H.1.H
HIPAA Security Regulations
Title: Evaluation
Security Rule: 164.308(a) (8)

Purpose: To ensure that each HIPAA Security Policy adopted by Emory and each Security Procedure developed and implemented by an Emory Business Unit is periodically evaluated for technical and non-technical viability.

Requirements:

1. Periodic Evaluation Generally
   a. Emory HIPAA Security Policies and Business Unit Security Procedures should initially be evaluated to determine their compliance with HIPAA Security Regulations. Once compliance with HIPAA Security Regulations is established, the Emory Security Policies and Business Unit Security Procedures should be evaluated on a periodic basis to ensure continued viability in light of technological, environmental or operational changes that could affect the security of ePHI.

2. Periodic Evaluation by HIPAA Security Officer
   a. The HIPAA Security Officer will review on an on-going basis the viability of Emory Security Policies and general approaches taken by Business Units in their Security Procedures.
   b. The HIPAA Security Officer will develop and recommend to the HIPAA Steering Committee any necessary Security Policy or Security Procedure changes.

3. Periodic Evaluation by WHSC HIPAA Steering Committee
   a. The HIPAA Steering Committee will reconvene on an annual basis to evaluate the technical and non-technical viability of EU Security Policies.
   b. Any member of the HIPAA Steering Committee, the Chief Information Security Officer, any Business Unit HIPAA Security liaison or any other person may suggest changes to the Security Policies or Procedures by submitting such suggestion to the HIPAA Steering Committee for consideration.
   c. If the Steering Committee recommends a new security standard or a change in Emory Security Policies or Procedures, such new standard or change will be communicated to the Business Units by the Security Liaisons, who will elicit feedback for a specific period of time and provide such feedback to the HIPAA Steering Committee.
d. If the HIPAA Steering Committee approves the change, such change will be propagated to the Business Units through policy updates and reminders. Each Business Unit will be required to update their Security Procedure in a timely manner to incorporate the change.

4. Evaluation Upon Occurrence of Certain Events
   a. In the event that one or more of the following events occur, the policy evaluation process described in Paragraph 2 will be immediately triggered:
      i. Changes in the HIPAA Security Regulations or Privacy Regulations
      ii. New federal, state, or local laws or regulations affecting the privacy or security of PHI
      iii. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures
      iv. A serious security violation, breach, or other security incident occurs

5. Evaluation of Business Unit Procedures by Business Units
   a. Each Business Unit must periodically (at least annually) evaluate its HIPAA Security Procedures to ensure that such Procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security Policies.

6. Internal Audit of Security Policies and Procedures
   a. All HIPAA Security Policies and Business Unit procedures are subject to periodic audits.

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: 3/19/2009
Authorized By: Emory HIPAA Security Steering Committee
Date of Last Edit: 3/19/2009
Review Date: 3/19/2009