H.1.F.i

HIPAA Security Regulations

Title: HIPAA Security Incident Response and Reporting Policy

Security Rule: 164.308(a)(6)

Purpose: To ensure that all security incidents and violations involving ePHI are appropriately identified, reported, documented and mitigated, to the extent practicable, as to any harmful effects of the incident.

Requirements:

1. Each ePHI system owner is responsible for the creation and implementation of procedures to support the reporting, documentation and mitigation of security and privacy incidents.

2. All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI must be addressed through such defined procedure. The procedure must include, at a minimum, the following items:
   a. A procedure for reporting suspected incidents to the business entity’s Help Desk
   b. A mechanism for reporting potential disclosures of ePHI to information security, compliance, legal, risk management, and unit leadership.
   c. A process for performing a risk analysis, assigning a severity level to each incident, and taking the appropriate action
   d. ePHI system owners must work with the HIPAA Working Group to develop recommendations and implement countermeasures to prevent the breach from occurring again
   e. All correspondence with outside authorities such as local police, FBI, media, etc. must be coordinated with the Compliance Office and Chief Information Security Officer.
   f. All incidents, actions taken and outcomes must be documented by the ePHI system owner and submitted to the appropriate HIPAA working group member

3. Incidents that should be reported include, but are not limited to:
   a. Virus, worm, or other malicious code attacks
   b. Network or system intrusions
   c. Persistent intrusion attempts from a particular entity
   d. Unauthorized access to ePHI, ePHI based system, or ePHI based network
e. Loss of ePHI data due to failure, error, or disaster

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