



## SAFEGUARDING AND STORING PHI PROTOCOL

### OVERVIEW

- DMHSA works to ensure, to the extent possible, that protected health information (PHI) is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other federal regulations governing confidentiality and privacy of health information. The following protocol is designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that is, or will be, contained in a consumer's mental health record.
- At the same time, the Department recognizes that easy access to all or part of a consumer's mental health record by DMHSA professionals involved in a consumer's care (nurses, psychiatrists, social workers, psychologist, therapists, and other professionals) is essential to ensure the efficient quality delivery of treatment and services.
- HIPAA requires covered entities to have appropriate administrative, technical, and physical safeguards for PHI.

### DEFINITION

- **Shadow Chart:** A chart containing only copies of information from the medical record used primarily by satellite offices. These copies of the relevant documents from the original medical record are not part of the legal medical record.
- **PHI for the purpose of this protocol:** includes ePHI (electronic protected health information) and PHI that is transmitted in any form or medium (verbally, in writing, etc.).
- **Satellite Office:** An office, which operates under DMHSA. (i.e., Children's, Healing Hearts, Drug and Alcohol, Residential Recovery Homes, etc.)
- **Off-site for purposes of this protocol:** Any location outside of DMHSA main facility.

### STANDARDS OF CARE

- All DMHSA staff members, especially medical record personnel are responsible for the security of all records.
- Information systems personnel, supervisors, and medical records personnel shall periodically monitor the Department's compliance regarding its reasonable efforts to safeguard PHI.

## SAFEGUARDING AND STORING PHI PROTOCOL

- DMHSA protocol is in effect whether the staff member is working off-site (i.e., satellite office) or within the main facility.
- All mental health records shall have the proper safeguards in place to protect them from loss, damage and destruction.
- All persons (consumers, visitors, vendors and others) who are not authorized to have access to PHI should be supervised, escorted, or observed when visiting or walking through an area where PHI may be easily viewed or accessed.
- Staff shall avoid using consumers' names or the names of consumers' family members in public areas (hallway, elevator, stairway, etc.) when persons who are not authorized to receive the information are present.

### **PROTOCOL**

While access to PHI and conversations regarding a consumer, often occur freely and quickly in treatment settings, the following safeguards should take place to the extent reasonably practicable.

#### Storage of Written PHI:

- Any documents/records, not in use, containing PHI should be placed with identifying information face down on counters, desks, shelves, and other places where consumers, visitors, or other unauthorized persons might see them.
  - Records and documents with PHI should not be left out on desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, locked filing cabinets, or other locked areas (i.e., Medical Records Office).
  - In workplaces where lockable storage is not available, employees must take reasonable efforts to ensure the safeguarding of confidential information.
- Storage of documents containing PHI, whether on-site or off-site, must be locked at all times except during use by authorized personnel.

#### Meetings Where PHI is Discussed

- Specific types of meetings where PHI may be discussed include, but are not limited to, shift change report, multidisciplinary treatment team meetings, and case presentations.
- Meetings must be conducted in an area that is not easily accessible to unauthorized persons.
- If possible, meetings must be conducted in a room with a door that closes.

## SAFEGUARDING AND STORING PHI PROTOCOL

- Voices must be kept to a moderate level to avoid unauthorized persons from overhearing.
- Only staff members who have a “need to know” the information will be present at meetings where PHI is discussed.
- The PHI that is shared or discussed at the meeting will be limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

### Telephone Conversations

- Telephones used for discussing PHI shall be located in as private of an area as possible.
- Staff members shall take reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
  - Lowering their voice;
  - Requesting that unauthorized persons step away from the telephone area; or
  - Moving to a telephone in a more private area before continuing the conversation.
- PHI shared over the phone will be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure.

### In-Person Conversations

- In-person conversations include conversations that are held, in the consumer’s room, with consumer/family in public areas, and with authorized staff in public areas (stairs, elevator, hallway, etc.).
- Reasonable measures will be taken to assure that unauthorized persons do not overhear conversations involving PHI. Such measures may include:
  - Lowering their voice;
  - Moving to a private area within the Department; or
  - If in consumer’s room, creating more privacy.
- In an emergency situation, where the ability to discuss PHI quietly and in private may not be practicable, take reasonable precautions to preclude the disclosure of PHI to the extent possible.

### Safeguards for Written PHI

- Photocopying documents that contain PHI should be kept to a minimum.
- All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure.

## SAFEGUARDING AND STORING PHI PROTOCOL

- Documents should not be easily accessible to any unauthorized staff or visitors.
- No records shall be stored in boxes with consumer names or in cabinets through which the consumer's names can be seen.
- Medical records will be stored in such a manner that mobile shelving will be secure to protect the records from damage by fire and/or water.

### Active Records on the Inpatient Unit (AIU)

- Active records shall be stored in an area that allows staff providing care to the inpatient consumer, to access the records quickly and easily as needed.
- Authorized staff shall review the medical record at the nursing station.
- Active medical records shall not be left unattended on the nurses' station desk or other areas where consumers, visitors and unauthorized individuals could easily view the records.
- Medication Administration Records (MAR), report sheets and other documents containing PHI shall not be left open and/or unattended.

### Active Business Office Files:

Active business office files shall be stored in a secure area that allows authorized staff access as needed.

### Inactive Business Office Files:

Inactive business office files shall be stored in a systematic manner in a location that ensures privacy and security of the information.

### All Records Stored in Medical Records Office:

- Information systems personnel will identify and document those staff members with access codes to the medical records office.
- The minimum number of staff necessary to assure that records are secured yet accessible shall have access codes allowing access to the medical records office.
- Staff members with access codes shall assure that the access code is not shared with unauthorized individuals.
- Medical records must be signed out if removed from the medical records office according to the Departments protocol.
  - Only authorized persons shall be allowed to sign out such records.

# SAFEGUARDING AND STORING PHI PROTOCOL

## Inactive Records:

- Inactive records will be filed in a systematic manner in a location that ensures the privacy and security of the information. Information systems personnel and medical records personnel shall monitor storage and security of such medical records.
- Information systems personnel will identify and document those staff members with access to stored medical records.
- The minimum number of staff necessary to assure that records are secured yet accessible shall have access codes/keys allowing access to stored medical records.
- Staff members with access codes/keys shall assure that the code/keys are not accessible to unauthorized individuals.
- Inactive records must be signed out if removed from their designated storage area.
  - Only authorized persons shall be allowed to sign out such records.
- Records must be returned to storage promptly.

## Voicemail/Answering Machine Messages:

- Prior to calling or leaving voicemails, staff must ensure the consumer has given permission (on the first contact/demographic form) to call and/or leave a message at the number he/she provided, except when law or Department policy otherwise permits.
- When leaving a voice mail or answering machine message for a consumer, always limit the amount of information disclosed to the minimum necessary, such as the provider name and telephone number, or other information necessary to confirm an appointment, or to ask the individual to call back.
  - For example, when confirming an appointment, the information should be limited to appointment date and time, the provider's name, and a contact name and telephone number.
- Generally, when leaving a message with a family member or friend answering the consumer's phone, the message should be limited to a request for the consumer to return the call; and staff may leave his/her name, telephone number, and the fact that he/she works at DMHSA.

## Breach of Confidentiality:

- In the event that the confidentiality of PHI is breached, the discovering staff's supervisor shall be notified immediately.
- Department protocol will be followed if medical records are missing.

## SAFEGUARDING AND STORING PHI PROTOCOL

- An incident report must be filed for all breaches of confidentiality, including missing records.
- The theft or loss of any PHI or any device containing PHI (i.e., laptop) shall be immediately reported to a Supervisor.
- Employees will immediately report any violations of this protocol to their Supervisor or the Director.

### PHI Not a Part of the Designated Record Set:

- Use of "shadow" charts is discouraged, except when necessary for satellite offices (i.e., Children's, Healing Hearts, Drug and Alcohol, Residential Recovery Homes, etc.) to operate efficiently.
- Shadow charts shall be safeguarded in the same manner as all other records.

### Bulletin Boards:

- Bulletin boards located in areas that may be seen by consumers or visitors should not contain any documents containing PHI, unless the consumer has agreed to the display by written or verbal permission.
  - This would include pictures, cards and notes of appreciation and consumer's signed artwork.

### Destruction of Written Documentation:

- Documentation that is not part of the original medical record and will not become part of the medical record (e.g., shadow charts or files, psychotherapy notes, etc.) shall be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.
- All shredding bins should be placed in an area where unauthorized persons cannot easily view or access the PHI contained in the shredding bin.

### Destruction of Electronic Documentation:

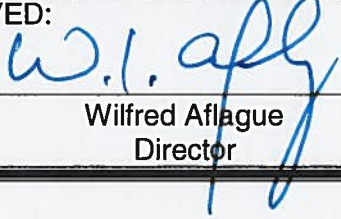
- Prior to the disposal of any computer equipment, including donation, sale or destruction, the Department must determine if PHI has been stored in this equipment and will delete all PHI prior to the disposal of the equipment.
  - All hard drives will be removed and destroyed as part of the destruction process.
- All media containing PHI or ePHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, faxes, hard drives, diskettes and CDs.

# SAFEGUARDING AND STORING PHI PROTOCOL

## REFERENCES

- 45 CFR § 164.530
- 45 CFR § 164.310(a)(1)
- 45 CFR § 164.310(b)

APPROVED:



\_\_\_\_\_  
Wilfred Aflague  
Director

Date: \_\_\_\_\_

