

**Policy #:** DHHS-02-16

**Issue Date:** 1/26/16

**I. SUBJECT**

HIPAA Privacy: Physical Safeguards

**II. POLICY STATEMENT**

The Maine Department of Health and Human Services (the Department) will use reasonable physical safeguards to maximize the confidentiality of protected health information (PHI), and other confidential client information (together, Protected Information or "PI") in any format.

**III. RATIONALE**

The Department must comply with state and federal requirements to safeguard the integrity, confidentiality and availability of PI.

**IV. PROCEDURE**

**1. Regarding Consumers and/or their Personal Representatives:**

- a. Consumers and/or their Personal Representatives (Consumers) will remain in public common areas until ready to be seen by Department staff.
- b. Consumers will register at the appropriate reception desks to be administratively cleared by the appropriate workforce member before being allowed to facility or program locations.
- c. Consumers will be escorted to and from interview, treatment or meeting rooms, as applicable.
- d. Computer screens will be turned away from public view, unless used by a workforce member to share information with a patient or family member.

**2. Regarding Workforce Members -** The Department's physical safeguards shall include, but not be limited to, the following:

- a. Access badges and keys that are issued by management to facilities, offices and workstations; loss of access badges and keys are required to be reported immediately consistent with Security of and Access to DHHS Office Policy.

- b. Paper records will not be left in areas easily accessible to the public, and will be stored securely when not currently required for a business purpose. Both clinical and financial paper files will be locked in a secure location at the end of each business day, where locks are available, otherwise, they will be put out of sight. Paper-based PI shall not be removed from the Department without approval of the workforce member's supervisor, and only with the understanding of the work purpose and the reasonable and appropriate safeguards to be observed.
- c. Reasonable physical safeguards will be applied to the Department desktop computers to prevent unauthorized access or removal of the media or hardware.
- d. When laptops or other portable media are not being used, they will be stored in a physically secure location. Portable media within the Department will be locked at the end of the business day.
- e. Portable media off-site that may contain PI must be secured through physical protections such as cabinet and door locks. These safeguards are in addition to observing appropriate administrative safeguards, such as Department Privacy and Security Policies, and appropriate technical protections such as strong technical safeguards provided by OIT and observed by the Department.
- f. Loss of portable media or possible unauthorized access to PI in any format will be reported immediately to the Privacy/Security Liaison for follow up with the Director of Healthcare Privacy.
- g. Off-site work performed via portable media or home computer must be cleared for physical security by the Privacy/Security Liaison, and must meet the Department policy standards to maintain the confidentiality, integrity and accessibility of data.
- h. Keys to the locked areas containing PI will be maintained by the appropriate member of management, and only issued as necessary and appropriate.
- i. Internal office doors or other areas will be secured if PI may be accessed in that location. External office doors are locked after business hours.
- j. Back-up media or non-current or inactive PI shall be stored and maintained in a secure, off-site location consistent with retention/distruction guidelines. An appropriate Business Associate Agreement shall be executed with any off-site storage vendor, and shall include necessary breach notification safeguards.
- k. Paper documents containing PI that is no longer needed will be placed into a shredding bin for collection consistent with the Department's Document Destruction Policy.
- l. Outdated hard-drives, copy machine and fax machine memories, CDs, etc. will be destroyed through OIT as required by current business standards, including sanitizing or wiping the memory and/or physically destroying/crushing the media to ensure that PI cannot be used or accessed.

- m. Transport of DHHS documents containing PI must be made by Department workforce or contractors who have signed an appropriate agreement containing confidentiality language with the Department.
- n. Upon destruction of paper, electronic or other forms of PI including hard-drive, film, CD, etc. by a professional, it is the policy of the Department to receive a "certificate of destruction" that will be maintained and to show our good faith efforts in protecting the PI in its possession.
- o. The Director of Facilities shall maintain a file with proof of destruction of PI.
- p. The Director of Facilities either a) maintains certain records of security efforts, including certificates of destruction and proof of security and access systems and maintenance, or b) has access to such records where maintained by others.
- q. All workforce members will receive training regarding the reasonable and appropriate safeguards required by our practice in an effort to protect PI and other information assets. Violations of this physical security policy, or any of the Department's privacy or security policies, shall be addressed by the Privacy/ Security Liaison in accordance with the Department Privacy and Security Sanctions policy.

**V. DEFINITIONS**

***Protected Health Information*** is information about a patient, including demographic information that may identify a patient, which relates to the patient's past, present or future physical or mental health or condition, related health care services or payment for such services.

**VI. DISTRIBUTION**

All Staff via e-mail and posting on the DHHS Intranet.

1/24/14  
Date

Mary C. Mayhew  
Mary C. Mayhew  
Commissioner