

HIPAA Procedure 5111 PR.2

Protected Health Information: Physical Security & Environmental Supports

Revision 4/20/05

Overview	1
Departmental business managers of the Covered Components are responsible for implementing physical safeguards such that .	1
General Recommendations	1
Environmental Safeguards.....	1
Physical Security of Portable Devices	2
Safeguards for Computing Display Screens	2
Recommendations: Specific Situations.....	2
YNHH, WHVA and Other Non-Yale Locations	3
YNHH	3
WHVA	3
Other non-Yale Business Locations.....	3

Overview

Departmental business managers of the Covered Components are responsible for implementing physical safeguards such that

- departmental protected health information (ePHI & PHI in all formats) is adequately protected from physical access by unauthorized individuals and
- environmental safeguards are in place to protect the integrity of all primary source PHI
- security measures are commensurate with the criticality of the data, as well as the risk of loss of confidentiality, access or integrity of the data.

Business Managers will maintain documentation of their plan to address risks that exist from loss of environmental supports or physical access to PHI by unauthorized individuals.

General Recommendations

- The current recommendations are to use [alarm keypad systems](#) (change key codes often) or ID key card swipes for labs, classrooms or areas accessed by multiple individuals. Keep current documentation of
 - who can authorize access to the area
 - individuals who currently have access and their status at the University
- Electronic storage devices (diskettes, CDs/DVDs, zip drives, external drives, video/audio tapes, USB drives, etc) and non-electronic PHI (images, medical records, lab results, paper files, etc.) should be kept in secure locations when not in use. Locked cabinets, closets and offices can provide this protection.

[Move and Gone reports](#) (needs permanent URL) should be used to remove access ASAP when an individual's status changes or if the individual leaves the University.

Environmental Safeguards

Primary source PHI for TPO (treatment, payment or healthcare operations), approved research, pre-research, should reside in an environmentally controlled location with:

- working fire extinguisher
- air-conditioning (important for electronic data)
- power supply – UPS (important for electronic data)

- back-up at another location

System Owners should identify and address risks that exist from loss of environmental supports to the PHI.

Physical Security of Portable Devices

- Portable electronic devices used to create, access, transmit or receive Protected Health Information (PHI) are subject to special requirements designed to minimize the risk of inappropriate disclosure of PHI through theft or accidental loss. Portable devices include, but are not limited to, laptop, notebook and sub-notebook computers, hand-held computers, palmtops, Personal Digital Assistants (PDAs), and smart phones.
 - The owner of a portable electronic device containing ePHI must provide reasonable safeguards, and manage the location of the device, so as to prevent unauthorized access to the ePHI. These measures must be commensurate with the data criticality and risk.
 - Any portable electronic device containing ePHI must be physically secure when unattended.
 - Physical security is the responsibility of the device owner, who is also responsible for appropriate disposition of the device when it is retired from use (see Policy 1609: Media Control).
- See also: [S.T.O.P.](#) Program

For *technical security* compliance issues see Policies [1610](#) (Systems and Network Security); [1607 PR1](#) (Encryption); and [5100](#) Electronic Protected Health Information (ePHI) Security Compliance.

Safeguards for Computing Display Screens

Users must ensure that 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.

- Whenever possible display screens must be positioned to minimize the risk of unauthorized individuals being able to intentionally or inadvertently view the screen.
- When in use, portable or hand-held devices should be held in a manner so as to avoid visual access by unauthorized individuals. When not in use, diligence is required in placement of the device, so as to avoid visual (and physical) access by unauthorized individuals.
- Password protected screen savers should be used to minimize unauthorized access from non-authenticated personnel. This functionality is built in to many operating systems, but there are also third party software solutions. Contact ITS, ITS-Med or your local IT support staff for assistance.
- Privacy screens (polarizing/anti-glare) are available in different mounting configurations and sizes to fit most monitor shapes and sizes. Contact ITS, ITS-Med or your local IT support staff for assistance.
- For some situations, display screen visors or shades may provide an alternative to a privacy screen. Contact ITS, ITS-Med or your local IT support staff for assistance.

Recommendations: Specific Situations

The Department of University Security Programs can make recommendations about appropriate options. Contacts:

- <http://www.yale.edu/yalesecurity/contact.html>
- some.one@yale.edu
- phone number

YNHH, WHVA and Other Non-Yale Locations

Personnel, especially within departments at the School of Medicine, create, access, receive and/or transmit PHI in all formats (electronic/ePHI, paper, film etc.) at non-University locations. The physical security of PHI at non-University locations must be protected in compliance with HIPAA regulations, just as it is on campus.

YNHH

Yale University Department of Security Programs will

1. coordinate the identification (in conjunction with YSM FD&O, YSM business managers and ISO-Med) and documentation of all locations where University PHI is located in YNHH physical space
2. serve as a liaison to Yale-New Haven Hospital security/facilities personnel to ensure adequate safeguards are made available to University personnel to comply with HIPAA physical security requirements.
3. provide yearly updates of location documentation and a list of members of the Yale/YNHH liaison group, as of 01 July. An electronic copy of this documentation will be sent by the Director of Yale University Department of Security Programs to the University HIPAA Privacy Officer to be kept on file.

WHVA

Yale University Department of Security Programs will:

1. coordinate the identification (in conjunction with University personnel at the West Haven VA Hospital, departmental business managers and ISO-Med) and documentation of all locations where University PHI is located in WHVA physical space
2. serve as a liaison to WHVA security/facilities personnel to ensure adequate safeguards are made available to University personnel to comply with HIPAA physical security requirements.
3. provide yearly updates of location documentation and a list of members of the Yale/WHVA liaison group, as of 01 July.

Other non-Yale Business Locations

Departmental Business Managers will

1. coordinate the identification and documentation of all locations where department PHI is located in an off-site physical space
2. when possible, establish a liaison arrangement with security/facilities personnel at the off-site location to ensure adequate safeguards are made available to University personnel to comply with HIPAA physical security requirements.
3. maintain documentation of location of the Department's PHI and a list of members of the liaison group, as of 01 July.

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.
