

HIPAA Policy 5100**Electronic Protected Health Information (ePHI) Security Compliance**

Responsible Office	Office of the Provost	Effective Date	04/20/05
Responsible Official	Chief Information Officer & HIPAA Privacy Officer	Last Revision	04/20/05

Policy Sections.....	4
5100.1 Institutional Responsibility.....	4
5100.2 Risk Assessment	5
5100.3 System Owner Responsibilities	5
5100.4 Safeguards.....	6
5100.5 Security Awareness and Training	7
5100.6 Reporting a Security Incident.....	7
5100.7 Reporting Violations.....	7
5100.8 Investigation and Enforcement Procedures	7
5100.9 Documentation Requirements	8

Scope

This policy provides an overview of technical, physical and administrative security compliance requirements for faculty, students, staff, and other individuals who create, access, transmit or receive *electronic* protected health information (ePHI).

This policy applies specifically to the University's Covered Components, designated as such for purposes of complying with the privacy provisions of the Health Insurance Portability and Accountability Act of 1996. The Covered Components are: (1) the Group Health Plan Component; and (2) the Covered Health Care Component, comprised of the Yale School of Medicine (YSM), School of Nursing, Department of Psychology clinics and Yale University Health Services (YUHS).

Policy Statement

Yale University Covered Components are required to be in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

Reason for the Policy

This policy provides an entry point and context for implementing measures to comply with the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA).

Overview of HIPAA Security Policies and Procedures

This policy, 5100 Electronic Protected Health Information (ePHI) Security Compliance, and a set of related policies and procedures are adopted to assure Yale University compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule which became effective on April 21st, 2005.

As an introduction to these policies, please refer to the overview of HIPAA Security located at the HIPAA Security web site (<http://hipaa.yale.edu/security>) and take the HIPAA Security online training course linked from the first page of that web site.

This policy, 5100 Electronic Protected Health Information Security Compliance, presents a master definition of terms (The Master Glossary of HIPAA IT Security Terms, below), and master reference lists for Related Information (Section title, below), Contacts (section below), Roles and Responsibilities (section below) and Forms and Exhibits (section below).

The following policies and procedures form a related set and all refer to the common glossary and other noted reference information. It will be easiest to read the other policies with a copy of this policy at hand.

HIPAA Security Specific Policies:

- **5100 – Security and Electronic Health Information (this policy)** – provides the overall approach to HIPAA Security management and includes the Master Glossary of HIPAA Security Terms used in the related set of policies and procedures
- **5123 – Electronic Communication of Health Related Information** – policy governing electronic communications of ePHI
 - [5123 PR.1](#) – ePHI messaging procedures
- **5111 – Physical Security Policy** – describes how to maintain physical security of ePHI Systems
 - [5111 PR.1](#), [5111 PR.2](#) – physical security procedures
- **5142 – Information Systems Activity Review** – how Yale monitors and reviews the activity of ePHI Systems
 - [5142 PR.1](#) – procedure to guide the Systems activity review
- **5143 – IT Security Incident Response Policy** – how clients report IT Security incidents, including those involving ePHI, and how the University will respond

Related IT Security Policies

- **1609 – Media Controls-** protecting confidential information, including ePHI
 - [1609 PR.1](#) - associated procedure
- **1601 – Information Access and Security** – describes who can access information systems, including ePHI Systems
 - [1601 PR.3](#) - procedure guiding management of access to ePHI Systems
- **1610 – Systems and Network Security** – describes how to maintain IT security of information systems including ePHI Systems
 - [1610 PR.1](#) - best practice computer security guidelines
 - [1610 PR.2](#) - disposal of computers

Definitions

[Master Glossary of HIPAA Security Terms](#) used in HIPAA Security related policies & procedures

An **Above-Threshold ePHI System** is a System that creates, accesses, transmits or receives: 1) primary source ePHI, 2) ePHI critical for treatment, payment or health care operations or 3) any form of ePHI and the host System is configured to allow access by multiple people. Examples include:

- A personal computer with a Microsoft Access database containing ePHI that is configured to allow access by more than one person,
- A departmental server with file shares containing ePHI,
- A computer system used to create, access, transmit or receive ePHI that is configured to allow access by a non-Yale vendor/contractor,
- A clinical care system which contains primary source ePHI, and
- A billing system which is critical for clinical operations.

See also: Basic ePHI systems.

The **Above-Threshold ePHI System Inventory Database** is a database maintained by the ISO which records System Owners' or their designees' self-assessment information for each Above-Threshold ePHI System. The ISO and University Auditing use the Above-Threshold ePHI System Inventory Database to identify Above-Threshold Systems for sampling audits and, during those audits, for accuracy of the self-assessments.

Administrative Safeguards are administrative actions and policies and procedures (1) to manage the selection, development, implementation, and maintenance of security measures, and (2) to protect ePHI and to manage the conduct of the Covered Components' workforce in relation to the protection of ePHI.

Basic ePHI System is a System that is typically used by a single individual and is used to create, access transmit or receive ePHI. However, a System, even if used only by a single user, which supports primary source ePHI or ePHI critical for treatment, payment or health care operations is an Above-Threshold System. See also Above-Threshold ePHI Systems.

Contingency Plan sets out a course of action that is maintained for emergency response, backup operations, and post-disaster recovery. The purpose of the plan is to ensure availability of critical resources and facilitate the continuity of operations in an emergency. The plan includes procedures for performing backups, preparing critical facilities that can be used to facilitate continuity of critical operations in the event of an emergency and recovering from a disaster.

Disaster Recovery Plan is the part of a Contingency Plan that documents the process to restore any loss of data and to recover computer systems if a disaster occurs (i.e., fire, vandalism, natural disaster, or System failure). The document defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process to attain the stated disaster recovery goals.

Electronic Protected Health Information (ePHI) is PHI in electronic form.

Emergency Mode Operation plan: is a subset of a disaster recovery plan that documents processes that support continued operation in case of an emergency. Emergency mode operations documentation includes emergency management/crisis management guidelines and procedures to maintain the integrity, availability and confidentiality of protected health information.

Yale's HIPAA Security Training is an online course available from HIPAA Web Site (<http://hipaa.yale.edu/>) which covers policy and practice for conforming to the HIPAA regulations at Yale University.

Information Security Office (ISO) is the Yale University Information Security Office with offices on Yale's central campus at Information Technology Services (ITS) and at the Yale Medical School at Information Technology Services – Medicine (ITS-Med).

Physical safeguards are measures, policies, and procedures to physically protect the Covered Components' Systems and related buildings and equipment that contain ePHI, from natural and environmental hazards and unauthorized intrusion.

Protected Health Information (PHI) is any information that identifies an individual AND relates to:

- The individual's past, present or future physical or mental health; OR
- The provision of health care to the individual; OR
- The past, present or future payment for health care.

Information is deemed to identify an individual if it includes either the patient's name or any other information that taken together or used with other information could enable someone to determine an individual's identity. (For example: date of birth, gender, medical records number, health plan beneficiary numbers, address, zip code,

phone number, email address, fax number, IP address, license numbers, full face photographic images or Social Security Number).

Risk Analysis is a documented assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI, and an estimation of the security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. Risk analysis involves determining what requires protection, what it should be protected from, and how to protect it.

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.

System is any electronic computing or communications device or the applications running thereon which can create, access, transmit or receive data. Systems are typically connected to digital networks. Examples of Systems include:

- A computer system whether or not connected to a data network,
- A database application used by an individual or a set of clients,
- A computer system used to connect over a network to another computer system,
- An analog or digital voice mail system,
- Data network segments including wireless data networks, and
- Portable digital assistants.

System Administrator is the technical custodian of a System. This individual provides the technology and processes to implement the decisions of the System Owner. In some circumstances, e.g. small systems, typically Basic ePHI Systems, the System Administrator and the System Owner may be the same person. System Administrators are responsible for the technical operation, maintenance and monitoring of the System. These duties include implementing appropriate technical, physical and administrative safeguards. See also System Owner.

System Owner is the authority, individual, or organizational head who has final responsibility for Systems which create, access, transmit or receive ePHI and including responsibility for the ePHI data. In some complex Systems, the functional responsibility for the System and the responsibility for one or more applications or ePHI data base(s) may lie with more than one individual. Decisions regarding who has access to the System and related ePHI data and responsibility for the Risk Analysis rest solely with the System Owner. The System Owner usually delegates responsibility for the technical management of a System to a qualified System Administrator or staff who are capable of implementing appropriate technical, physical and administrative safeguards. See also ‘System Administrator’.

Technical safeguards are the technology and the policy and procedures for its use that protect ePHI and control access to it.

Policy Sections

5100.1 Institutional Responsibility

Yale University’s Chief Information Officer shall be responsible for the development and implementation of policies and procedures that are designed to achieve ongoing compliance with the HIPAA Security Rule.

5100.2 Risk Assessment

The Yale University Information Security Office, in collaboration with the Offices of Risk Management, General Counsel and HIPAA Privacy, shall perform an institutional security Risk Assessment across the Covered Components to address HIPAA requirements.

The Yale University Information Security Office, in collaboration with other University Offices, shall perform system specific risk assessments of selected individual critical Systems containing ePHI. These risk assessments shall be documented and shall provide a baseline for subsequent reviews.

On a continuing basis, the ISO shall implement a process to identify ePHI Systems or categories of systems and provide procedures by which System Owners responsible for ePHI-containing Systems can assess compliance with security policies and procedures. (See Information System Activity Review below under Related Information and 0000.3 –System Owner Responsibilities below in this policy).

System Owners who create, access, transmit or receive electronic Protected Health Information (ePHI) must review all Systems and applications with ePHI for which they are responsible and evaluate their vulnerabilities to threats as described in 0000.3 below. Analysis must be done to determine what technical, physical and administrative safeguards are required and how best to implement those safeguards.

5100.3 System Owner Responsibilities

A. Above-Threshold ePHI Systems.

System Owners with responsibility for Above-Threshold ePHI Systems must:

1. Perform a security self-assessment each year of the Above-Threshold ePHI System(s) (“Annual Assessment”).
2. Evaluate the risks to the confidentiality, integrity and availability of the ePHI.
3. Determine what physical, administrative and technical safeguards may be necessary to adequately address the identified risks, based on the Annual Assessment, HIPAA Security policies and procedures and other University guidance. As appropriate, System Owners must develop, document, implement and test a Contingency Plan that includes (1) A Backup Plan (2) An Emergency mode operation plan; and (3) A Disaster Recovery Plan.
4. Manage the Above-Threshold ePHI System(s) in accordance with applicable University procedures including HIPAA Security policies.
5. Successfully complete the HIPAA Security Training offered by the University.

The Annual Assessment completed by System Owners consists of a web-based questionnaire, the answers to which are tracked by ISO in the Above-Threshold ePHI System Inventory Database..

B. Basic ePHI Systems.

System Owners responsible for Basic ePHI systems shall:

1. Successfully complete the HIPAA Security Training offered by the University.
2. Manage the Basic ePHI systems in accordance with the University’s policies and procedures including implementing safe computing practices, HIPAA Security rules, policies and procedures (see Systems and Network Security Policy for required Systems security procedures - identified below under Related Information).

Yale’s HIPAA Security Training details responsibilities and standards for maintaining security of ePHI systems and data and provides information and links to additional resources.

C. Additional Support.

System Owners with responsibility for any ePHI systems may contract with qualified Yale System Administrators to assume System Administrator responsibility or for other support for ePHI systems and applications.

5100.4 Safeguards

The Covered Components shall use reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of ePHI, in accordance with the policies and procedures related to the HIPAA Security Rule. Guidance on appropriate safeguards is provided by:

1. Yale HIPAA Security Policies and Procedures
2. HIPAA Security Training (See link in Related Information below)

Yale's HIPAA Security Training covers the responsibilities of end-users, System Owners, business managers and System Administrators to ensure that appropriate safeguards for ePHI are implemented in accordance with Yale policy.

In case of uncertainty, those responsible for ePHI systems should contact the ISO.

Responsible System Owners may delegate responsibility for implementing safeguards to a qualified IT support group.

- **Physical safeguards**

- Appropriate physical safeguards must be implemented to ensure the confidentiality of all ePHI data regardless of physical location including, but not limited to, ePHI in University data centers, departmental ePHI and ePHI located on non-Yale property.
- Physical safeguards must be implemented for portable computing devices (i.e., laptop, smart phone, PDA) and media storage devices (i.e., USB mini-drive, CD, DVD, diskette).
- University policy and procedure relating to the use, storage and disposal of media containing ePHI are designed to prevent unauthorized access to ePHI.

- **Technical Safeguards**

- System Owners responsible for ePHI data systems, applications and devices are responsible for ensuring that appropriate technical safeguards consistent with University policies are implemented. The adequacy of technical safeguards shall be reviewed regularly in accordance with University policies and procedures. Technical safeguards include, for example, use of antivirus software or activating log-in tracking procedures where appropriate.

- **Administrative Safeguards**

- A range of administrative safeguards is employed to protect ePHI, both at the institutional level and at the System Owner level. HIPAA Security Training is required for all workforce members of the Covered Components who deal with ePHI and sanctions will be imposed for noncompliance with policies and procedures. The ISO monitors electronic information activity and the University Internal Audit also audits compliance with HIPAA Security within the scope of their normal audit activities.
- In addition, System Owners with responsibility for an Above-Threshold ePHI System must develop administrative safeguards for such systems including: (1) A Contingency Plan; (2) An Emergency mode operation plan; and (3) A Disaster Recovery Plan. These plans shall be developed by the responsible System Owner or by a delegated, qualified IT support group. Templates for plans are available (See Forms & Exhibits below). The plans shall be consistent with University policies and procedures and shall be commensurate with the risks to confidentiality, integrity and availability of the ePHI.

- Covered Components may permit a business associate to create, access, transmit or retain ePHI on behalf of the Covered Component only when a business associate agreement is entered into with the business associate that contains all of the requisite assurances in accordance with Policy 5033 Disclosure of PHI to Business Associates.

5100.5 Security Awareness and Training

The ISO shall ensure that HIPAA Security awareness and training programs are in place and available to all members of the workforce who create, maintain, transmit or access ePHI. The ISO shall update the content and the method of the awareness and training programs as needed.

HIPAA Security Training is required of all workforce members in Covered Components who work with ePHI and their participation in training is tracked and reviewed annually to determine if they have completed HIPAA Security Training and to identify Above-Threshold ePHI Systems. Responsible System Owners for Above-Threshold ePHI Systems are surveyed annually on HIPAA Security related practices on their Systems to help ensure that appropriate safeguards for ePHI are implemented in accordance with Yale policy.

5100.6 Reporting a Security Incident

Incidents must be reported to any office of the ISO.

5100.7 Reporting Violations

- If a System Owner has observed or otherwise is aware of a violation of this policy, s/he may report any evidence to the ISO (information.security@yale.edu or information.security@med.yale.edu).
- Individuals who report violations must not be subjected to retaliation or harassment (Policy [5026.2](#)).

5100.8 Investigation and Enforcement Procedures

- Reported violators will be investigated by the ISO and, where appropriate, referred to the HIPAA Privacy Office or other University authorities. The ISO is also authorized to investigate security concerns identified through means other than a reported violation, including routine and targeted monitoring activities.
- Yale IT staff can also be authorized to investigate alleged violations under the direction of the ISO and/or the appropriate disciplinary authority.
- **Disciplinary Procedures:** Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Handbook, Staff Personnel Policies and Practices Manual, various student regulations (e.g. the Undergraduate Regulations for undergraduates, the relevant manuals for graduate and professional school students), and other applicable materials. Staff members who are members of University-recognized bargaining units will be disciplined for violations of this Policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.
- **Sanctions:** Individuals found to have violated this policy may be subject to penalties provided for in other University policies dealing with the underlying conduct. Violations involving ePHI may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator of the affected System, Privacy Officer and Information Security Officer.

- Individuals found in violation of this policy may appeal or request reconsideration of any imposed sanctions in accordance with the appeals provisions, if any, of the relevant disciplinary procedures.
- **Legal Liability.** In addition to University discipline, individuals found in violation of this policy may be subject to criminal prosecution, civil liability, or both.

5100.9 Documentation Requirements

- A written record of an action, activity, or assessment that is required by Yale HIPAA security policies to be documented, must be maintained for six (6) years from the date of its creation or the date when it was last in effect whichever is later. Examples include Security Incident reports, Contingency Plans, policies and procedure histories and business associate agreements.

Special Situations/Exceptions

Units of the Covered Components (e.g. Yale University Health Services) may establish practices and procedures that apply specifically to that unit provided that the practice or procedure is consistent with University policy and requires equal or greater security for ePHI.

Related Information

This section provides a master list of policies, procedures and other information related to HIPAA Security policies and is referred to from other HIPAA Security related policies and procedures.

- [5111](#) Physical Security
- [5123](#) Electronic Communications
- [5026](#) Reporting Protected Health Information (PHI) Compliance Issues
- [1601](#) Information Access and Security
- [1607](#) Information Technology Appropriate Use Policy
- [1607-PR1](#) Endorsed Encryption Implementation Procedure
- [1609](#) Media Controls
- [1610](#) Systems and Network Security Policy and related procedures
- [1610-PR1](#) covers required Systems security practices
- [5003](#) Accounting for Disclosures
- [5033](#) Disclosure of PHI to Business Associates Procedure
- [5039](#): Disclosure of De-identified Information and of Limited Data Sets
- [HIPAA Security Training](#)
- [System Administrators Reference Guide](#)

Forms and Exhibits

This section provides a master list of Forms and Exhibits related to HIPAA Security policies and is referred to from other HIPAA Security policies and procedures.

[5100 EX.A](#): Criticality & Recovery Preparedness Levels for ePHI Systems

[5100 EX B](#): Break Glass Guidance: Granting Emergency Access to Critical ePHI Systems'

[5100.FM.C](#): IT Contingency Plan -- includes a data backup plan, disaster recovery plan and emergency mode of operation plan

[5123 EX.A](#): Guidance on the Use of Email Containing PHI

Contacts

This section provides a master list of contacts related to HIPAA Security policies and is referred to from other HIPAA Security related policies and procedures.

Subject	Contact	Phone
HIPAA Privacy	Chief HIPAA Privacy Officer Deputy HIPAA Privacy Officer, YSM Deputy HIPAA Privacy Officer, YSN Deputy HIPAA Privacy Officer, Psychology Deputy HIPAA Privacy Officer, UHS	436-3650 785-6085 737-5700 436-3650 432-0076
HIPAA Security	ISO, Medical Campus Office ISO, Central Campus Office and University Information Security Officer	785-5204 432-1248
IT	ITS: Distributed Support Specialists ITS-Med Help Desk ITS – Yale School of Nursing YUHS IT Help Desk	<u>DSP</u> 785-3200 785-5405 436-8608

Roles and Responsibilities

This section provides a master list of roles and responsibilities related to HIPAA Security policies and is referred to from other HIPAA Security related policies and procedures.

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 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

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.
