H.1.A.i/ii
HIPAA Security Regulations
Title: Risk Analysis and Mitigation Policy
Security Rule: 164.308(a)(1)

Purpose: To appropriately identify the potential vulnerabilities and mitigate the risks associated with storing ePHI, transmitting ePHI locally and outside of Emory, and transmitting ePHI to Emory components that are not part of the Emory Covered Entity. Each entity involved in the storage or transmission of ePHI must utilize the following risk analysis and mitigation strategy:

1. Identify and document all ePHI systems
2. Periodically re-inventory all systems, including those storing or transmitting ePHI
3. Identify the potential vulnerabilities of each system
4. Mitigate the risk to each system, including those storing or transmitting ePHI
5. For all identified systems, including those storing or transmitting ePHI, maintain all safeguards and mechanisms necessary to prevent accidental or deliberate exposure.

Requirements:
All systems and applications that store, process, or transmit ePHI must be identified.

1. An inventory must be performed by the ePHI system owner at least annually to ensure that the ePHI inventory is accurate and up-to-date.
2. Each identified system or application must be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of its ePHI.
3. Appropriate and reasonable security measures and safeguards must be implemented for each system or application. The level, complexity and cost of those security measures and safeguards should be commensurate with the risk to Emory. These security measures may consist of administrative, physical, and/or technical safeguards as defined in the HIPAA Security Regulations Policies and must be sufficient to meet or exceed all HIPAA Security Rule Standards and Implementation Specifications.
4. System criticality should be determined by each owner:
   a. High Criticality: the system contains large numbers of critical/confidential data accessed by large numbers of end-users. Additionally, systems should be considered highly critical if a period of downtime has an extremely high impact to the University, whether financially, to the reputation of or from a patient care perspective.
b. Medium Criticality: the system contains either large numbers of critical/confidential data accessed and a small number of end-users, or a small number of critical/confidential data and a large number of users. Systems should be considered at a medium level of criticality if a period of downtime has a moderate to high impact to the University, whether financially, to the reputation of or from a patient care perspective.

c. Low Criticality – Systems with a small number of critical/confidential data accessed by a small number of users. Systems should be considered less critical if a period of downtime has low to little impact to the University, whether financially, to the reputation of or from a patient care perspective.

5. The potential risks and vulnerability to the integrity, confidentiality, and availability of each ePHI repository must be reassessed at least annually. The security measures and safeguards implemented for each ePHI repository must also be reassessed in a manner commensurate with the identified changes in risk and vulnerability and updated if necessary. Any security measures or safeguards found to be insufficient to meet the requirements must be documented and tracked in a remediation plan.

6. The policies and procedures that are defined and implemented to meet the HIPAA Security Regulations will reflect the minimum level of security that must be maintained to ensure the integrity, confidentiality, and availability of ePHI. Additional security measures should be implemented if appropriate.

7. When it becomes technically feasible, all ePHI systems must be moved into a network zone that is compliant with Emory’s HIPAA policies and standards.

This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their 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