

HIPAA Policy 5111

Physical Security

Responsible Office	Office of the Provost	Effective Date	4/14/03
Responsible Official	Chief Information Officer & HIPAA Privacy Officer	Last Revision	4/20/05

Policy Sections	2
5111.1 Physical Access and Environmental Supports of ITS and ITS-Med Data Centers.....	2
5111.2 Physical Access and Environmental Supports on Yale Property Outside the Data Centers	2
5111.3 Physical Access and Environmental Supports on Non-Yale Property	2
5111.4 Physical Security of Portable Electronic Devices.....	2
5111.5 Safeguards for Computing Display Screens	2

Scope

This policy applies 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 School of Medicine, School of Nursing, Department of Psychology clinics and Yale University Health Services.

This policy was developed to protect against unauthorized physical access to protected health information (PHI) in all formats (electronic or ePHI, paper video, audio etc.). This policy covers PHI on campus and on non-Yale property.

Policy Statement

Unauthorized physical access to protected health information (PHI) is prohibited.

Reason for the Policy

This policy was designed to comply with the federally mandated privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) - Public Law 104-191.

Definitions

Protected Health Information (PHI) - Protected Health Information means 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, NetID or Social Security Number)

Data Center - A data center is a centralized repository for the storage, management, and dissemination of data and information organized around a particular area or body of knowledge (e.g., University financial and HR data, or patient scheduling, billing and medical records). At Yale University this refers to centrally controlled data centers owned and operated by ITS or ITS-Med.

Policy Sections

This Policy is designed to set physical parameters to ensure the integrity of PHI and restrict access to unauthorized individuals.

5111.1 Physical Access and Environmental Supports of ITS and ITS-Med Data Centers

The University is responsible for maintaining a *Physical Facility Security Plan* for University ITS and ITS-Med Data Centers. The University Physical Facility Security Plan ensures that PHI (Protected Health Information) in any format (electronic, paper, audio tapes, transcripts, videotapes, etc.) that is housed in University and ITS-Med data center locations meets HIPAA requirements for physical security. Copies of the University's Physical Facility Security Plan are maintained by Yale University Office of Facilities, ITS and ITS-Med.

5111.2 Physical Access and Environmental Supports on Yale Property Outside the Data Centers

It is the responsibility of departmental business managers to implement safeguards such that protected health information within their department is protected from physical access by unauthorized individuals and environmental safeguards are in place to protect the confidentiality, access and integrity of PHI as commensurate with data criticality and risk assessment. The Department of University Security Programs can assist individual departments in selecting appropriate options.

5111.3 Physical Access and Environmental Supports on Non-Yale Property

It is the responsibility of departmental business managers to certify that protected health information located at non-Yale business locations (e.g., YNHH, WHVA) is adequately protected from physical access by unauthorized individuals and that environmental safeguards are in place to protect the confidentiality, access and integrity of PHI as commensurate with data criticality and risk assessment. The Department of University Security Programs can provide consultations and work as a liaison with the other location for physical security issues.

Physical access to PHI or ePHI that is maintained at home, at a non-Yale business location or on non-Yale owned equipment is the responsibility of the individual.

5111.4 Physical Security of Portable Electronic Devices

Portable electronic devices used to create, access or receive Electronic Protected Health Information (ePHI) will be subject to special requirements designed to minimize the risk of inappropriate disclosure of ePHI through theft or accidental loss.

5111.5 Safeguards for Computing Display Screens

Procedures must be in place to ensure that the inappropriate access or viewing of the display screen of any computing device that creates, receives or distributes ePHI (Protected health Information) is minimized. Compliance is paramount in patient or research-subject areas.

Procedures

[5111 PR.1](#) Physical Facility Security Plan for University and ITS/ITS-Med Data Centers

[5111 PR.2](#) Physical Access and Environmental Supports to Protected Health Information

Related Information

Policy [1609](#): Policy and Procedure on Media Controls

Policy [1601](#): Authorization, establishment, modification & termination of information access

Forms and Exhibits

5111.EX.A - Yale University Physical Facility Security Plan (forthcoming)

Contacts

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

Subject	Contact	Phone
Assistance with physical security options	Department of Security	785.5555

Roles and Responsibilities

Please 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.
