# CHAPTER 3
# PHYSICAL AND TECHNICAL SAFEGUARDS

## I. GENERAL RULE

The purpose of this Chapter is to establish physical and technical safeguards that must be followed when Protected Health Information (PHI) is being used or disclosed. DMH has established administrative safeguards that are designed to protect the integrity, security, and confidentiality of PHI created and/or maintained by DMH.

**Confidentiality** is the assurance that information is shared only among authorized persons or organizations.

**Integrity** is the assurance that information is not changed unless an alteration is known, required, documented, validated, and approved.

**Availability** is the assurance that systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them, under both routine and emergency circumstances.

Nothing in this Chapter specifically authorizes the use or disclosure of PHI. Included among DMH's safeguards are procedures establishing when PHI may be used and disclosed by Workforce Members. (*See* Chapter 6, Uses and Disclosures of Protected Health Information, and Chapter 8, Authorization for Use and Disclosure of Protected Health Information.)

The requirements of the DMH Information Security Handbook must also be followed. If at any time a DMH Workforce Member believes a discrepancy exists between the DMH Information Security Handbook and this DMH Privacy Handbook, guidance must be sought from the DMH Privacy Officer. The DMH Information Security Handbook can be accessed on the DMH Intranet web site.

## II. SPECIFIC REQUIREMENTS AND PROCEDURES

### A. Physical Workspace

1. **Information Resources.** All Information Resources used by a Workforce Member must meet the requirements of and be used in accordance with the DMH Information Security Handbook.

2. **Paper, and/or Other Hard Copy PHI.** When using PHI that is in hard copy, efforts shall be made to avoid inadvertent disclosures to others (e.g., viewing it privately). PHI shall not be left unattended in plain view in any area accessible to persons not authorized to view the PHI, including on printers, copiers, fax machines, scanners, or other office

devices. Such PHI shall be kept, if possible, in a locked office and/or filing cabinet and/or in another secured location when not in use. *See* also Section II.I. on Storage.

3. **Voice Messages.**

   a. **Receipt of PHI.** If voicemail and/or other voice messages are used to receive PHI, access to the messages must be available only through the use of passwords. Unique passwords must be used. The password may not be set to default and the last four digits of the telephone number may not be used. Passwords must be changed whenever it is learned that they are no longer confidential.

   b. **Playing Voice Messages and Communicating PHI Via Voice Messages**. Care must be taken in playing and leaving voicemails or other voice messages that contain PHI to ensure confidentiality. Workforce Members must be aware of their environment and think before playing voice messages using the speaker system. Additionally, voice messages containing PHI should not be left on an answering machine or any other Device unless the Workforce Member knows that access to the Device is limited in such a way to ensure confidentiality. Workforce Members should not assume that an answering machine or similar Device is secure and confidential.

## B. Verbal Communications and Telephone Use

1. **General.** DMH policies and procedures relating to PHI apply to verbal communications as well as to electronic and/or paper communications. When a Workforce Member communicates PHI verbally, they must be aware of their environment (e.g., whether other individuals are present that can overhear their conversation) and take appropriate actions to minimize the chance of inadvertent disclosures to others. The following shall be considered:

   **a.** Talking in the most private setting possible.

   **b.** Keeping the volume level low enough so as not to be overheard.

   **c.** Using a code number, or similar mechanism, to identify a specific individual, if there is no way to prevent being overheard. (Use of an individual's initials or other information derived from the individual's identifying information is not an acceptable code. *See* Chapter 6, Section VIII.A.2.)

   Although all reasonable care shall be taken to minimize the chance of individuals inadvertently overhearing PHI, this requirement is not

intended to prevent Health Care Providers from talking to each other and/or to the individuals whom they are treating. In some situations (e.g., a busy nursing station) it may be necessary for Health Care Providers to speak loudly to ensure appropriate treatment. This is permissible even if there is a chance that individuals other than Health Care Providers or the individual being treated may be overheard. Similarly, it is expected that health care staff verbally may coordinate services at facility nursing stations; that Health Care Providers will discuss treatment with a patient or another Health Care Provider in a joint treatment area, and that Health Care Providers will discuss a patient's condition during training rounds, etc.

2. **Postings.** All Locations should consider posting signs in elevators and in other public places reminding Workforce Members of the need to minimize conversation including PHI in such places.

3. **Accounting**. Disclosures by verbal communication may be subject to an accounting pursuant to the Chapter 12, Right to an Accounting of Certain Disclosures of Protected Health Information.

4. **Use of Speaker Phones.** Workforce Members shall be particularly cautious when using a speaker phone. Action should be taken to minimize the possibility of the conversation being overheard (e.g., closing of the door, reducing speaker volume, refraining from use where practical.)

5. **Use of Wireless Telecommunication Devices**. Wireless, cellular and cordless telephones shall be used for communicating PHI only if no other means of communicating is available and the communication is necessary at the time to complete a work-related function. Communication of PHI should be done orally or through a secure electronic system, such as using “Secure:” email and secure file transfer protocol. (*See* Sections II.D., below.). **Texting of PHI between Workforce Members or to others is prohibited**.

## C. Printing and Copying PHI

1. **Printing and Copying by Workforce Members.** Workforce Members may not print or copy PHI unless necessary to perform their job functions. In printing or copying PHI, the following protocols shall be followed:

   **a.** the printer or copier used must be in a secure area; or

**b.** the printer or copier used is equipped with a mailbox or secured print (these will hold the job until the owner enters a PIN at the printer); or

**c.** if the printer or copier used is in a public or shared location, then the copies shall not be left unattended at the printer or copier.

Wherever practical, printing and copying of PHI should occur on devices in a secured area or with mailbox/secured print function.

**2. Location of Printers and Copiers**

**a.** To the extent feasible, printers and copiers used for printing or copying of PHI are to be in secured locations, where the setup is designed to minimize unauthorized access.

**b.** If a printer or copier is placed in a public location, a sign must be posted above it reminding Workforce Members to use the machine's mailbox or secured print, if any, or, if none, to retrieve printed or copied documents immediately. The following language is recommended for such sign: "Do not leave Protected Health Information (PHI) unattended on this device."

**3. Repairs**

All printers or copiers that are to be repaired must have the queue stopped and purged to prevent unauthorized individuals, such as a repair person, from viewing PHI.

## D. Electronic Transmissions; File Transfer Protocol and Electronic Mail

DMH has specific requirements regarding the use of electronic transmissions including PHI. These requirements are set forth in Chapter 5, Section IV.A. of the DMH Information Security Handbook regarding use of the Commonwealth Secure File Transfer Solution Protocol and Chapter 7 of the DMH Information Security Handbook, regarding the use of Electronic Mail, including, without limitation, the requirement to include the DMH Confidentiality Notice in all emails containing PHI and the proper use of encrypted ("Secure:") email. (*See* also DMH Procedures for Transmitting Protected Health Information Between DMH Locations.)

## E. Fax Transmittal of PHI

The following procedures shall be followed with regard to fax machines used to transmit or receive PHI and in transmitting and receiving PHI by

fax. (*See* also DMH Procedures for Transmitting Protected Health Information Between DMH Locations.)

1. **Location of Fax Machines.** Fax machines used to communicate PHI are to be in secured locations, where the setup is designed to minimize unauthorized access.

2. **Sending PHI.** When sending a fax containing PHI, the following protocols shall be followed.

    a. **Cover Page**. The cover page accompanying the fax must include a confidentiality notice approved by the DMH Privacy Officer. *See* attachment at the end of this Chapter labeled "Fax Covered Sheet" for language that has been approved. In addition, the cover page must specify the name of the intended recipient, their telephone, and fax numbers, and the name, address, and telephone number of the sender. The cover page should not contain PHI/PI.

    b. **Verifying Destination.** Reasonable efforts shall be made to ensure that the fax is sent both to the proper recipient and the correct destination. This shall include doing the following:

        i. Verifying that the recipient will be available to receive the faxed PHI (i.e., call the recipient to confirm they will attend receipt or the fax machine is in a secure location).

        ii. Preprogramming frequently used numbers into the machine to prevent misdialing errors.

        iii. Periodically and/or randomly checking all speed-dial numbers to ensure their currency and validity.

        iv. Periodically reminding those who are frequent recipients of PHI to notify DMH if their fax number changes.

        v. For new recipients, verifying the fax number by telephone and/or by requesting a fax or email from the intended recipient with the recipient's fax number.

    c. **Security.** PHI shall not be left unattended at the fax machine. The memory feature of a fax machine shall not be used unless the Workforce Member remains in attendance at the fax machine until confirmation or receipt is received or the fax job is cancelled.

**d. Confirmation.** Reasonable efforts shall be made to ensure that the fax was sent to the correct destination, which may include review fax transmission receipts and/or telephone confirmation of receipt.

3. **Misdirected Faxes.** If the intended recipient does not receive a fax because of a misdial, the internal logging system of the fax machine shall be reviewed to obtain the misdialed number. If possible, a telephone call should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed. If the recipient cannot be reached by telephone, a fax should be sent to the recipient asking that the entire content of the misdirected fax be destroyed and that a call confirming the same be made to the sender. Misdirected faxes containing PHI shall be reported to the Person in Charge or the applicable DMH Privacy Coordinator, so that they can determine if further actions are needed, including, but not limited to, recording the misdirected fax in the accounting of disclosures. (*See* Chapter 12, Right to an Accounting of Certain Disclosures of Protected Health Information).

4. **Receiving PHI.** Each Division or unit that has a fax machine used to receive PHI is responsible for developing procedures for ensuring that incoming faxes are properly handled in compliance with this Handbook. The procedures, at a minimum, shall include:

   **a.** Regular checks of the fax machine for incoming faxes so they are removed promptly and delivered to the named recipient.

   **b.** The destruction of PHI and/or the following of sender's instructions for PHI faxed in error. Additionally, the sender shall be notified immediately of any receipt of PHI in error.

   **c.** Managing PHI received as confidential in accordance with this Handbook (e.g., distributing faxes in sealed envelopes).

## F. Physical Transmission (by hand, by courier, by courier service (such as FedEx or UPS), by mail, or by any other physical means)

If PHI is to be transported by hand, mail or courier, the procedures in this Section II.F. must be followed. (*See* also DMH Procedures for Transmitting Protected Health Information Between DMH Locations.)

1. Enclose the PHI in a sealed envelope with the receiver's name and address on it and clearly legible. The envelope must be marked "CONFIDENTIAL." After the content is placed in the envelope, it must be double checked to confirm the address of the envelope matches the

address of the intended recipient before the envelope is sealed. The envelope must also have the sender's name and return address on it.

2. If sending by courier service or certified or registered mail, the tracking number should be kept and used when necessary.

3. If a Workforce Member becomes aware that PHI was not delivered or was inadvertently misdelivered, the Workforce Member must notify the Person in Charge or the applicable DMH Privacy Coordinator immediately so that actions may be taken to recover the PHI. Similarly, if a Workforce Member receives PHI by mistake, they shall make an effort to contact the sender or, if that is not possible, the individual about whom the PHI is received, to return the PHI. If the PHI cannot be returned, it should be destroyed. Mis-deliveries may be subject to an accounting pursuant to Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information.

## G. Access to and Use of Information Resources

DMH has specific requirements regarding access to Information Resources. These requirements are set forth in Chapter 4 of the DMH Information Security Handbook.

DMH has specific requirements regarding the use of Information Resources. These requirements are set forth in Chapter 5 of the DMH Information Security Handbook.

## H. Use of Passwords

1. A Workforce Member is responsible for the use of any Information Resource under their login User ID and password.

2. Workforce Members may not share passwords or User IDs with any other individual and may not allow any other individual to access DMH systems under their User ID. Workforce Members may not access DMH systems under any User ID other than their own.

3. EHS Support Services is able to provide technical assistance to users without ever having to ask users to reveal their passwords.

4. Workforce Members may not store written passwords anywhere near the Devices where the passwords are used.

5. If a Workforce Member suspects that their password(s) is known to another, the Workforce Member must change their password(s) to prevent unauthorized access. The Workforce Member may need to

contact EHS Support Services for assistance.

## I. Storage of PHI

All storage systems used by DMH for information that contains PHI shall be designed and implemented to ensure the safety, security, and integrity of the PHI. The storage method selected shall be dependent on the security of the area and the volume of PHI to be stored. (*See* also Chapter 6, Physical and Technical Security, of the DMH Information Security Handbook.)

1. **Paper PHI.**

   a. **Onsite Storage.** If the Location responsible for maintaining records containing PHI is shared with other divisions, units, etc. not responsible for maintaining such records, the shelves or file cabinets containing PHI must be lockable and kept locked whenever records staff are not in attendance. If PHI records are retained in a lockable office that is not shared with other staff or in a separate locked filed room, open shelf filing is acceptable if the office or file room is locked when staff is not in attendance. Storage area environments should not cause damage to the records and should meet accreditation and safety standards.

   b. **Offsite Storage.** Offsite storage shall meet the above standards, be approved by the DMH Privacy Officer and, as applicable, and have a signed Business Associates agreement with DMH. A record tracking system must be in place to identify when a record has been removed, who took the record, and where it is located.

   c. **Microfilm.** When a microfilm copy of the original paper record has been produced, it may be used as a permanent record of the original if permitted by the Secretary of State's Office. Duplicate microfilmed records shall be kept by the DMH Location that created the original with suitable equipment for viewing. The original microfilm shall be maintained offsite in a fireproof vault or, if the original microfilmed record has a permanent retention period, it should be transferred to the State Archives. A log shall be maintained of all microfilmed records and cross-indexed, or otherwise linked with a common identifier.

2. **Electronic PHI.** Electronic storage of records containing PHI must have a permanent retrievable capability.

3. **Medical Devices.** PHI stored in medical devices (e.g., EKG machines) must be used and secured in a manner similar to paper PHI and disposed of in a manner similar to electronic PHI.

4. **Retention.** Records containing PHI must be retained in accordance with the applicable Statewide Record Retention Schedule and DMH regulations.

## J. Offsite Use of PHI

Workforce Members may take and/or use PHI away from a DMH Location only if necessary to carry out their duties. If PHI is removed from a DMH Location, then the following procedures shall be followed:

1. Only that amount of PHI that is necessary to carry out the required job function shall be removed.

2. The original PHI shall not be removed unless it is necessary to carry out the required job function.

3. If PHI is lost or stolen, the Workforce Member's Person in Charge and the applicable DMH Privacy Coordinator shall be notified as soon as possible.

4. PHI that is not in the Workforce Member's direct possession shall be kept in a secured manner to protect such PHI from being accessed intentionally or unintentionally.

5. Any documentation or equipment, such as laptops, smartphones, pagers, beepers, etc., that contain PHI shall be secured from access by those without authorization. The Workforce Members shall take such precautions at their place of residence as well as at all other locations.

6. All equipment, briefcases, etc., shall be labeled so that they can be returned to the proper location if lost or misplaced.

## K. Disposal of PHI.

Dispositioning of PHI in paper or electronic format shall be carried out pursuant to the Massachusetts Statewide Records Retention Schedule, the Massachusetts Records Conservation Board procedures, DMH regulations, and these procedures. Generally, when the disposing of PHI is permitted by the Massachusetts Record Retention Schedule, the original version of the PHI can only be disposed of if DMH has received written the approval of the Massachusetts Records Conservation Board to

do so (see https://www.sec.state.ma.us/divisions/archives/records-management/agency-records.htm). When disposing of records containing PHI, the method used must ensure that there is no possibility of the reconstruction of PHI.

1. **Paper Records**. If PHI is in paper form, it can only be disposed of by placing it in **locked** shredding bins. Shredding bins must be kept in areas that can be locked and are not accessible to the general public.

2. **Electronic Information Resources.**

   **a.** DMH has specific requirements regarding the return of Commonwealth owned electronic Information Resources when DMH is done utilizing them. These requirements are set forth in Chapter 6, Section IX. of the DMH Information Security Handbook.

   **b.** DMH has specific requirements regarding the return of leased electronic Information Resources that store or process electronic PHI. These requirements are set forth in Chapter 6, Section X.B. of the DMH Information Security Handbook.

3. **Third Parties Hired to Dispose of PHI**. If a third party is hired to dispose of documents and/or equipment that may contain PHI, they must have as part of their DMH contract a Business Associate Agreement. *See* Chapter 7, Section I.

4. **Documentation.** A record of the destruction of PHI maintained in a DMH Designated Record Set must be retained. The record must include: date of destruction; method of destruction; description of records; inclusive date of records; statement that the records were destroyed in the normal course of business; the signatures of the individual supervising and witnessing the destruction. Destruction documentation shall be retained permanently by the applicable DMH Designated Record Set Contact Person.

## L. Other Policies, Procedures, and Guidance.

Workforce Members are responsible for following all other policies, procedures, guidance, guidelines, and the like, applicable to DMH that may be issued by the Commonwealth, including by DMH, from time to time. (*See* Section III for examples.)

## III. LEGAL REFERENCES; ATTACHMENTS; RELATED POLICIES AND PROCEDURES

### A. Legal References.

Physical Safeguards 45 CFR 164.530
Destruction 164.308(a)(5)
Training 164.530(b)
Record Retention 104 CMR 27.16

### B. Attachments.

Fax Transmission Cover Sheet – Confidentiality Notice

### C. Related Policies and Procedures.

DMH Security Handbook
EOHHS Acceptable Use Policy
Massachusetts Statewide Records Retention Schedule
Procedures for Transmitting Protected Health Information Between DMH Locations
Procedure for Use of DMH Owned Electronic Devices
Telehealth, Teleconference, and Texting Procedure
Telework Policy
Telework Acknowledgement

## Fax Transmission Cover Sheet

### Confidentiality Notice:

The documents accompanying this facsimile transmission contain information from the Department of Mental Health which may be CONFIDENTIAL AND/OR PRIVILEGED. It may also contain PROTECTED HEALTH INFORMATION (PHI), which is personal and sensitive information related to a person's health care. If this facsimile contains PHI, it is being sent to you after appropriate authorization from the person has been obtained or under circumstances that do not require the person's authorization.

The information is intended for the use of the individual or entity named on this transmittal sheet. If you are not the intended recipient, or the employee or agent responsible for delivering it to the intended recipient, the disclosure, copying or distribution of this information is strictly prohibited. If you have received this facsimile in error, please notify the sender by telephone immediately. Thank you.