H.1.E
HIPAA Security Regulations
Title: Security Awareness and Training Policy
Security Rule: 164.308(a) (5)

Purpose: To ensure that all Emory workforce members are appropriately made aware of and trained in compliance with all of Emory’s HIPAA Security Policies and Procedures.

Requirements: In order to implement the purpose of this policy, the following procedures must be observed:
1. The responsible individual for each covered component is responsible for ensuring that all users and workforce members (including managers) have received the appropriate level of HIPAA Security Awareness Training. The minimum level of HIPAA Security training must consist of, but is not limited to, the following requirements:

   - HIPAA Security Regulations Policies
   - HIPAA Regulations: Sanction Policy
   - Confidentiality, Integrity, and Availability (CIA)
   - Individual security responsibilities
   - Common security threats and vulnerabilities and security best practices.
   - Protection from malicious software
   - Security incident reporting
   - Password management practices
     - Creating good passwords
     - Changing passwords at proscribed intervals
     - Safeguarding passwords

2. The responsible individual for each covered component is responsible for ensuring that all Information Technology staff members and all workforce members who are responsible for the setup, installation, or management of computer systems and networks containing ePHI have the appropriate level of HIPAA Security training. HIPAA Security training for these workforce members must consist of, but is not limited to, the following requirements:

   - HIPAA Security Regulations Policies
   - HIPAA Security Regulations: Sanction Policy
   - Confidentiality, Integrity, and Availability (CIA)
   - Individual security responsibilities
   - Common security threats and vulnerabilities
   - Password Structure and Management procedures
   - Server, desktop computer, and mobile computer system security procedures
including, but not limited to:
  i. Security patch and update procedures
  ii. Virus and Malicious Code protection procedures
  iii. Device and Media Control procedures
  iv. Incident response and reporting procedures

3. The responsible individual for each covered component must also ensure that the appropriate IT staff are aware of and trained to comply with the following HIPAA Security plans and procedures:
   a. Login Monitoring procedures
   b. Audit Control and Review Plan
   c. Data Backup Plan
   d. Disaster Recovery Plan
   e. Information Access Management
   f. Information System Activity Review
   g. Password Structure
   h. Security Regulations Reminders

4. Each entity must maintain formal documentation of the current level of HIPAA training for each of its workforce members.

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