CHAPTER 6
PHYSICAL AND TECHNICAL SECURITY

I. OVERVIEW

This Chapter 6 sets forth the safeguards DMH has put in place to protect the physical and technical security of its Information Resources, including data. This includes, but is not limited to, protection from unauthorized access, theft, loss, or environmental hazards. Pursuant to HIPAA privacy requirements, access to Information Resources is limited to Workforce Members who are authorized to access such information, as set forth in Chapter 4, Section II, Obtaining Access, of this Handbook.

DMH endeavors to implement reasonable and appropriate security measures. To determine the appropriate measures, full consideration is given to DMH business needs, available resources and technologies, and the level of sensitivity of data that needs to be protected. This Chapter 6 addresses Workforce Member responsibility to ensure the safety and security of Information Resources, including, without limitation, data and electronic devices, while they are commuting/in transit and/or Teleworking.

In addition to this Chapter 6, Workforce Members must comply with Chapter 3 of the Privacy Handbook regarding Physical and Technical Safeguards and Chapter 7 of this Handbook regarding Electronic Mail.

II. DMH SECURITY PLANS FOR INFORMATION RESOURCES

The purpose of a Security Plan is to address how Information Resources, Sensitive Information, including PHI, located at each DMH Location will be protected from unauthorized access, theft, loss, and environmental hazard.

A. Responsibility for Developing a Security Plan for Each DMH Location

1. **Person in Charge**. The Person in Charge of each DMH Location or designee is responsible for developing, implementing, and documenting a Location specific Security Plan. In developing the Plan, particular focus must be given to those Information Resources and Devices that store, transmit, and/or receive EPHI. (*See* attached Security Plan Form.)

2. **Contents of the Security Plan.** A Security Plan must, at a minimum, incorporate the standards set forth in this Chapter 6 regarding physical and technical security.

3. **Implementation Date and Annual Review.** A DMH Location shall have a Security Plan, developed and reviewed in accordance with this Chapter 6. Any new Location shall develop, document, and implement its Security Plan prior to commencing operations. The Person in Charge or designee must review and amend, as necessary, the Security Plan at a minimum annually, or more frequently as appropriate considering the nature of the EPHI maintained at the Location, improvements in security technologies, and the number and type of Information Security Incidents that may have occurred at the Location. (*See* Chapter 2, Information Security Incident Reporting and Response Procedures.)

4. **Annual Review of Security Plan Compliance and Other Safeguards.** On an annual basis the applicable Information Security Coordinator or the DMH ISO or designee will review the Security Plan and other safeguards compliance of each Location with the Person in Charge. This review should include a walk-through of the Location with the Person in Charge or designee to ensure that changes to the Location involving data and security have been addressed in the Security Plan and to identify issues that could result in security breaches or other compliance issues. DMH has developed a Security Walk Through Job Aid, which is attached to this Chapter 6.

5. **Copies to the DMH ISO.** Each Person in Charge or designee is responsible for providing the DMH ISO with a copy of their Security Plan, all modifications to it, and each annual compliance review. The DMH ISO shall review each Security Plan for compliance with this Chapter 6 and reasonableness.

6. **Retention**. Each Security Plan, modification, and annual compliance review must be maintained by the Person in Charge in accordance with the Massachusetts Statewide Records Retention Schedule published by the Secretary of State's Office; provided, however, that a Security Plan must be maintained for a minimum of six (6) years from its last effective date.

III. ENTRANCES TO DMH LOCATIONS

To the extent possible, physical access to any building at a Location where there are Information Resources must be limited. A Security Plan must account for the entrances to all such buildings by indicating which will be open to the public, limited for use by Workforce Members only, open to vendors, or locked and used only for emergency exit purposes, etc. If there are buildings where no electronic Information Resources are

located and where no Sensitive Information is maintained this should be noted in the Security Plan and such building(s) need not otherwise be addressed in the Security Plan.

A. General Rules

1. **Locking Doors.** Doors that are not used as entrances into a building must be locked or configured so that they can only be used to exit the building. Workforce Members shall not leave these doors unattended if at any time they are being kept open for a purpose.

2. **Entrances for Workforce Members Only**

   a. Workforce Members may enter and exit a building only via public entrances or entrances specifically designated for Workforce Members only.

   b. If Workforce Members are authorized to enter a building through entrances specifically designated for Workforce Members only, they may not permit non-Workforce Members to enter or leave a building through such entrances.

3. **Public Entrances**

   a. Public access to a building, to the extent possible, should be limited to entrances that lead to common areas within the building that can be monitored by appropriate staff.

   b. Public entrances should be well marked with signage. Hours of operation should be clearly noted.

4. **Vendors and Other Non-Workforce Members.** Vendors and other non-Workforce Member access to a building should be limited to entrances that can be monitored by appropriate staff.

IV. RESTRICTED AREAS

A. General Rule

1. **Identifying Restricted Areas**. A Security Plan shall identify the Restricted Areas at the DMH Location and indicate how access to such Restricted Areas is controlled. Examples of Restricted Areas include the following:

   - nursing/patient care stations;

- billing offices;
- contract offices;
- copiers/ fax/ printer rooms;
- mailrooms;
- medication rooms;
- storage closets;
- information services equipment rooms;
- an office with human resource records (Massperform, EPRS, disciplinary letters and/or investigations, etc.);
- administration offices;
- offices with Workstations;
- cubicles with Workstations;
- check-in-desks;
- security desks;
- business offices;
- records rooms/medical records rooms;
- personnel file storage;
- pharmacies;
- wire closets/computer labs; and
- patients care areas (i.e., inpatient units, shelters, and outpatient clinics),

2. **Controlling Access**. Access to Restricted Areas that cannot be controlled by locked doors shall be controlled by such other means as are reasonable given the type of space, such as gates, postings, around the clock coverage, surveillance cameras, etc. Where locked doors control access to Restricted Areas, such doors shall be locked when the areas are unattended. Only authorized Workforce Members shall receive keys to access such areas or otherwise be allowed to access such areas. (*See* Section IV.B., below.)

3. **Access by Non-Workforce Members**. If a vendor, member of the general public, or other non-Workforce Member needs to enter a Restricted Area, the non-Workforce Member must be escorted and monitored by a Workforce Member while in the Restricted Area.

4. **Data Centers.** Data centers (location of servers, switches, and routers) shall be secured by a combination of two or more of the following security features: guards; sign-in, multi-factor authentication for entry, access login, and video monitoring.

5. **Network Wire Closets**. Network wire closets (location of switches) must be located in areas where access can be

controlled, at a minimum, by door keys with restricted distribution.

6. **Computer Training Rooms.** Computer training rooms must be located in areas where access can be controlled, at a minimum, by door keys with restricted distribution. The DMH Office of Learning and Development must maintain centrally a current list of all computer training rooms located in DMH Locations. For each training room, the DMH Office of Learning and Development shall know how access to the training room can be gained (i.e., who maintains the keys, etc.)

7. **Environmental Controls.** Environmental controls must be appropriate for the electronic Information Resources located in a Restricted Area.

   A Security Plan shall address the need to protect all Information Resources in a Location against fire, water damage, and other environmental hazards, such as power disruption and extremes in temperature. The Person in Charge is responsible for working with staff in the Location (or Area) and the DMH Administration and Finance Division to ensure necessary resources are budgeted and procured.

B. Access Card/Keys

1. **Access Card/Key Control Plan.** As part of its Security Plan, each Location must have a written Access Card/Key Control Plan that describes the process for assigning, distributing, and collecting access cards/keys to doors of their Restricted Areas.

2. The Access Card/Key Control Plan must provide that access cards/keys and similar devices may be issued only:

   a. with the written approval of the Person in Charge or their designee;

   b. to Workforce Members who need them to perform their jobs; and

   c. a written record is kept of the access card(s)/key(s) or similar device(s) assigned to each Workforce Member.

   The Access Card/Key Control Plan must include a procedure for periodically updating or confirming the accuracy of the written record of what access cards/keys have been assigned to

Workforce Members. It must include provisions for timely changing of locks when access cards/keys to Restricted Areas are reported as missing or lost.

3. **Workforce Members' Responsibilities.** Workforce Members who are issued access cards/keys are responsible for:

   a. returning their access cards/keys to their DMH Supervisor, or the person designated by Person in Charge for the applicable Location to be responsible for such, when they are asked to do so, are transferred to another Location, stop working for DMH, or are placed on administrative leave, or are otherwise a "departing Workforce Member", as that term is defined in Chapter 4, Section III.B. (*See* also Section IX, below.)

   b. not allowing others to use their access cards/keys; and

   c. reporting lost and/or stolen access cards/keys to their DMH Supervisor, or personnel designated by the Person in Charge as soon as they become aware of such.

4. Access cards that are not also identification badges/keys must not have identifying information on them other than a return mail address.

C. Suspicious Activities

Workforce Members are to report immediately to their DMH Supervisor or campus security any unauthorized access, entry or suspicious activity they observe, such as an unknown person not wearing a DMH approved ID or visitor badge when such badges are required. (See Section V, below.)

V. IDENTIFICATION BADGES

A. Workforce Members

1. When at a DMH Location all Workforce Members shall wear a visibly displayed DMH issued photo identification badge, which includes sufficiently unique information to enable DMH to identify the Workforce Member, such as their name, job title, and/or work Location. All Facility Workforce Members, including students, who examine, observe or treat clients must wear an identification badge which readily discloses, at a minimum, the first name, licensure status, if any, and staff position of the

Workforce Member so examining, observing or treating a client. Workforce Members shall not alter their DMH issued identification badges. It is not sufficient for Workforce Members to have their badges on their person; they must be prominently displayed in a manner that makes them readily visible to others. It is the responsibility of management staff to ensure that Workforce Members comply with this requirement.

2. When a Workforce Member's assignment to a particular Location ends, or the Workforce Member's access to a particular Location is no longer authorized, they must return their identification badge to their DMH Supervisor, or the person designated by the Person in Charge for the applicable Location to be responsible for such.

B. Visitors' Badges

DMH recognizes that not all Locations are able to require all visitors to obtain and wear DMH visitor identification badges. This is, however, a goal DMH strives toward. To facilitate this the following rules must be complied with as are applicable to a Location:

1. **Currently using Visitor Badges**. If a Location currently issues badges to visitors and/or vendors, it may only cease such practice subject to the approval of the DMH ISO. The Person in Charge of the Location must notify the DMH ISO and explain why it is not reasonable to continue the practice.

2. **Currently not using Visitor Badges.** If a Location does not currently issue badges to visitors and/or vendors, the Location must indicate in its Security Plan why it is not practical or feasible to do so. If the Location previously issued visitor badges and then ceased, the Security Plan must include the date the change in practice was approved by the DMH ISO.

3. **Restricted Areas.** Regardless of whether the Location issues such badges, the Location must have in place a process for authenticating and logging a visitor's identification prior to giving the visitor access to Restricted Areas.

   The visitor logs shall contain:

   - the name and organization of the person visiting;
   - signature of the visitor;
   - form of identification;
   - date of access;

- time of entry and departure; and
- purpose of visit.

The Person in Charge or designee shall periodically review such visitor logs. The DMH ISO, or designee, may review the visitor logs at such times as determined by the DMH ISO.

4. **General Rules Regarding Visitor Badges**. If visitor badges are issued the following shall apply:

   a. Visitors shall be instructed to have their badges on their person at all times and the badges must be prominently displayed in a manner that makes them readily visible to others.

   b. The badges should have unique identifiers, such as a number, or an alphanumeric string. The badges must be signed out when entering and returned when exiting the Location by the visitor.

VI. MAINTENANCE RECORDS – PHYSICAL LOCATION SECURITY

A Security Plan must include procedures for documenting and managing the repairs and alterations to the physical security components of the DMH Location, including locks, doors, and other physical access control hardware. The documentation must capture:

- what repairs/alterations were made;
- the reason(s) for the repair/alterations;
- the dates they were made; and
- who made them.

The procedures shall also specify who at the Location is responsible for maintaining the documentation; and how the Location will ensure that before any repairs/alterations/new construction all physical security issues are addressed.

VII. WORKSTATIONS, PRINTERS, OTHER DEVICES, AND DIGITAL MEDIA

A. **Use of Personally Owned Devices is Prohibited**. Use of a personally owned device to access Information Resources is expressly prohibited. DMH Managers may permit exceptions for: 1) incidental or emergency situations or; 2) for interim use once a

Workforce Member has submitted a request for a Device and before the Device has been issued.

B. Safeguards Applicable to Workstations and Printers

Note: Except as noted below, the following applies to all Commonwealth (i.e., state-issued) Workstations and, if permitted to use a personally owned device (see Section IIV.A., above), personally owned/leased desktops, laptops, and similar computing devices (collectively "computers"), and all printers.

1. Workforce Members using personally owned computers must run anti-virus software, with the most up-to-date virus definitions, on the computer used for remote access at all times and must update this software from the vendor's web site regularly.

2. All computers must be password protected. Workforce Members must log off, lock or disconnect from the Network whenever leaving the immediate vicinity of any computer.

3. In placing a Workstation at a DMH Location, the following shall apply:

a. Workstations must be placed to minimize the possibility of unauthorized use and to protect against theft.

b. Workstations must be placed to minimize the possibility of unauthorized viewing of EPHI. When necessary, privacy filters/screens should be attached to monitors.

4. Local printers should be placed next to or near the Workstations or Workforce Members that use the printer. Multi-function networked printers should be placed in non-public areas only, with the exception of printers having the mailbox functionality to send documents to a secure mailbox on the printer for later printing by a Workforce Member with access to the secure mailbox, if such functionality is utilized. (*See* also Chapter 3, Section II.C., Printing and Copying PHI, of the DMH Privacy Handbook.)

5. All Commonwealth Workstations, monitors, and printers must be plugged into a surge protector. Care must be taken to not overload electrical outlets with too many devices.

6. When Commonwealth desktop computers are moved from one office to another the Workforce Member(s) must inform the EHS Support Services of such move. This ensures the inventory is kept current. (*See* also Section X, below.)

7. Commonwealth Workstations located at non-DMH Locations, such as remote working locations, court houses and other non-DMH Locations, shall be protected with security controls equivalent to those at a Location.

8. A Commonwealth Workstation at a Location using an ethernet cable to connect to the Network may be used by any Workforce Member authorized to access the Network in accordance with Chapter 4, Section II, Obtaining Access, of this Handbook; provided, however, that a DMH Manager may restrict the use of any Commonwealth Workstation and a Commonwealth Workstation in a Restricted Area may only be used with the prior approval of a DMH Manager responsible for that Restricted Area. No personally owned computers or any other personally owned devices may be used in a Restricted Area.

9. EPHI and other Sensitive Information shall be stored in a Network folder only and not in a local hard drive. If it is necessary to temporarily store EPHI on a Commonwealth Workstation, it must be transferred to the Network and deleted from such Workstation as soon as possible. At a minimum, this must be done weekly and prior to it being returned to EHS IT. (*See* Section IX. below.)

10. When a Workforce Member returns a Commonwealth laptop it must be sent to EHS IT for re-imaging.

    A Commonwealth laptop can be assigned to a Workforce Member only by EHS IT and only after EHS IT has received from the Workforce Member a signed Laptop Issuance Form.

11. Workforce Members will not change any configuration settings on Commonwealth computers without the permission of EHS Support Services, except those concerning screen resolutions.

C. Devices and Digital Media.

1. **Compliance with EHS Standards**. If a Workforce Member uses a device (state-issued or, if permitted, personally owned (*see* Section VII. A., above))and such device has wireless

access to the Network, it must comply with the EHS Mobile Device Policy/Agreement.

2. **Digital Media.** The use of Digital Media is expressly prohibited without prior authorization from a DMH Manager. In no event may removable or Digital Media devices be used to transfer PHI without express authorization. If authorized, DMH must provide an encrypted, password protected drive to be used only for the purpose of that specific job duty. When not in use, digital media must be stored securely at all times.

3. **Storage of Sensitive Information**. Workforce Members should not store EPHI or other Sensitive Information on a Device or Digital Media unless necessary to perform their job function and then only such EPHI as is necessary to perform the Workforce Member's job function may be temporarily stored in such Device or Digital Media. If it is necessary to temporarily store EPHI on a Device or Digital Media, it must be transferred to the Network and deleted from the Device or Digital Media as soon as possible. At a minimum, this must be done weekly and prior to it being returned to EHS IT. (*See* Section IX. below.)

4. **Safeguards applicable to all Devices and Digital Media**. Appropriate physical security measures must be taken to prevent access to and/or theft of Devices and Digital Media.

    a. When not in use Devices and Digital Media must be stored physically secured, e.g., locked in office, desk drawers, etc.

    b. During transportation Devices and Digital Media should remain under visual and/or physical control to the extent possible. If that is not possible, then appropriate safeguards must be taken to protect the Device, Digital Media, and removable components. To the extent possible, Devices and Digital Media should not be left unattended. It is the Workforce Member's responsibility to take all reasonable steps necessary to maintain control of their Devices and Digital Media in transit.

    c. All Devices must be password protected. Workforce Members will log off, lock or disconnect whenever leaving the immediate vicinity of any Device in use.

    d. Precautions should be taken to avoid the unauthorized viewing of EPHI or other Sensitive Information in public or common areas. Workforce Members are responsible to

ensure there is not unauthorized viewing of EPHI or Sensitive Information when Teleworking or otherwise working remotely.

e. Workforce Members shall not store Sensitive Information on unsecured non-digital media. All non-digital media (such as, paper) containing Sensitive Information must be locked in a filing cabinet (or other locked device) or secured within a locked room when not in use. Non-digital media shall not be left unsecured while unattended.

f. All Digital Media containing Sensitive Information that leaves the DMH environment must be marked on the Digital Media that it contains Sensitive Information. This may be done by marking the Digital Media as confidential, sensitive, or with some other similar marking or indication.

g. Workforce Members are responsible for securing their data and Devices while Teleworking, in transit to/from their assigned work Location, or otherwise working remotely.

VIII. REGULARLY DELETING AND/OR DISPOSING OF EPHI

Workforce Members shall take reasonable and appropriate steps to dispose of EPHI when it is no longer needed and has satisfied the period of retention under the Massachusetts Statewide Records Retention Schedule and DMH regulations, or the EPHI is a copy and is not subject to retention. If such EPHI is maintained on an electronic Information Resource, it shall be deleted using the procedures that are appropriate for deleting data from the particular electronic Information Resource. (*See* Sections IX and X, below and Chapter 3, Section II.K., Disposal of PHI, of the DMH Privacy Handbook.)

IX. WHEN A WORKFORCE MEMBER IS PERMANENTLY DONE UTILIZING A DMH ELECTRONIC INFORMATION RESOURCE THAT HAS BEEN ASSIGNED TO THEM

When a Workforce Member is permanently done using an electronic Information Resource that was assigned to them, the Workforce Member, or their DMH Supervisor, must contact EHS Support Services to return the resource to EHS IT or notify it that the resource is no longer in use. Prior to doing so, the Workforce Member, or their DMH Supervisor must follow the procedures set forth in this Section IX.

A. Ensure that All Commonwealth Records on the DMH Electronic Information Resource Are Transferred and Deleted

The Workforce Member, or their DMH Supervisor, must ensure that all Commonwealth records maintained on the electronic Information Resource are transferred to another electronic media for retention pursuant to the Massachusetts Statewide Records Retention Schedule and DMH regulations. After the Commonwealth records have been transferred to another electronic media, the records shall be deleted from the electronic Information Resource using the procedures for deleting information applicable to the particular electronic Information Resource.

B. Return the Electronic Information Resource to EHS IT

After ensuring that all Commonwealth records have been transferred to another electronic media and deleted, the Workforce Member, or their DMH Supervisor, must contact EHS Support Services to return the electronic Information Resource to EHS IT or otherwise follow instructions from EHS IT.

X. SPECIAL RULES FOR MOVING A NON-PORTABLE INFORMATION RESOURCE THAT STORES EPHI

A. DMH Location to Another DMH Location

Prior to moving a Non-Portable Information Resource, which stores or processes EPHI, from one DMH Location another; a back-up of the EPHI on such Information Resource, if any, shall be created. It shall be the responsibility of the Person in Charge of the original Location where the Non-Portable Information Resource is being moved from, or their designee, to contact EHS Support Services to arrange for this back-up. If appropriate, the Person in Charge shall have the information deleted prior to moving the Information Resource.

Prior to moving such equipment, the person responsible for maintaining the equipment will be notified of the move. Immediately following the move, the person responsible for maintaining the equipment will calibrate and/or run quality controls on the equipment prior to use.

B. DMH Location to a Non-DMH Location

Prior to returning a rented or leased electronic Information Resource that stores or processes EPHI to the owner or lessor, or

otherwise moving such Information Resource to a non-DMH Location (e.g., surplusing the Information Resource), the Person in Charge of the Location is responsible for ensuring that all EPHI is deleted from the Information Resource prior to it leaving the DMH Location. If appropriate, the Person in Charge shall have the information backed-up prior to it being deleted from the Information Resource.

XI. HELP AND MAINTENANCE

Workforce Members should not attempt to fix problems with a Workstation/Device themselves. Workforce Members shall contact the EHS Support Service and report a problem as soon as possible. When calling EHS Support Services, Users need to supply their name, Workstation/Device location, and Workstation/Device number.

If a Workforce Member encounters a problem with a Network printer, it is important that they notify the EHS Support Service so the problem can be corrected promptly.

XII. CITATIONS

Regulatory Reference	Facility Access Controls 45 CFR 164.310(a)(1) and (2) Workstation Use 45 CFR 164.310(b) Workstation Security 45 CFR 164.310(c) Facility Security Plan 45 CFR 164.310(a)(2)(ii) and (iii) Access Control and Validation 45 CFR 164.310(a)(2)(iii) Facility Maintenance Records 45 CFR 164.310(a)(2)(iv) Protection from Malicious Software 45 CFR 164.308(a)(5)(ii)B Encryption 45 CFR 164.312(a)(2)(iv) and (c)(1) Mass. General Laws c.111 § 70E

XIII. REFERENCED POLICIES AND PROCEDURES

Massachusetts Statewide Records Retention Schedule
EHS Mobile Device Policy/Agreement
DMH Privacy Handbook

XIV. ATTACHMENTS

Security Plan Form
Security Walk Through Job Aid