HIPAA Procedure 5142 PR.1
Information Systems Activity Review
Revision Date: 4/20/05

ISAR: Systems Activity Review

This procedure identifies current best practices for reviewing ePHI Systems' activities.

Definitions

Please refer to the "Master Glossary of essential HIPAA Security Terms" in Policy 5100 Electronic Protected Health Information Security Compliance for additional definitions.

Identifying and Tracking ePHI Systems

The ISO will identify Above-Threshold ePHI Systems connected to the Yale University Data Network by procedures such as:

- Registration forms to be completed before connection of devices
- Scanning the network for connected devices
- Network based registration systems e.g. Ethernet MAC address data base or future implementations, and
- Identification of Above-Threshold System Administrators as part of auditorium and web-based training sessions.

Entries in the Above-Threshold ePHI Systems Inventory Database will be updated yearly by the responsible system administrators or data owners.

Configuration Compliance and Activity Review

Information Security office (ISO) will utilize the data in the Above-Threshold ePHI Systems Inventory Database to identify Above-Threshold systems that may need remediation to meet HIPAA requirements. Those systems will be prioritized according to data criticality and the apparent extent of deviation from University standards for HIPAA Security compliance. ISO will assist System Owners to carry out a detailed risk analysis to determine possible steps to eliminate deviation from University standards.

ISO will pay particular attention to optimizing system logging activities and the development of procedures for the review of system logs.

Log and audit standards for Above-Threshold systems:

Log and Audit messages must contain at a minimum:

- Unique timestamp
- System name
- User or daemon where applicable
- Resulting message

For Basic Systems, periodic sampling, or spot checks will be used to review system logs and access reports.

- Group Policy for Windows systems in the Yale University School of Medicine and Yale University School of Nursing AD is set to enforce specific event log and audit settings.

Review of Security Incident Response Reports

ISO will review Security Incident Response reports and link incident reports to corresponding system records in the Above-Threshold ePHI Systems Inventory Database. ISO will provide summary reports to the HIPAA Privacy Officer and to the University CIO.

System User Privileges Grants and Changes Logs

Where appropriate, ISO will expand the Above-Threshold ePHI Systems Inventory Database scope to include questions or sections to address documentation of user privilege grants and changes.

User-Level System Access, Activity, and Transaction Logs

ISO and/or Internal Audit will carry out spot checks of user-level access, activity and transaction and exception logs.