H.2.D

HIPAA Security Regulations:

Title: Device and Media Control Policy

Security Rule: 164.310(d)(1)

Purpose: To ensure that ePHI stored or transported on storage devices and removable media is appropriately controlled and managed. These can include hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards and memory sticks.

Requirements:

1. If a removable media or storage device containing ePHI that may be needed in the future is to be destroyed or otherwise disposed of, a retrievable, exact copy of the ePHI must be made and secured prior to destruction or disposal of the media or storage device.

2. If equipment containing ePHI that may be needed in the future is to be moved, a retrievable, exact copy of the ePHI must be made and secured prior to moving the equipment.

3. If the media or storage device contains ePHI that is not further needed or required and does not contain a unique copy of the ePHI, a data destruction tool must be used to destroy the data on the device or media prior to disposal or reuse. A typical reformat is not sufficient as it does not overwrite the data.

4. Removable media and storage devices containing ePHI must not be made available for reuse. If the media or storage device contains ePHI that is required or may be needed in the future, a retrievable, exact copy of the ePHI must be made prior to reuse.

5. If the device or media contains ePHI that is not needed or required, and is not a unique copy, a data destruction tool must be used to destroy the data on the media or device prior to disposal. A typical reformat is not sufficient as it does not overwrite the data.

6. If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not required.

7. When using storage devices and removable media to transport ePHI, a procedure must be implemented to track and maintain records of the movement of those devices and media and the parties responsible for the device and media during its movement.
8. Removable media or storage devices containing ePHI must be encrypted in order to ensure the protection of the data in the event that media or device is lost or stolen.

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: April 21, 2011

Review Date: April 21, 2011