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. Nothing in this Chapter specifically authorizes the use or disclosure of PHI. DMH has established administrative safeguards that are designed to protect the integrity, security and confidentiality of PHI created and/or maintained by DMH. Included among those safeguards are guidelines establishing when PHI may be used and disclosed by DMH Workforce Members. (See Chapter 6, Uses and Disclosures of Protected Health Information and Chapter 8, Authorization for Use and Disclosure of Protected Health Information.)

DMH has additional policies and procedures that govern the use of electronic devices that are not related directly to PHI. DMH Workforce Members are responsible for knowing and carrying out these policies and procedures. These policies and procedures can be accessed on the DMH Intranet web site.

II. SPECIFIC REQUIREMENTS AND DMH PROCEDURES

A. Workstations

1. **Computers.** If a computer is used by a DMH Workforce Member to gain access to or enter PHI, the following protocols must be followed:

    a. To the extent possible, a workstation should be arranged so that neither the monitor nor the keyboard can be viewed accidentally by another person walking by the workstation.

    b. A computer must not be unattended unless the applicable DMH Workforce Member logs out or the "lock workstation" option is activated which requires a password to be entered to reactivate the computer.

    c. When leaving the office for the day, Workforce Members must log off their computers.

    d. Workforce Members may not have their e-mails automatically forwarded to any address outside of the MAGnet system (i.e., to any address that ends in other than "state.ma.us").

e. A password must be used to access the computer. See Section II. H. for rules on Passwords.

2. **Paper, Floppy Disk 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, laptops 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. See also Section II. I. on Storage.

3. **Verbal Communications and Telephone Use.** See Section II. D. on Verbal Communications.

4. **Voice Mail.**

   a. **Receipt of PHI.** If voicemail and/or an answering machine 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 no longer are confidential. Voicemail messages shall not be played over the speaker system and answering machine volume shall be turned down so that messages may not be overheard.

   b. **Communicating PHI.** No PHI shall be communicated to voice mail or to an answering machine unless it is an emergency.

B Printing and Copying PHI

DMH Workforce Members may not print or copy PHI unless necessary to perform their job functions. In printing or copying PHI, the following protocols should be followed:

1. Printers and copiers used for printing or copying of PHI should be in a secure location. If a printer is located in a public access area, PHI shall not be printed on it unless the printer is equipped with a mailbox or secured print. This holds the job until the owner enters a PIN at the printer. The job owner must stay at the printer while the job prints.

2. Printed documents containing PHI never must be left unattended on or by a printer or copier.

3. Unless they are equipped with a mailbox or secured print, all printers or copiers located in public access areas must have a sign posted above them reminding people that no PHI may be printed there.

4. 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.

5. PHI sent to a shared printer should be promptly removed.

C. 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.

1. Location of Fax Machines. Fax machines used to communicate PHI shall not be located in areas accessible to the general public. To the extent possible, they should be located in areas that allow access only to those who require 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. At a minimum, this notice shall include instructions for the recipient regarding actions to be taken if the fax has been misdirected. Included at the end of this Chapter is an approved confidentiality notice. In addition, the cover page must specify the name of the intended recipient, his/her telephone and fax numbers, and the address and telephone number of the sender. The cover page must not contain PHI.

b. **Stamped Confidential.** Documents containing PHI that are faxed should be stamped "CONFIDENTIAL."

c. **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.

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 e-mail from the intended recipient with the recipient's fax number.

vi. Confirming receipt either by the fax machine or by telephone.

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

e. **Documentation.** Retain all fax cover sheets, together with the copies of the information faxed and fax activity confirmation sheets from the recipient. Disclosures by fax may be subject to an accounting pursuant to the Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information.

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 are to be recorded in the audit trail of disclosures of PHI in accordance with the Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information, and thus shall be noted in the appropriate tracking system. Misdirected faxes containing PHI shall be reported to one's supervisor and to the DMH Privacy Officer.

If a DMH Workforce Member receives a misdirected fax from another DMH Workforce Member or a non-DMH individual or entity and the fax contains PHI, the Workforce Member shall attempt to contact the sender to notify him/her of the error. If the sender does not retrieve the PHI, it should be destroyed.

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 the DMH Privacy Handbook. The procedures, at a minimum, shall include:

   a. Regular checks of the fax machine for incoming faxes so that 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).

D. Verbal Communications

1. **General.** DMH policies and procedures relating to PHI apply to verbal communications as well as to electronic and/or paper communications. When a DMH Workforce Member communicates PHI verbally, he/she must be aware of his/her 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.

   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 Provider in a joint treatment area, and that Health Care Providers will discuss a patient's condition during training rounds, etc.

2. **Postings.** Central, Area, Site offices, facilities and programs 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. **Audit Trail**. Disclosures by verbal communication may be subject to an accounting pursuant to the Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information .

E. Use of Electronic Mail (E-Mail)

DMH Workforce Members may not e-mail PHI unless necessary to perform their job functions or with special written permission from a supervisor. In e-mailing PHI, the following protocols must be followed:

1. **State.Ma.Us**. PHI may be sent by e-mail if (a) the receiver's address ends in "state.ma.us" and (b) the e-mail is sent from an address that also ends in "state.ma.us".

2. **To Others Addresses.** PHI may be sent by e-mail to an address that does not end with "state.ma.us" only if the Commonwealth of Massachusetts Secure File and Email Delivery System (SFED) is used or the DMH Privacy Officer otherwise approves the email.

   The following procedures must be followed to use the Commonwealth of Massachusetts Secure File and Email Delivery System (SFED):

   a. Send the SFED Notification Memorandum: Prior to using the SFED System to send an e-mail to a person for the first time, the DMH workforce member must inform the intended recipient of the system by sending the *SFED Notification Memorandum*. This will tell the recipient what to do when they get a notice that they have a SFED e-mail. The SFED Notification Memorandum can be found on the DMH Intranet web site's Privacy page, which is accessed by selecting the "Get HIPAA" icon on the DMH Intranet Home Page.

   b. Establish an SFED account for the recipient: To establish a new SFED account, a DMH workforce member must send an e-mail with the word **Secure:** (NOTE THE COLON) in the subject line to the individual's e-mail address. This only works if the email is sent from a Department computer that is on the state e-mail system. An account remains established after this is done.

   c. To use the SFED system for an established user: Once an account is established for an individual, any workforce member may use the account to send PHI to the individual. To do this the workforce

member must use a DMH computer on the state e-mail system and type the word **Secure:** (NOTE THE COLON) in the subject line, addressing it to the intended recipient's regular e-mail address.. The placement of **Secure:** in the subject line tells the network that the SFED system is being used.

Because state e-mail address are already behind the state firewall and therefore secure, DMH workforce members who have a state e-mail address are not to create SFED accounts for themselves.

3. **Procedures.** In using e-mail to send PHI, the following procedures shall be followed:

   a Caution should be exercised if using the e-mail Global Address List (GAL). When using GAL, do not assume that a name appearing in it ends in "state.ma.us." Many of these names are actually Internet e-mail addresses that have been added to the GAL to provide a convenient way to send mail to contractors, vendors, business partners and other external entities.

   b. The e-mail must include the following Confidentiality Notice, name of the sender and the sender's direct telephone number:

      Confidentiality Notice: Protected Health Information from the Massachusetts Department of Mental Health

      Protected Health Information is personal and sensitive information related to a person's health care. It is being e-mailed to you after appropriate authorization from the person or under circumstances that do not require the person's authorization.

      If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, the disclosure, copying or distribution of this information is Strictly Prohibited**.** If you have received this message by error, please notify the sender immediately.

      Important Warning: This message is intended only for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law.

   c. Reasonable precautions must be taken to ensure that e-mails are directed to the right person and destination, (e.g., by double-

checking the addressee when there are multiple people on the GAL with the same first or last name, or even the same last name).

d. Discreet subject headers shall be used, such as "Personal and Confidential Communications."

e. To the extent possible, e-mails containing PHI shall be flagged in the system to allow for confirmation of receipt.

f. Misdirected e-mails. If a DMH Workforce Member becomes aware that he/she misdirected an e-mail, a telephone call should be made to the recipient requesting that the entire content of the misdirected e-mail should be deleted from his/her system. If the recipient cannot be reached by telephone, another e-mail should be sent with such instructions and asking the recipient to confirm the deletion of the information.

If a DMH Workforce Member receives a misdirected e-mail from another DMH Workforce Member or a non-DMH individual or entity and the e-mail contains PHI, the Workforce Member shall attempt to contact the sender by telephone if possible, or if that is not possible, by e-mail to notify him/her of the error. The misdirected email should be double deleted.

4. Documentation. Disclosures by e-mails may be subject to an accounting pursuant to the Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information.

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. should be followed. If the PHI to be sent is very sensitive, a DMH Worker should consider sending the PHI by a method that would allow tracking.

1. The PHI should be enclosed in a sealed envelope with the receiver's name on it. The envelope should be marked "CONFIDENTIAL."

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

3. If a DMH Workforce Member becomes aware that PHI was not delivered or was inadvertently misdelivered, the Workforce Member

must notify his/her supervisor and the DMH Privacy Officer immediately so that actions may be taken to recover the PHI. Similarly, if a DMH Workforce Member receives PHI by mistake, he/she 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.

4. Disclosures by mail, courier, etc. may be subject to an accounting pursuant to the Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information.

G. Access to DMH Electronic Data Systems

Access to a DMH electronic data system containing PHI must be approved in writing by the DMH Workforce Member's supervisor or appointing authority. Upon termination of employment or of DMH Workforce Member status, the supervisor must notify DMH AIT to terminate the network account and the Workforce Member's access to various electronic data systems.

H. Use of Passwords

1. DMH Workforce Members must adhere to the password guidelines contained in the DMH Policy (DMH-AIT-STD99-1). This policy is posted on DMH's Intranet web site.

2. DMH Workforce Members may not share passwords or User IDs with any other individual. DMH AIT staff is able to provide technical assistance to users without ever having to ask users to reveal their passwords.

3. DMH Workforce Members may not store written passwords anywhere near the devices where the passwords are used.

4. DMH Workforce Members may not access DMH systems under any User ID other than their own, and may not allow any other user to access DMH systems under their User ID.

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.

1. Paper PHI.

a. **On Site Storage.** If the office 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 environment should not cause damage to the records and should meet accreditation and safety standards.

b. **Off- Site Storage.** Off- site 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. Duplicate microfilmed records shall be kept by the DMH locale that created the original with suitable equipment for viewing and the original microfilm shall be maintained off-site in a fireproof vault. A log shall be maintained of all microfilmed records and cross-indexed, or otherwise linked with a common identifier**.** (See 104 CMR 27.17 for special rules for microfilming facility records.)

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 the 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 DMH record disposal schedules.

J. Off-Site Use of PHI

DMH 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 DMH Workforce Member's supervisor and the DMH Privacy Officer shall be notified as soon as possible.

4. PHI that is not in the DMH 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, pagers, beepers, palm pilots, 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, brief cases, etc., shall be labeled so that they can be returned to the proper location if lost or misplaced.

K. Use of Portable Electric Devices

Portable Electronic Devices shall be used for creating or maintaining PHI only if the following criteria and procedures are met.

1. **Laptops.** The DMH AIT Department must issue all laptops used for DMH business. DMH AIT Departments will configure the laptop to include both a power-on and a BIOS/CMOS setup password. They also will encrypt local personal user files that may contain PHI. When connected to the DMH network, all DMH workstation policies take effect. PHI should not be stored on a DMH laptop if it is possible. If it is necessary to temporarily store PHI on a laptop, it must be transferred to the DMH network and deleted from the laptop as soon as possible. However, at a minimum, it must be done prior to the laptop being re-assigned to another DMH Workforce Member. When a laptop that has been assigned to a DMH Workforce Member is returned to the AIT Department, the laptop must be re-imaged before it is assigned to another DMH Workforce Member.

2. **Other Devices.** If DMH Workforce Members use other portable electronic devices, e.g., palm pilots, they must be password-protected devices. Only such PHI as is necessary shall be retained in such devices and, if possible, codes etc., shall be used to prevent wrongful disclosure of PHI. No generic logon may be used on the equipment. The assigned user must have credentials or a local logon account stored on the equipment.

3. **General Use.** Portable electronic devices shall not be used in locations where it is possible for unauthorized individuals to view PHI and when not in use, such devices must be secured from unauthorized access.

4. **Use of PHI Other than at A DMH Location.** If such laptops or other electronic devices are used at other than DMH locations to create and/or to maintain PHI, then the rules of Section II. J. apply. Under no circumstances shall any such device be left unattended in an unsecured area.

L. 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.

M. Remote DMH Data Network Access

DMH Workforce Members requiring remote access (from beyond the MAGnet firewall) to DMH's data network and systems, and who have access to PHI will be authorized only to use "service-based" Virtual Private Networking (VPN) technology as their remote access methodology. VPN is the only technology suited for PHI due to its incorporation of Triple-DES, IPSec encryption, and is the most secure RA method currently available to the Commonwealth. If a DMH Workforce Member otherwise has remote access, he/she shall not use it to communicate PHI. Use of VPN will be limited as follows:

1. VPN machines will be DMH-engineered and DMH-issued and VPN will not be enabled on equipment not owned by DMH. Use of this approach and provisions will allow DMH to ensure that the equipment has been installed and configured according to DMH standards and controlled through DMH authentication and policy enforcement.

2. VPN enabled equipment also will include power-up and BIOS/CMOS setup password protection, as well as a data encryption solution for protection against unauthorized use due to theft.

3. DMH Workforce Members may have access through VPN to all systems, applications, and databases to which they have access in their DMH offices or would have access in their DMH offices were they working at that location.

4. Business Associates may have access through VPN to all databases to which they need access for the purpose of fulfilling their contractual obligations to DMH

5. While using VPN, the user is subject to all DMH privacy policies and procedures.

N. Electronic Data Interchange (EDI) Including by File Transfer Protocol (FTP)

PHI exchanged via EDI or FTP must be done only by approved AIT DMH Workforce Members.

O. Transporting Tape and Other Backup Media with PHI

When tapes or other backup media containing PHI are transported, the following procedures shall be followed:

1. When tapes from the backups of DMH Data servers containing PHI are transported to another location, the tapes need to be transported in a secure fire resistant locking courier bag.

2. Keys for the courier bag must remain at the server room and the location where the media is stored. The individual transporting the media must not have the key.

3. If a DMH Workforce Member becomes aware that PHI was not delivered or was misdelivered inadvertently, the Workforce Member must notify his/her or supervisor and the DMH Privacy Officer immediately so that actions may be taken to recover the PHI.

P. Disposing of Electronic or Paper-Based PHI. Destruction of PHI in paper or electronic format shall be carried out pursuant to DMH Regulations and Disposal Schedules. Records approved for destruction must be destroyed so that there is no possibility of the reconstruction of PHI.

1. **Paper Records**. If PHI is in paper form, it can only be disposed by either shredding it or placing it in locked recycling bins. Paper to be shredded must be kept in a secure location.
2. **Disk or Cartridge**. If PHI is on a floppy disk, hard disk, tape cartridge, audio tape, video tape, round reel, compact disk (CD), digital video disk (DVD) or any other type of electronic/magnetic hard media, it must be delivered to an AIT Workforce Member for proper destruction. When electronic records or computerized data are destroyed, they must be non-retrievable permanently and irreversibly.
3. **Hard Drives.** Hard drives that have failed and need to be replaced cannot be released to the hardware maintenance vendor, but must stay

in the control of DMH until they can be destroyed physically by AIT staff.

4. **Laptops and Desk Tops.** When disposing of older, obsolete desktops and laptops, the LAN staff must ensure the erasure of all data from hard drives using the standard DMH data wiping software (i.e., Autoclave v0.3). This should be done before initiation of the Commonwealth's standard procedure for disposal of surplus equipment. Surplus hard drives that are not currently installed in a machine should be wiped clean as well. If that cannot be done, the drive must be physically destroyed to render it unusable (e.g., use a power tool and drill a number of holes through the device).

   Maintaining the confidentiality of the PHI data on the removed hardware is the responsibility of the person removing the equipment.

5. **Medical Devices.** When disposing of PHI contained in a medical device, the PHI shall be disposed of in a manner consistent with the type of electronic PHI storage used by the device.

6. **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.

III. LEGAL REFERENCE AND ATTACHMENT

HIPPA 45 CFR 164.530
104 CMR 27.17
Fax Transmission Cover Sheet – Confidentiality Notice