HIPAA Policy 5143
Yale University IT Security Incident Response

Responsible Office	Yale University Information Security	**Effective Date**	08/17/10
Responsible Official	Yale University Information Security Officer	**Last Revision**	01/03/2012

Scope

This policy governs the University's general response, documentation and reporting of incidents affecting computerized and electronic communication information resources, such as theft, intrusion, misuse of data, other activities contrary to the University's Acceptable Use Policy, denial of service, corruption of software, computer- and electronic communication-based HIPAA violations, and incidents reported to Yale by other institutions and business entities. This policy does not include damage to personal computers owned by students, unless their computers contribute to the Incident defined by the parameters in Definitions, below.

Policy Statement

The Yale University IT Security Incident Response Policy and subordinate procedures define standard methods for identifying, tracking and responding to network and computer-based IT Security Incidents.

Reason for the Policy

The Yale University IT Security Incident Response Policy is established to protect the integrity, availability and confidentiality of confidential or proprietary information, including ePHI to prevent loss of service and to comply with legal requirements. This policy establishes the coordination of the University's response to computerized and electronic communication systems incidents to enable quicker remediation, information gathering and reporting of infrastructure-affecting and HIPAA-Security related events.

Definitions

An **IT Security Incident ("Incident")** is any activity that harms or represents a serious threat to the whole or part of Yale's computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a "virus," "malware" or similar issue that has little impact on the day-to-day business of the University is not considered an Incident under this policy.

Please also refer to the Master Glossary of HIPAA Security Terms in the Definitions section within Policy 5100 Electronic Protected Health Information Security Compliance.

Policy Sections

5143.1 Identification of Incidents
Any member of the Yale community or individual or organization outside of Yale may refer an activity or concern to the Information Security Office. The ISO itself can also identify an Incident through its proactive monitoring of Yale's network and information system activities. Once identified, the ISO will use standard internal procedures to log and track Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in the remainder of this policy.

5143.2 Establishment of an IT Security Incident Response Team
The Information Security Office (ISO) is responsible for Incident interdiction and remediation of computer- and electronic communication -based resources affected by these incidents. ISO will consult key representatives of Yale ITS, administrators in affected schools, Yale Health Services, Yale Police, Disaster Recovery, and the Legal, Public Affairs, Internal Audit, Academic and Administrative Systems Departments, or other units, as warranted, to establish an IT Security Incident Response Team appropriate to respond to a specific Incident. .

5143.3 Risk Assessment Classification Matrix
The ISO will establish an internal risk assessment classification matrix to focus the response to each Incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an "escalation" of contacts across the University, and will indicate which authorities at Yale to involve and which procedure would be applicable for each class of incident.

5143.4 Documentation and Communication of Incidents
The Information Security Office will ensure that Incidents are appropriately logged and archived. Any IT Security Incidents involving ePHI will be so identified in order to implement the relevant HIPAA Security procedures. Incident reporting will be provided by the Information Security Office to the Yale University ITS Advisory Committee.

Wherever possible, documentation of such Incidents will cross-reference other event databases within the University, such as the Information Security Office trouble ticketing and network monitoring systems, and Yale Police Case Reports. Any Incidents involving systems that are tracked in the Above-Threshold ePHI System Inventory Database will be cross referenced in that database with the ISO incident tracking log.

The Information Security Office or IT Security Incident Response Team representatives will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.

5143.5 Subordinate Procedures
The ISO will maintain standard subordinate procedures for the response and investigation of each Incident, as well as securing the custody of any evidence obtained in the investigation. The application of these procedures will be governed by the classification matrix described in Section 0000.3 above. The procedures will specify the location and method of custody for each incident, if custody of evidence is required.

5143.6 Role of Yale Personnel, Training
Yale personnel are required to report Incidents to the HIPAA Security Officer Hotline (203) 627-4665

5143.7 Relationship to State and Federal Agencies
A response plan or remediation defined by this policy may be preempted as required or at Yale's discretion by the intervention of federal and state executive officials.

5143.8 Incident Prevention
Wherever possible, the University will undertake to prevent Incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its IT resources.

5143.9 Modifications and Adjustments
This policy and its procedures will be reviewed at least annually to adjust processes, identify new risks and remediations.

Special Situations/Exceptions

Any personally-owned devices, such as PDAs, phones, wireless devices or other electronic transmitters which have been used to store ePHI and are determined to contribute to an Incident, may be subject to seizure and retention by Yale Police until the Incident has been remediated, unless the custody of these devices is required as evidence for a court case. By using these devices within the Yale network for business purposes, individuals are subject to University policies restricting their use (see Related Information).

Procedures

The ISO maintains internal procedures for Incident logging, tracking and reporting, for evidence custody and related practices.

Related Information

Policy 1610 Systems and Network Security

Policy 1607 Yale University Information Technology Appropriate Use Policy

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

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

Please also refer to the comprehensive summary of HIPAA Security **Roles and Responsibilities** provided within Policy 5100 Electronic Protected Health Information Security Compliance.

Revision History