ppdev Policies, Procedures, & Forms

**Yale University Procedures**

# HIPAA Procedure 5142 PR.1 Information Systems Activity Review

**Revision Date: 12/2/2019**

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

## Definitions

A Source System is a system that is the authoritative data source for a given data element or piece of information used for patient care or billing.

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 Source Systems

The University Information Security Office (ISO) will use multiple approaches to identify source systems and shall create and maintain a tracking database for identified source systems:

- The University shall use communications as proactive methods to query members of the Covered Components to self-identity source systems that will be included in the Source System Inventory Database.
- Using the Source System Inventory Database, the ISO shall send annual notices to Source System Owners requiring validation or update of the required system information.
- Using the Source System Inventory Database, the ISO shall identify system entries that are incomplete, out-of-date or appear to fall outside of Yale's IT Security standards and follow up with System Owners, Business Officers and other personnel to ensure that the information is updated, or practices reviewed.

The ISO shall implement a procedure to perform an annual spot check to verify the accuracy of selected systems' data in the Source System Inventory Database

## Configuration Compliance and Activity Review

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

The 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 Source Systems:

Log and Audit messages must contain at a minimum:

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

## Review of Security Incident Response Reports

The ISO will review Security Incident Response reports and link incident reports to corresponding system records in the Source System Inventory Database. The ISO will provide summary reports to the HIPAA Privacy Officer and to the University CIO.

## System User Privileges Grants and Changes Logs

Where appropriate, the ISO will expand the Source System 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

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

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.