HIPAA Policy 5111
Physical Security

Responsible Office	Office of the Provost	**Effective Date**	8/18/10
Responsible Official	Chief Information Officer & HIPAA Privacy Officer	**Last Revision**	12/1/2019

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).

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 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.

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 Data Centers

The University is responsible for maintaining a *Physical Facility Security Plan* for University ITS 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 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 and ITS.

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

It is the responsibility of departmental Lead Administrators 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, availability and integrity of PHI as commensurate with Minimum Security Standards. The Department of University Security (Physical Security) can assist individual departments in selecting appropriate options. Safeguards must be implemented throughout the life cycle of devices containing PHI, including through decommissioning (see also Policy 1609, Media Controls and associated procedures.)

5111.3 Physical Access and Environmental Supports on Non-Yale Property

It is the responsibility of departmental Lead Administrators 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 store, access, transmit 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 is minimized. Compliance is paramount in patient or research-subject areas.

5111.6 Physical Security of Paper Records

You must secure paper records that include protected health information: Policy guidelines for physical security.

You must immediately report all incidents that may involve the loss or theft of any such paper records.

Call: (203) 432-3262 to report potential breaches

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

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 12/2019