PURPOSE:
The purpose of this policy is to provide guidelines for the safeguarding of Protected Health Information ("PHI") at My Health Onsite and to limit unauthorized disclosures of PHI that is contained in a patient’s Medical Record, while at the same time ensuring that such PHI is easily accessible to those involved in the treatment of the patient.

POLICY:
The policy of My Health Onsite is to ensure 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. The following procedure 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 patient’s Medical Record. At the same time, My Health Onsite recognizes that easy access to all or part of a patient’s Medical Record by health care practitioners involved in a patient’s care (nurses, attending and consulting physicians, and others) is essential to ensure the efficient quality delivery of health care.

The HIPAA Compliance Officer is responsible for the security of all Medical Records. All staff members are responsible for the security of the active Medical Records at the work stations.

PROCEDURE:
My Health Onsite’s HIPAA Compliance Officer shall periodically monitor My Health Onsite’s compliance regarding its reasonable efforts to safeguard PHI.

Safeguards for Verbal Uses
These procedures shall be followed, if reasonable by My Health Onsite, for any meeting or conversation where PHI is discussed.

Meetings during which PHI is discussed:
1. Specific types of meetings where PHI may be discussed include, but are not limited to:
   a. Huddles or Operational meetings
   b. Family Care Conferences
2. Meetings will be conducted in an area that is not easily accessible to unauthorized persons.
3. Meetings will be conducted in a room with a door that closes, if possible.
4. Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.

5. Only staff members who “need to know” the information will be present at the meeting. (See the Policy “Minimum Necessary Uses and Disclosures.”)

6. 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:
1. Telephones used for discussing PHI are located in as private an area as possible.

2. Staff members will take reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
   a. Lowering the voice
   b. Requesting that unauthorized persons step away from the telephone area
   c. Moving to a telephone in a more private area before continuing the conversation

3. 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 exam rooms
- With patient/family in public areas
- With authorized staff in public areas

Reasonable measures will be taken to assure that unauthorized persons do not overhear conversations involving PHI. Such measures may include:
1. Lowering the voice
2. Moving to a private area within the health center
3. If in exam room, close the door

Safeguards for Written PHI
All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or visitors.
Active Records at designated work stations:
1. Active Medical Records shall be stored in an area that allows staff providing care to patients to access the records quickly and easily as needed.
2. Authorized staff shall review the Medical Record at the designated work stations.
3. Active Medical Records shall not be left unattended at designated work stations or other areas where patients, visitors and unauthorized individuals could easily view the records.
4. Documents containing PHI shall not be left open and/or unattended.
5. Only authorized staff shall review the Medical Records. All authorized staff reviewing Medical Records shall do so in accordance with the minimum necessary standards.
6. Medical Records shall be protected from loss, damage and destruction.

Thinned Records, Inactive Medical Records:
1. Thinned and inactive Medical Records will be filed in a systematic manner in a location that ensures the privacy and security of the information. The HIPAA Compliance Officer shall monitor storage and security of such Medical Records. When records are left unattended, records will be in a locked room, file cabinet or drawer.
2. The HIPAA Compliance Officer will identify and document those staff members with keys/codes to stored Medical Records. The minimum number of staff necessary to assure that records are secure yet accessible shall have keys allowing access to stored Medical Records. Staff members with keys/codes shall assure that they are not accessible to unauthorized individuals.
3. Records must be returned to storage promptly.
4. In the event that the confidentiality or security of PHI stored in an active or inactive Medical Record has been breached, My Health Onsite’s HIPAA Compliance Officer shall be notified immediately.
5. Health Center procedure will be followed if Medical Records are missing.

Office Equipment Safeguards

Computer access:
1. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations.
2. All users of computer equipment must have unique login and passwords.
3. It is recommended that passwords be changed every 90 days for applications which PHI can be accessed such as the EHR.
4. Posting, sharing and any other disclosure of passwords and/or access codes is not permitted.
5. Access to computer-based PHI shall be limited to staff members who need the information for treatment or health care operations.
6. Health Center staff shall log off their workstation when leaving the work area.
7. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.
8. Employee access privileges will be removed promptly following their departure from employment.
9. Employees will immediately report any violations of this Policy to their supervisor and the HIPAA Compliance Officer.

Printers, copiers and fax machines:
1. Printers will be located in areas not easily accessible to unauthorized persons.
2. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment. 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.”
3. Documents containing PHI will be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location.
4. Documents containing PHI that must be disposed of due to error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed.

Destruction
Written:
Documentation that is not part of the Medical Record and will not become part of the Medical Record (e.g., report sheets, shadow charts or files, notes, lists of vital signs, weights, 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.
<table>
<thead>
<tr>
<th>SAFEGUARDING &amp; STORAGE OF PHI</th>
<th>Policy# HPA5004</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECTION 5: HIPAA</td>
<td>PAGE: 5 OF: 5</td>
</tr>
<tr>
<td></td>
<td>EFFECTIVE: 8/24/17</td>
</tr>
<tr>
<td>APPROVED BY: CQI TEAM</td>
<td>REVISED: 10/4/17</td>
</tr>
</tbody>
</table>

**Electronic:**

Prior to the disposal of any computer equipment, including donation, sale or destruction, the health center must determine if PHI has been stored in this equipment and will delete all PHI prior to the disposal of the equipment.