

**HIPAA Policy 5100      Protected Health Information (PHI) Security Compliance**

---

<b>Responsible Office</b>	Office of the Provost	<b>Effective Date</b>	08/17/10
<b>Responsible Official</b>	Chief Information Officer & HIPAA Privacy Officer	<b>Last Revision</b>	08/09/23

---

<b>Policy Sections.....</b>	<b>4</b>
<b>5100.1 Institutional Responsibility.....</b>	<b>4</b>
<b>5100.2 Risk Assessment.....</b>	<b>4</b>
<b>5100.3 System Owner Responsibilities.....</b>	<b>4</b>
<b>5100.4 Reporting Violations and Potential Breaches.....</b>	<b>5</b>
<b>5100.5 Investigation and Enforcement Procedures.....</b>	<b>5</b>
<b>5100.6 Documentation Requirements.....</b>	<b>6</b>
<b>5100.7 Technical, Administrative, and Physical Security Standards.....</b>	<b>6</b>
<b>5100.8 Training.....</b>	<b>6</b>
<b>5100.9 Passwords.....</b>	<b>6</b>
<b>5100.10 Information Technology (IT) Appropriate Use Policy.....</b>	<b>6</b>
<b>5100.11 Paper Records.....</b>	<b>6</b>
<b>5100.12 Device Configuration Standards.....</b>	<b>7</b>
<b>5100.13 Smartphones and Other Mobile Data Devices.....</b>	<b>7</b>
<b>5100.14 Removable Media Devices.....</b>	<b>8</b>
<b>5100.15 Personal Computers and Remote Access.....</b>	<b>8</b>
<b>100.16 File Transfer.....</b>	<b>8</b>
<b>5100.17 Use of ITS Managed Servers.....</b>	<b>9</b>
<b>5100.18 Ensure computing Devices are Physically Secured.....</b>	<b>9</b>
<b>5100.19 Removal of Paper or Electronic PHI.....</b>	<b>10</b>
<b>5100.20 Yale Email Accounts.....</b>	<b>10</b>
<b>5100.21 Recognize when a computer may be compromised.....</b>	<b>10</b>
<b>5100.22 Know your IT support providers and their role in HIPAA Security Compliance.....</b>	<b>10</b>
<b>5100.24 Commercial Data Storage (“Cloud”) Services and Personal Internet-Accessible Data Storage.....</b>	<b>10</b>

---

**Scope**

This policy applies to the University's [Covered Components](#) and those working on behalf of the 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, which includes the School of Nursing, the Department of Psychology clinics, Yale Health and the School of Medicine (except the School of Public Health and the

Departments of Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, Pharmacology, and WM Keck Biotechnology Resources Laboratory).

---

## Policy Statement

Yale University is committed to providing the highest quality health care, which includes respecting patients' and research participants' rights to maintain the privacy of their health information. The standards for protecting health information are described in the federal law known as the Health Insurance Portability and Accountability Act (HIPAA). Yale's HIPAA policies are designed to ensure the appropriate security of all protected health information across the University, in compliance with the law.

---

## Reason for the Policy

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

---

## Definitions

### Above-Threshold ePHI System

A System that creates, stores, 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.

### Administrative Safeguards

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

A system that is typically used by a single individual and is used to create, store, 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

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

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)

PHI in electronic form.

**Emergency Mode Operation Plan**

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 Privacy and Security Training**

Yale requires completion of an initial online course entitled "Foundational HIPAA Privacy and Security Training" as well as an annual refresher entitled "Annual HIPAA Security Attestation and HIPAA Refresher." Both courses are available from HIPAA Web Site (<http://hipaa.yale.edu/>).

**University Information Security Office** is the Yale University Information Security Office

**Physical safeguards**

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)**

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**

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")**

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**

Any electronic computing or communications device or the applications running thereon which can create, store, 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**

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**

The authority, individual, or organizational head who has final responsibility for Systems which create, store, 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 member who is capable of implementing appropriate technical, physical and administrative safeguards. See also 'System Administrator'.

**Technical safeguards**

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 (ISO), in collaboration with the Offices of Risk Management, Office of the General Counsel and HIPAA Privacy shall perform an institutional security Risk Assessment across the [Covered Components](#) to address HIPAA requirements. The HIPAA risk assessment will be reviewed and updated accordingly at least every two years.

The University Information Security Office (ISO) , 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 5100.3 –System Owner Responsibilities below in this policy).

System Owners who create, store, access, transmit or receive ePHI must review all systems and applications with ePHI for which they are responsible and evaluate their vulnerabilities to threats as described in 5100.3 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 cooperate with the University's efforts to maintain HIPAA compliance by:

1. Participating in ISO-led risk assessments
2. Regularly evaluating risks to the confidentiality, integrity and availability of the ePHI and reporting identified or suspected risks to the ISO.
3. Determining 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. Managing the Above-Threshold ePHI System(s) in accordance with applicable University procedures including HIPAA Security policies.
5. Successfully completing the HIPAA Security Training offered by the University on an initial and annual basis.

## **B. Basic ePHI Systems.**

System Owners responsible for Basic ePHI systems shall:

1. Successfully complete the HIPAA Security Training offered by the University, including both the initial and annual training.
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 Reporting Violations and Potential Breaches**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) must immediately report violations of this Policy and/or incidents that may involve the loss of, improper disclosure of, or improper access to PHI or ePHI (for example, the loss or theft of paper PHI; the loss or theft of a computer, smartphone, hard disk or thumb drive storing ePHI; the use of commercial data storage services, including cloud services, that have not been endorsed by Yale; or an electronic intrusion into a computer storing ePHI). Reports should be made to the HIPAA Security Officer hotline: (203) 627-4665.

Even if you believe that no ePHI or PHI was compromised, you must notify the University Information Security Office ([information.security@yale.edu](mailto:information.security@yale.edu)) if you believe that any type of sensitive data was compromised. You must also promptly notify your immediate supervisor and administrative unit head if any Yale University physical or information asset is damaged.

Individuals who report violations must not be subjected to retaliation or harassment (Policy [5026.2](#)).

---

### **5100.5 Investigation and Enforcement Procedures**

Reported violations will be investigated by the University Information Security Office (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 HIPAA policy 5020 Disciplinary Policy for Violation of the Privacy or Security of Protected Health Information.

Individuals found to have violated this policy also 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.

**Legal Liability.** In addition to University discipline, individuals found in violation of this policy may be subject to criminal prosecution, civil liability, or both.

---

**5100.6 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.

---

**5100.7 Technical, Administrative, and Physical Security Standards**

Any electronic computing or communications device or the applications running thereon which can create, store, access, transmit or receive electronic Protected Health Information (ePHI) data must be maintained in accordance with this policy as well as associated HIPAA and information Security policies (see Related Information below for specific policies and procedures as well as [hipaa.yale.edu](http://hipaa.yale.edu)). ePHI data systems are considered high risk and must meet the minimum security standards described at <https://cybersecurity.yale.edu/protectyourdata>.

System Owners responsible for ePHI data systems (including but not limited to applications and devices) are responsible for ensuring all security standards outlined in the University HIPAA Policies and other supporting Information Technology Policies, are implemented throughout the lifespan of the system. System Owners should review the security configurations routinely as well as in response to system changes.

Compliance with security standards and electronic information activity may be monitored by ISO and by University Internal Audit in the course of normal auditing and monitoring activities.

---

**5100.8 Training**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) must complete Yale's Foundational [HIPAA Privacy and Security training](#) as well as the Annual Security Attestation and HIPAA Refresher or be granted an exception by the HIPAA Privacy Officer.

---

**5100.9 Passwords**

All faculty, staff, trainees, students, and others in [Yale University HIPAA Covered Components](#) must use "strong" passwords (8 – 14 characters, with 2 letters and 2 non-letters) for computer and application access, and comply with ITS password security standards located at <http://hipaa.yale.edu/sites/default/files/files/1610-GD01-Selecting-Good-Passwords.pdf>. Passwords shall be reset at least annually.

---

**5100.10 Information Technology (IT) Appropriate Use Policy**

All faculty, staff, trainees, students, and others in [Yale University HIPAA Covered Components](#) must read and abide by [Yale's Information Technology \(IT\) Appropriate Use Policy 1607](#) and other relevant policies. The Information Technology Acceptable Use Policy (ITAUP) is the overarching policy governing the use of computing technology at the university and applies to all individuals who use Yale University computing and networking facilities, including all individuals in the HIPAA covered components. Among critical provisions, the ITAUP prohibits sharing of accounts and passwords unless specifically authorized. The ITAUP also prohibits obtaining unauthorized access to IT systems or permitting others to do so.

---

**5100.11 Paper Records**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) must secure paper records that include PHI in compliance with [Yale's standards for physical security](#) of such records.

---

**5100.12 Device Configuration Standards**

All devices, other than smartphones covered in section 5100.13 below (laptops, desktops, tablets, etc), used in connection with Yale employment or training within the [Covered Entity](#) must follow current University Minimum Security Standards for high risk, HIPAA data.

Please see the [University Minimum Security Standards](#) detailed information regarding configuration requirements.

Any exceptions to the above standards must be vetted by the University ISO, To request an exception, see <https://cybersecurity.yale.edu/policyexceptions>.

Exception for access control policies have been established by the Yale-New Haven Health System (approved by Yale University as of 11/20/2013)

*When accessing an application or system owned or managed by the Yale-New Haven Health System (YNHHS), users shall follow any documented access control policy and guidelines established by YNHHS for that application or system. Where Yale policy imposes a higher standard, in order to better protect PHI, users may employ the Yale standard.*

---

**5100.13 Smartphones and Other Mobile Data Devices**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) must implement current security standards for smartphones and other mobile data devices that create, store, access, transmit or receive ePHI, whether Yale-issued or personal. This includes:

1. **Run supported software and Operating Systems:** Software must be kept up to date: You must use the most recent operating system available for your mobile data device, and you must apply available security updates for any other software (for example, applications) in a regular and timely manner unless instructed otherwise by Yale ITS.
  - a. All applications that create, store, access, send or receive ePHI must meet Yale security standards. Please contact [hipaa.security@yale.edu](mailto:hipaa.security@yale.edu) for additional information. Custom developed applications used on mobile data devices must undergo a Security Planning Assessment (SPA) (<https://cybersecurity.yale.edu/spa>).
2. **Encrypt data:** The data on your mobile data device must be encrypted. If you backup the data from your device to another device that is not encrypted (for example, if you backup your tablet using your unencrypted computer) the backup data must be encrypted.
3. **Use secure passwords:** You must use a password with a minimum of four characters. Your mobile data device must be set to delete all data or lock internally after 10 unsuccessful attempts to enter a password. The device must also require a password after 45 minutes of less of inactivity. Do not share this password with anyone.
4. **Use secure network connections:** All network traffic must use strong, industry standard encryption. Use WiFi networks known to be secure (such as "Yale Secure"). If you cannot use a WiFi network you know uses encrypted traffic, you must use Yale's VPN services to connect to the Yale network.
5. **Enroll in a remote wipe capability:** a feature that allows remote wiping of data in the event a device is lost or stolen must be enabled on the device.

6. **Use Secure Bluetooth** – Turn off Bluetooth when not needed. Be cautious about connecting to others via Bluetooth. Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
7. **No circumvention of device security:** You must not circumvent the security of your mobile data device by removing limitations designed to protect the device (“jailbreaking”), and you must not tamper with your device by using unauthorized software, hardware, or other methods.
8. All other [Minimum Security Standards required for High Risk, HIPAA mobile devices](#). These standards outline further requirements for user accounts, network exposure, and appropriate sanitization and recycling of the device when it is no longer needed.

Exception for access control policies have been established by the Yale-New Haven Health System (approved by Yale University as of 11/20/2013)

*When accessing an application or system owned or managed by the Yale-New Haven Health System (YNHHS), users shall follow any documented access control policy and guidelines established by YNHHS for that application or system. Where Yale policy imposes a higher standard, in order to better protect PHI, users may employ the Yale standard.*

---

#### **5100.14 Removable Media Devices**

All faculty, staff, trainees, students and others in Yale University HIPAA Covered Components may never store ePHI on thumb drives or other removable media devices unless they are encrypted. Yale ITS Provides encrypted, secure USBs. See [https://yale.service-now.com/it?id=service\\_offering&sys\\_id=87688dcd6fbb31007ee2abcf9f3ee427](https://yale.service-now.com/it?id=service_offering&sys_id=87688dcd6fbb31007ee2abcf9f3ee427) for more details.

---

#### **5100.15 Personal Computers and Remote Access**

All devices that create, store, access, transmit, or receive ePHI must meet [Yale's Minimum Security Standards for High Risk, HIPAA data](#). This includes:

- Personal computers tablets, and mobile devices used to create, store, access, transmit, or receive ePHI, and/or
- Personal computers, tablets, and mobile devices used to create a remote access connection to a Yale system that creates, stores, accesses, transmits or receives ePHI.

Exception for access control policies have been established by the Yale-New Haven Health System (approved by Yale University as of 11/20/2013):

*When accessing an application or system owned or managed by the Yale-New Haven Health System (YNHHS), users shall follow any documented access control policy and guidelines established by YNHHS for that application or system. Where Yale policy imposes a higher standard, in order to better protect PHI, users may employ the Yale standard.*

---

#### **5100.16 File Transfer**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) may only forward ePHI data files or datasets outside the University or YNHHS networks, using the encrypted email service or an encrypted storage device. Information on email encryption can be found at <https://cybersecurity.yale.edu/email-encryption>.

---

**5100.17 Use of ITS Managed Servers**

All servers used to store ePHI must be managed by ITS whenever any one of the following conditions apply:

- a. You are storing the ePHI of 500 or more patients;
- b. Access to the ePHI is shared by more than one user;
- c. The files containing the ePHI comprise 500 GB of data or more.

Exceptions must be approved by the Yale Information Security Office. In approved circumstances, the following requirements apply:

- a. The computer must subscribe to the ITS backup service;
- b. The computer must be registered in the IP Address Management System.
- c. The database or system must complete an ISO [Security Planning Assessment \(SPA\)](#).

---

**5100.18 Ensure computing Devices are Physically Secured**

Reasonable and appropriate physical security must be implemented to secure computing devices housing ePHI including:

- Privacy filters must be installed on computer screens that display ePHI and can be viewed by the public or non-clinical staff.
- A screensaver that hides the screen after 10 minutes of inactivity and requires a password to restore the display must be used.
- When computers may be unattended or unmonitored for extended periods, the space should be secured through locking the room or area to minimize unauthorized physical access to your computer and data or data theft (e.g. inserting a disk or CD with tools for “hacking”)
- A locking cable or equivalent physical protection (e.g. locked cabinets) used for all devices when not in the user’s physical custody.
- ePHI in local departments, data centers, or on non-Yale property must be inventoried to include the exact location of ePHI and the specified and adequate physical security implemented to ensure that individuals who have no need to access ePHI systems cannot do so. These protective measure cover all types of computing mediums such as data servers, desktop PCs, personal digital assistants(PDAs), USB devices, CDs, DVDs, Diskettes, memory sticks, flash cards, smart phones and any future medium used to store ePHI -- whether these computing mediums are located on Yale property or not.
- Portable computing devices must never be left unattended and unlocked.

These standards are applicable to all sites where Yale ePHI may be created, stored, accessed, transmitted, or received, including Yale business locations outside New Haven which must abide by appropriate security policies which meet the same standards.

Additionally, all faculty, staff and trainees are reminded to be cognizant of security. If you see someone in your area and you are uncertain if they have legitimate business to be there, either engage them to provide appropriate help or contact the Yale Security Department.

See Policy [5111](#) Physical Security policy and related procedures for additional details.

---

#### **5100.19 Removal of Paper or Electronic PHI**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) must securely destroy or delete paper PHI or ePHI when no longer needed or when retiring computers, smartphones or other mobile devices such as thumb drives. Refer to Procedure 1609 PR1, Disposal of Media Containing Confidential or Protected Health Information.

---

#### **5100.20 Yale Email Accounts**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) must not configure Yale email accounts which may receive or transmit ePHI to auto-forward messages to non-Yale email accounts. (e.g. Google, Yahoo, Hotmail)

For email transmission of ePHI, implement and use only the procedures permitted in [Policy 5123](#) Electronic Communication of Health-Related Information (Email, Voice Mail, and other Electronic Messaging Systems).

---

#### **5100.21 Recognize when a computer may be compromised.**

All faculty, staff, trainees, students and others in [Yale University HIPAA Covered Components](#) are expected to remain vigilant in their attention to information security and mitigate potential incidents in a timely manner. If you notice your personal computer is exhibiting any unusual behavior (e.g. rebooting by itself, suddenly slowing dramatically), seek assistance from your IT support staff to determine if your computer may have been compromised.

---

#### **5100.22 Know your IT support providers and their role in HIPAA Security Compliance**

All faculty, staff, and students on campus have access to IT support staff and must be aware of who they are and the services they provide before you need them. IT support staff (Help Desks and Technicians) are trained in routine information security support and Yale's [cybersecurity website](#) has comprehensive information on general IT security best practices. Yale's HIPAA Security page has information on specific HIPAA Security policies for all faculty, staff, trainees, students and others in the [Covered Components](#).

If you have any questions about HIPAA Security Compliance or IT security concerns generally, you should contact one of the University Information Security Office at [information.security@yale.edu](mailto:information.security@yale.edu).

---

#### **5100.24 Commercial Data Storage ("Cloud") Services and Personal Internet-Accessible Data Storage**

ePHI may not be stored on any commercial data storage service unless the service has been approved by ITS and has signed a Business Associate Agreement with Yale. Approved applications can be found at <https://cybersecurity.yale.edu/protectyourdata>. Under no circumstances may ePHI be stored on a personal Internet-accessible data storage device.

---

### **Special Situations/Exceptions**

Units of the [Covered Components](#) (e.g. Yale Health) 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.

#### **Exception for access control policies established by Yale-New Haven Health System (YNHHS)**

(Please see Section 5100.12.)

---

### **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
- **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**
- 
- [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
- [1609-PR01](#) Disposal of Media Containing Confidential or Protected Health Information
- [1610](#) Systems and Network Security Policy and related procedures for non-ePHI data
- [1610-PR1](#) covers required Systems security practices for non-ePHI data
- [1610 PR.02](#) - disposal of computers
- [1610 PR.05](#) – Device Security Standards
- [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

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

---

## Contacts

Subject	Contact	Contact Information
HIPAA Privacy	Chief HIPAA Privacy Officer	203-432-5919 hipaa@yale.edu
HIPAA Security	University Information Security Office	Information.security@yale.edu
ITS	Central Campus Help Desk Medical School campus Help Desk	203-432-9000 203-785-3200

---

## 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 10/26/2011, 11/20/2013 (Covered entity definition change, exception for YNHHS access control policies added), 9/24/14 (device encryption requirements updated and 3<sup>rd</sup> party storage section added). 11/9/2019, 5/2022 clarification on personal devices, 2/2023 removed email limits on mobile devices and updated terminology. 8/2023 updates to mobile device (sec 13) and data transfer (sec 16) requirements.

---

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.

---