Policy Statement

Working with University Auditing, system owners will identify, track and periodically audit source systems containing ePHI for compliance with all applicable laws, regulations and University policies and procedures including all HIPAA regulations.

The source system owner will work with the Yale University Information Security Office to promptly respond to any Security Incidents, including a review of HIPAA regulation compliance for any source system containing ePHI.

Reason for the Policy

To ensure that system owners 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 Source Systems containing ePHI**

The ISO will use multiple approaches to identify source systems containing ePHI and shall create and maintain a tracking database for identified source systems containing ePHI:

- The University shall use the HIPAA security training module and other communications as proactive methods to query members of the Covered Components to self-identity source systems containing ePHI that will be included in the Source System Containing ePHI Inventory Database.
• Using the Source System Containing ePHI Inventory Database, the ISO shall send annual notices to Source System containing ePHI Owners requiring validation or update of the required system information.

• Using the Source System Containing ePHI Inventory Database, the ISO shall identify system entries that are incomplete, out-of-date or appear to fall outside of Yale’s IT Security standards and follow up with System Owners, Business Officers and other personnel to ensure that the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 Containing ePHI Inventory Database

ISAR.2 Audit ePHI Systems

ISAR.2.1 Source Systems Containing ePHI
The Yale University Department of Internal Auditing working with the system owners shall perform reviews of source systems containing ePHI 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 Source Systems Containing ePHI Inventory Database as follows:

• Profile I – High Risk Data Criticality - The activity in systems whose data profile as High criticality (primary source for Treatment Payment or Operations of health care business (TPO)) shall be reviewed on an annual basis.

• Profile II – Moderate Risk Data Criticality - The activity in systems whose data profile as Moderate 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 two years.

• Profile III – Low Risk 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 three years.

ISAR.2.2 Basic ePHI Systems
The Yale University Department of Internal Auditing working with the system owner 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 source 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 for all systems in the Source Systems Containing ePHI Inventory Database.

ISAR.4 Activity Review Scope
The system owner 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.