HIPAA Procedure 5111 PR.2
Protected Health Information: Physical Security & Environmental Supports

Revision 12/2/2019

Overview

Departmental lead administrators 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.

Lead administrators 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.

WorkDay Hires and Staffing Reports 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.

Recommendations: Specific Situations

The Department of University Security (Physical Security) can make recommendations about appropriate options. Contacts: https://your.yale.edu/community/public-safety/yale-security-department

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 and in transit between locations must be protected in compliance with HIPAA regulations, just as it is on campus.

Other non-Yale Business Locations

Departmental lead administrators 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.

Transporting PHI

PHI, including but not limited to, patient lists, personal notes on patient care, treatment records, human research records etc., must be secured in transit against loss, theft, or inappropriate access including the following controls, as appropriate:

1. When PHI must be transported within the University or to off-site locations, the minimum necessary PHI should be transported.
2. An inventory of PHI being transported must be created and stored separately so that in the event of a data breach, the information that was lost can be identified.
3. PHI must be transported in closed containers such as closed envelopes to minimize portions of the PHI being lost en route.
4. When PHI will be transported off campus, a lock box or lock bag must be used to secure the information and must not be left unattended in a visible location of the vehicle.

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.