H.1.C

HIPAA Security Regulations

Title: Workforce Security Policy

Security Rule: 164.308(a)(3)

Purpose: To ensure that all members of the workforce have been properly cleared to obtain access to EPHI and that the appropriate level of access to EPHI is granted.

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

1. Each covered entity within Emory must implement a procedure to determine that each of its workforce member’s scope of access to EPHI is appropriate to the scope of the workforce member’s duties and responsibilities. This determination must represent the minimum necessary access to EPHI that is required for the workforce member to do his/her job.
2. A background check must be performed by Human Resources (or an agent working on behalf of human Resources) on all workforce members requiring access to PHI. The background check must be completed and deemed satisfactory by Human Resources before access to PHI is granted.
3. Each entity must comply with the policies and procedures for authorizing, managing, and terminating access to EPHI for workforce members detailed in the University’s HIPAA Security Regulations: Information Access Management Policy.

All Emory workforce members are subject to the Emory University Code of Conduct http://emory.hr.emory.edu/policies.nsf/203cdb16bd651af85256be6004fd9ce/3e81 as it relates to the appropriate use of EPHI.

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