
HIPAA Policy 5142

Information System Activity Review

Responsible Office	Information Security Office, Internal Auditing	Effective Date	04/20/05
Responsible Official	Information Security Officer	Last Revision	04/20/05

Policy Sections	1
ISAR.1 Identify and Track Above Threshold ePHI Systems.....	1
ISAR.2 Audit ePHI Systems.....	2
ISAR.2.1 Above Threshold ePHI Systems.....	2
ISAR.2.2 Basic ePHI Systems.....	2
ISAR.3 Respond to Security Incidents.....	2
ISAR.4 Activity Review Scope.....	2
ISAR.5 System Activity Review.....	2

Policy Statement

Working with University Auditing, the Yale University Information Security Office (ISO) will develop systems and procedures to identify, track and periodically audit Above-Threshold ePHI Systems and to periodically audit Basic ePHI Systems for compliance with all applicable laws, regulations and University policies and procedures including all HIPAA regulations.

The Yale University Information Security Office will work with other University offices to promptly respond to any Security Incidents, including a review of HIPAA regulation compliance for any involved Above-Threshold or Basic ePHI Systems.

Reason for the Policy

To ensure that systems containing electronic protected health information (ePHI) are identified, appropriately categorized, monitored and reviewed to ensure compliance with institutional policies and procedures and Federal HIPAA regulations related to system activity controls, and to discourage, prevent and detect security violations.

Definitions

Please refer to the Master Glossary of HIPAA Security Terms in the Definitions section within Policy [5100](#) Electronic Protected Health Information Security Compliance.

Policy Sections

ISAR.1 Identify and Track Above Threshold ePHI Systems

The ISO will use multiple approaches to identify ePHI Systems and shall create and maintain a tracking database for Above-Threshold ePHI Systems:

- The University shall use the HIPAA security training module and other communications as proactive methods to query members of the Covered Components to self-identify Above-Threshold ePHI Systems that will be included in the Above-Threshold ePHI System Inventory Database.

- Using the Above-Threshold ePHI System Inventory Database, the ISO shall send annual notices to Above-Threshold ePHI System Owners requiring validation or update of the required system information.
- Using the ePHI 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 Above-Threshold ePHI System Inventory Database

ISAR.2 Audit ePHI Systems

ISAR.2.1 Above Threshold ePHI Systems

The Yale University Department of Internal Auditing working with the ISO shall perform reviews of Above-Threshold Systems activity and IT security configuration on a defined periodic basis and in conjunction with any routine audits or response to Security Incidents. The frequency and scope of the required activity reviews will be commensurate with each system's data criticality profile based on self-assessment as recorded in the Above-Threshold ePHI Systems Inventory Database as follows:

- **Profile I – High Data Criticality** - The activity in systems whose data profile as High criticality (primary source for TPO) shall be reviewed on an annual basis.
- **Profile II – Medium Data Criticality** - The activity in systems whose data profile as Medium criticality (Primary source for billing or scheduling or other healthcare operations not related to treatment; or primary source for approved research study) shall be reviewed on a rotating basis not to exceed three years.
- **Profile III – Low Data Criticality** - The activity in systems whose data profile as Low criticality (Primary source of PHI for pre-research; or secondary source of PHI for research/pre-research; secondary source of PHI for treatment, payment or healthcare operations; or teaching) shall be reviewed on a rotating basis not to exceed five years.

ISAR.2.2 Basic ePHI Systems

The Yale University Department of Internal Auditing working with the ISO shall perform reviews of Basic Systems activity and IT security configuration on a defined periodic basis and in conjunction with any routine audits or response to Security Incidents.

ISAR.3 Respond to Security Incidents

ISO will develop criteria for use in reporting from the ePHI database aimed at identifying systems that deviate from HIPAA requirements. ISO will work with system owners and administrators to ensure that compliance is achieved. In particular, ISO will examine the procedures for review of system logs.

ISAR.4 Activity Review Scope

The ISO will promptly respond to any security Incidents and will follow-up to assure appropriate compliance with these policies and applicable regulations for any ePHI containing systems involved with security Incidents. Procedure for filing Security Incident Reports and Response are identified under Related Information below.

ISAR.5 System Activity Review

The activity review process shall include an audit of system activity logs and reports at a level commensurate with a particular system's profiled data criticality category. This process may include a

review of the following types of system activity information either as a full review or as a spot check or sampling:

- Review of Security Incidents Response reports
- System user privileges grants and changes logs
- User-level system access logs, if available
- User level system activity logs, if available
- User level transaction log reports, if available
- Exception reports
- The required level of system activity logging and reporting capabilities, and the actual scope of the activity review for each risk profile should differ based upon a system's assigned data criticality level. These logging capabilities and review requirements are defined in the **ISAR Procedure (ISAR.PR1 Systems Activity Review)**.

Procedures

[5142 PR.1](#): Information Systems Activity Review Procedure

Related Information

Policy [5143](#): Security Incident Response & Reporting

Please also refer to the comprehensive summary of HIPAA Security **Related Information** provided within Policy [5100](#) Electronic Protected Health Information Security Compliance.

Forms and Exhibits

Please refer to the comprehensive summary of HIPAA Security **Forms and Exhibits** provided within Policy [5100](#) Electronic Protected Health Information Security Compliance.

Contacts

Please refer to the comprehensive summary of HIPAA Security **Contacts** provided within Policy [5100](#) Electronic Protected Health Information Security Compliance.

Roles and Responsibilities

Please refer to the comprehensive summary of HIPAA Security **Roles and Responsibilities** provided within Policy [5100](#) Electronic Protected Health Information Security Compliance.

Revision History

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.
