H.1.A.iv

HIPAA Security Regulations

Title: Information System Activity Review Policy

Security Rule: 164.308(a)(1)

Purpose: To ensure that system activity for all systems which have been classified as “Medium Criticality” or “High Criticality” (See HIPAA Security Regulations: Risk Analysis and Mitigation Policy) is appropriately monitored and reviewed.

Requirements:

1. Each ePHI system owner must establish, document, and implement an internal audit procedure in order to regularly review records of system activity. The internal audit procedure may utilize audit logs, activity reports, or other mechanisms to document and manage system activity.

2. System activity should be reviewed at intervals proportional to the associated risks of the relevant information system or the EPHI repositories stored on, processed by, or transmitted by the relevant system. The interval of the system activity review must not exceed, but may be less than, 30 days. Evidence that the reviews have been conducted should be documented and retained for at least 1 year.

3. An “Audit Control and Review Plan” must be created by each ePHI system administrator. This plan must include:
   a. Systems and Applications to be logged
   b. Information to be logged for each system
   c. Procedures to review all audit logs and activity reports

4. Security incidents must be detected, logged and reported immediately to the appropriate system management, security and privacy officers.

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