site storage or backup service, an approved written contract (i.e., Business Associate Agreement) must be entered into in order to ensure that the vendor will safeguard the ePHI in accordance with all applicable HIPAA Security and HIPAA Privacy rules and the provisions of this policy. This contract must be approved by the Office of the General Counsel.

5. Removable backup media containing ePHI must be encrypted. Encryption algorithms must be compliant with FIPS 140-2 and must utilize randomly generated keys of 128 bits or longer for symmetric algorithms (e.g. AES) or 2048 bits or longer for asymmetric algorithms (e.g. RSA).

The provisions of this policy apply to, but are not necessarily limited to, backups for all files, records, images, voice or video files that may contain ePHI.

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