WEBER HUMAN SERVICES	**Policy & Procedure** HIPAA/PRIVACY **SAFEGUARDING AND STORING PHI**	**NUMBER** 19
		APPROVED 2/21/2014
		REVIEWED 5/11/2017
		REVISED

PURPOSE:

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

POLICY:

The policy of this Facility is to ensure, 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. 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 client's Medical Record. At the same time, the Facility recognizes that easy access to all or part of a client's Medical Record by health care practitioners involved in a resident's care (nurses, physicians, therapists, and others) is essential to ensure the efficient quality delivery of health care.

The HIPAA Security Officer is responsible for the security of all Medical Records. All staff members are responsible for the security of the active Medical Records.

PROCEDURE:

The Privacy Officer and Security Officer shall periodically monitor the Facility's compliance regarding its reasonable efforts to safeguard PHI.

Safeguards for Verbal Uses

These procedures shall be followed, if reasonable by the Facility, for any meeting or conversation where PHI is discussed.

Meetings during which PHI is discussed:

1. Meetings will be conducted in an area that is not easily accessible to unauthorized persons.
2. Meetings will be conducted in a room with a door that closes, if possible.
3. Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.
4. Only staff members who have a "need to know" the information will be present at the meeting. (See the Policy "Minimum Necessary Uses and Disclosures.")
5. 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.

<u>In-Person conversations:</u>

- In private offices
- With client/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 Facility

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.

1. Documents with PHI shall not be left unattended in other areas where clients, visitors and unauthorized individuals could easily view or access the records.
2. Documents containing PHI shall not be left open and/or unattended.
3. Only authorized staff shall view the Medical Records. All authorized staff reviewing Medical Records shall do so in accordance with the minimum necessary standards.
4. Medical Records shall be protected from loss, damage and destruction.
5. When transporting documents with PHI away from WHS, the documents shall always be secured in a locked storage device.

<u>PHI Not a Part of the Designated Record Set:</u>

1. Any documentation of PHI shall be stored in a location that ensures, to the extent possible, that such PHI is accessible only to authorized individuals.

Office Equipment Safeguards

<u>Computer access:</u>

1. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals.
2. All users of computer equipment must have unique login and passwords.

3. Passwords shall be changed every 180 days.
4. Posting, sharing and any other disclosure of passwords and/or access codes is prohibited except to designated IT staff for the purpose of resolving computer issues, afterwhich the password should be promptly changed.
5. Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment or health care operations.
6. Facility staff members 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, Security Officer or Facility Privacy Officer or the Compliance Hotline.

<u>Printers, copiers and fax machines:</u>

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.