HIPAA Policy 5142
Information System Activity Review

Policy Sections

| ISAR.1 Identify and Track Source Systems | 1 |
| ISAR.2 Audit ePHI Source 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, system owners will identify, track and periodically audit source systems for compliance with all applicable laws, regulations and University policies and procedures including all HIPAA regulations.

If identified as a source system, the system owner will work with the Yale University Information Security Office (ISO) to promptly respond to any Security Incidents, including a review of HIPAA regulation compliance for any source system.

Reason for the Policy

To ensure that source systems 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

Source System
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 HIPAA Security Terms in the Definitions section within Policy 5100 Electronic Protected Health Information Security Compliance or at https://hipaa.yale.edu/policies-procedures-forms/hipaa-glossary-terms

Policy Sections

ISAR.1 Identify and Track Source Systems
The 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Using the Source System Inventory Database, the ISO shall identify system entries that are incomplete, out-of-date or appear to fall outside of Yale’s IT Security standards and follow up with System Owners, Business Officers and other personnel to ensure that the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.

**ISAR.2 Audit ePHI Source Systems**

The Yale University Department of Internal Auditing working with the system owners shall perform reviews of source 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.

**ISAR.3 Respond to Security Incidents**

ISO will develop criteria for use in reporting from the Source System Inventory 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 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. 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

**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**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Privacy</td>
<td>Chief HIPAA Privacy Officer</td>
<td>203-432-5919</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:hipaa@yale.edu">hipaa@yale.edu</a></td>
</tr>
<tr>
<td>HIPAA Security</td>
<td>University Information Security Office</td>
<td><a href="mailto:Information.security@yale.edu">Information.security@yale.edu</a></td>
</tr>
<tr>
<td>ITS</td>
<td>Central Campus Help Desk</td>
<td>203-432-9000</td>
</tr>
<tr>
<td></td>
<td>Medical School campus Help Desk</td>
<td>203-785-3200</td>
</tr>
</tbody>
</table>

**Roles and Responsibilities**

**Office of the Provost**
Responsible for University compliance issues including HIPAA

**Office of General Counsel**
Interprets HIPAA regulations; reviews and approves all HIPAA related contracts including contracts with Business Associates or for research contracts

**Chief Information Officer**
Individual responsible for planning, development, evaluation, and coordination of University information and technology systems

**University Chief Information Security Officer**
Individual responsible for overseeing information security and ensuring compliance with security requirements of HIPAA

**Chief HIPAA Privacy Officer**
Individual responsible for overseeing and ensuring HIPAA compliance throughout Yale University; coordinates compliance related activities through the following deputies in each of the covered schools, departments, or other entities:

Deputy Privacy Officer, School of Medicine

Deputy Privacy Officer, School of Nursing

Deputy Privacy Officer, Yale Health Services

Deputy Privacy Officer, Yale Health Plan/Benefits Office

Deputy Privacy Officer, Department of Psychology Clinics
Procurement Office

Identifies Business Associates and ensures appropriate contracts are in place

Revision History
Revised 11/2019

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.