AUTHORITY: Compliance Officer

RESPONSIBILITY: MHC Staff, Delegate

LAST REVIEW DATE: 08/08/2018; Review Frequency 1 Year

PURPOSE OF PROCEDURE: To provide guidelines for the safeguarding of Protected Health Information ("PHI") with MHC and to limit unauthorized disclosures of PHI that is contained in an individual's file, while at the same time ensuring that such PHI is easily accessible to those involved in providing service to the individual

POLICY STATEMENT: MHC ensures, to the extent possible, that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other federal or state regulation governing confidentiality and privacy of health information

This process is designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that is contained in an individual's record

MHC recognizes that easy access to all or part of an individual's file is essential to ensure the efficient quality delivery of service

1. *MHC's Compliance Officer shall periodically monitor compliance regarding reasonable efforts to safeguard PHI*

2. *Safeguards for Verbal Uses: These procedures shall be followed, if reasonable by MHC, for any meeting or conversation where PHI is discussed*

   2.1. Specific types of meetings where PHI may be discussed include, but are not limited to:
   - Grievances & Appeals Meetings
   - Medical Review Meetings
   - Adhoc member Complaint Meetings
   - Member Services Staff Meetings
   - Customer Service Meetings with TPA

2.2. Meetings are conducted in an area that is not easily accessible to unauthorized persons

2.3. Meetings are conducted in a room with a door that closes, if possible

2.4. Voices are kept to a moderate level to avoid unauthorized persons from overhearing

2.5. Only staff individuals who have a *need to know* the information are present at the meeting. (See the Policy, Minimum Necessary Uses and Disclosures, co_pro37)

2.6. The PHI that is shared or discussed at the meeting is limited to the minimum amount necessary to accomplish the purpose of sharing the PHI

3. *Telephone conversations: Telephones used for discussing PHI are located in as private an area as possible*

3.1. Staff individuals takes reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
- Lowering the voice
- Requesting that unauthorized persons step away from the telephone area
- Moving to a telephone in a more private area before continuing the conversation

3.2. PHI shared over the phone is limited to the minimum amount necessary to accomplish the purpose of the use or disclosure

4. *In-Person conversations:* Reasonable measures are taken to assure that unauthorized persons do not overhear conversations involving PHI
- With individual/family in public areas
- With authorized staff in public areas

4.1. Such measures may include:
- Lowering the voice
- Moving to a private area within the CO-OP

5. *Active Records:* Active records shall be stored in an area that allows staff providing service to individuals to access the records quickly and easily as needed

5.1. Authorized staff shall review the record in-house, unless it is signed out in accordance with CO-OP procedure

5.2. Active records shall not be left unattended where unauthorized individuals could easily view the records

5.3. Only authorized staff shall review the records. All authorized staff reviewing records shall do so in accordance with the minimum necessary standards

5.4. Records shall be protected from loss, damage and destruction

6. *Active Business Files:* Active Business Files shall be stored in a secure area that allows authorized staff access as needed

7. *Thinned Records Inactive Records:* Thinned and inactive records are filed in a systematic manner in a location that ensures the privacy and security of the information

7.1. The Health Information Manager or a designee shall monitor storage and security of such records

7.2. When records are left unattended, records are in a locked room, file cabinet or drawer

7.3. The Administrator identifies and document those staff individuals with keys to stored records

7.3.1. The minimum number of staff necessary to assure that records are secure yet accessible shall have keys allowing access to stored Records

7.3.2. Staff individuals with keys shall assure that the keys are not accessible to unauthorized individuals

7.4. Inactive records must be signed out if removed from their designated storage area

7.4.1. Only authorized persons shall be allowed to sign out such records

7.5. Records must be returned to storage promptly

7.6. In the event that the confidentiality or security of PHI stored in an active or inactive record has been breached, MHC's Privacy Official and Administrator shall be notified immediately

8. *Inactive Business Files:* Inactive Business Files shall be stored in a systematic manner in a location that ensures privacy and security of the information

9. *Office Equipment Safeguards:* Only staff individuals who need to use computers to accomplish work-related tasks shall have access to computer workstations, terminals and systems

    9.1. All users of computer equipment must have unique login and passwords

    9.2. Passwords shall be changed every 90 days (See Password Policy, it_pro08)

    9.3. Workstations automatically lock after 10 minutes of activity, forcing the user to re-enter their passwords

    9.4. Domain accounts are locked and network resources are inaccessible after five unsuccessful attempts to log in

    9.5. Posting, sharing and any other disclosure of passwords and/or access codes is prohibited except as pre-approved and documented by the Compliance Officer

    9.6. Access to computer-based PHI shall be limited to staff individuals who need the information for treatment, payment, health care operations or business reasons

    9.7. CO-OP staff individuals shall lock or log off their workstation when leaving the work area

    9.8. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen

    9.9. Employee network access and privileges are promptly disabled following their departure from employment

    9.10. Employees immediately report any violations of this Policy to their supervisor, Administrator or CO-OP Compliance Officer

10. *Printers copiers and fax machines:* Printers are located in areas not easily accessible to unauthorized persons

10.1. If equipment cannot be relocated to a secure location, a sign is posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment

10.1.1. Sample language: *Only authorized staff may view documents generated by this (indicate printer, copier, fax, etc.). Access to such documents by unauthorized persons is prohibited by federal law*

10.2. Documents containing PHI are promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location

10.3. Documents containing PHI that must be disposed of due to error in printing are destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed