

## Policy 1610 Systems and Network Security Policy

<b>Responsible Office</b>	Office of the Provost	<b>Effective Date</b>	04/20/05
<b>Responsible Official</b>	Chief Information Officer Privacy Officer	<b>Last Revision</b>	04/20/05

<b>Policy Sections</b> .....	<b>2</b>
1610.1 Use and Configuration of Computing or Communication Systems.....	2
1610.2 Computing and Communications Systems Security for individuals who create, access, transmit or receive Electronic Protected Health Information.....	2
1610.3 Remote Access for Individuals not affiliated with Yale University:.....	2

### Scope

This policy establishes IT security requirements for faculty, students, staff, and other individuals who use computing or communications Systems during the course of their work at Yale University. This includes Systems use on-campus as well as from remote locations, such as home, hotels and other off-campus locations.

This policy also applies specifically to the University's Covered Components, designated as such for purposes of complying with the 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

This policy defines University standards for managing computing and communications Systems and access to Yale University's data network and electronic data resources. All Confidential Information including electronically stored information must be protected in a manor commensurate with its sensitivity, value and criticality; this includes protecting computing and communications Systems containing that data accordingly. Safeguards regarding confidentiality and privacy of Yale information apply equally at on-campus locations and at any remote location. Procedures associated with this policy establish currently appropriate required and best practices for managing computing and communications Systems and network access.

The University may, at any time, change any or all of the conditions under which any individual is granted computing or communications Systems or data network access privileges and may terminate such privileges at any time.

### Reason for the Policy

Sound business practice as well as compliance with regulations requires appropriately protecting the confidentiality, integrity and availability of Yale electronic information. The efficiency of conducting Yale business depends on minimizing the impact of information security vulnerabilities.

Compliance with the requirements of the 1996 HIPAA regulations requires implementation of procedures to protect the confidentiality, integrity and availability of electronic Protected Health Information.

---

## Definitions

**Data Network Access** is the use of a communication System to communicate or exchange data among two or more Systems by any means including both wired and wireless network access.

**Remote Access** is any access to a device on the Yale University data network through a non-Yale controlled network, device, or medium, for example by DSL, cable modem or dial-up connection.

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

---

### 1610.1 Use and Configuration of Computing or Communication Systems

Any individual who uses a computing or communications System to create, access, transmit or receive Yale related information is responsible for protecting that information in a manner commensurate with its sensitivity, value, and criticality. Appropriate procedures regarding confidentiality and privacy of information are to be followed at all times regardless of location on or off-campus. Appropriate procedures are detailed in the Systems Security procedure referenced below under Procedures.

Damage to, loss, or unauthorized disclosure of any Yale University physical or information assets must be promptly reported to the employee's immediate supervisor and the cognizant administrative head. Any incident where sensitive data is thought to have been compromised must be reported to the ISO.

Individuals who are granted access to Yale's Systems including the data network, whether from on-campus or via Remote Access, are responsible for protecting against the loss, damage or compromise of Yale University physical and electronic information assets.

---

### 1610.2 Computing and Communications Systems Security for individuals who create, access, transmit or receive Electronic Protected Health Information

Compliance with the associated procedure ([1610 PR1](#) Systems and Network Security Procedure) is specifically required for any individuals who create, access, transmit or receive ePHI on computing or communications Systems including over Yale's networks.

---

### 1610.3 Remote Access for Individuals not affiliated with Yale University:

Individuals not associated with the University (vendors/contractors, research collaborators) with remote access privileges must utilize a secure access method. Such individuals working with ePHI may be required to sign a Business Associate agreement that includes text approved by General Counsel, which specifies HIPAA compliance before they are granted remote access.

Non-Yale vendors/contractors with Data Network Access privileges must utilize a secure method for access that provides equivalent or better security as that of a University Virtual Private Network connection, and be able to provide documentation of those methods.

---

## 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.

---

## Procedures

Procedure [1610 PR.1](#) – Systems and Network Security Procedure

Procedure [1610.PR.2](#) -Disposal of Obsolete Computers and Peripherals

## Related Information

[Policy 1607](#): Information Technology Appropriate Use Policy

[Policy 1609](#): Media Control

[Policy 5033](#): Disclosure of PHI to Business Associates

Procedure [3501.PR.22](#): Non-Employees: Directory Listing and Access Privileges

Please also refer to the comprehensive summary of HIPAA Security **Related Information** 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

Subject	Contact	Phone
Information Security	University Information Security Officer	432-1248
	YSM - Director, Systems Engineering & Security	785-5204
ITS	ITS: Distributed Support Specialists	<a href="#">DSP</a>
	ITS-Med Help Desk	737-2233
	ITS - Yale School of Nursing YUHS IT Help Desk	785-5405 436-8608

Please also refer to the comprehensive summary of HIPAA Security **Contacts** provided within [Policy 5100](#) Electronic Protected Health Information Security Compliance.

## 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 Information Security Officer

Individual responsible for overseeing information security and ensuring compliance with security requirements of HIPAA

- Deputy Privacy Officer, Department of Psychology Clinics

**Procurement Office**

Identifies Business Associates and ensures appropriate contracts in place

**Grants & Contracts Administration**

Responsible for negotiating data use agreements and research related contracts.

**Institutional Review Boards (HIC, HSC, HSRRC)**

Responsible for review and approval of waivers of authorization for research purposes.

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**

---

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.

---