H.1.E.i

HIPAA Security Regulations

Title: Security Regulations Reminders Policy

Security Rule: 164.308(a)(5)

Purpose: To ensure that all Emory workforce members are made and kept appropriately aware of all changes or updates to HIPAA Security Regulations policies and procedures and current threats or vulnerabilities to EPHI.

Requirements: In order to implement the purpose of this policy, the following procedures must be observed:

1. The HIPAA Security Steering Committee or Compliance Office must notify each component of the Emory covered entity of any of the following events:
   a. A new HIPAA Security Regulations policy or procedure has been approved.
   b. A current HIPAA Security Regulations policy or procedure has been updated.

2. Each business unit (i.e., “covered component”) is responsible for ensuring that its workforce is made aware of all changes or updates to Emory’s HIPAA Security Regulations policies and procedures.

3. Each business unit must establish and implement a procedure to periodically disseminate information regarding threats, breaches or vulnerabilities that have been determined by the entity to be a threat to EPHI.

4. Each business unit must document the security reminders implemented. Documentation should include the type of reminder, the reminder content, the date it was implemented, and the audience to whom it was communicated.

See: HIPAA Security Regulations: Incident Response and Reporting Policy

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