HIPAA/PRIVACY
Safeguarding and Storing Protected Health Information

Patient Name: FIRST LAST **Date:** 05/08/2019

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 patient's Medical Record, while at the same time ensuring that such PHI is easily accessible to those involved in the treatment of the resident.

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 patient's Medical Record. At the same time, the Facility 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, therapists, and others) is essential to ensure the efficient quality delivery of health care.

The Administrator is responsible for the security of all Medical Records. All staff members are responsible for the security of the active Medical Records at the nursing stations.

PROCEDURE

The Facility Privacy Official and Administrator 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. Specific types of meetings where PHI may be discussed include, but are not limited to:
   a. Shift Change Report
   b. Daily Standup or Department Head meetings
   c. Interdisciplinary Plan of Care meeting
   d. Medicare meeting
   e. Bill review meetings
   f. Family Care Conference
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.


1*61038*2019-04-25*1762*0*NOSIG*2*1

5. 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.")
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 patient 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 Facility
3. If in patient room, pulling the privacy curtain

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 on Nursing Unit:

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 nursing station, unless it is signed out in accordance with Facility procedure.
3. Active Medical Records shall not be left unattended on the nurses' station desk or other areas where patients, visitors and unauthorized individuals could easily view the records.
4. Medication Administration Records, Treatment Administration Records, report sheets and other documents containing PHI shall not be left open and/or unattended.

1*61038*2019-04-25*1762*0*NOSIG*2*2

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.

Active Business Office Files:

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

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 Health Information Manager or a designee 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 Administrator will identify and document those staff members with keys 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 shall assure that the keys are not accessible to unauthorized individuals.
3. Inactive Medical Records must be signed out if removed from their designated storage area. Only authorized persons shall be allowed to sign out such records.
4. Records must be returned to storage promptly.
5. In the event that the confidentiality or security of PHI stored in an active or inactive Medical Record has been breached, the Facility Privacy Official and Administrator shall be notified immediately.
6. Facility procedure will be followed if Medical Records are missing.
7. In the event of a change in ownership of the Facility, the Medical Records shall be maintained as specified in the Purchase and Sale Agreement.

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.

PHI Not a Part of the Designated Record Set:

1. Use of "shadow" charts or files is discouraged.
2. 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

Computer access:


1*61038*2019-04-25*1762*0*NOSIG*2*3

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 90 days.
4. Posting, sharing and any other disclosure of passwords and/or access codes is strongly discouraged.
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, Administrator or Facility Privacy Official.

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.

Electronic:

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


1*61038*2019-04-25*1762*0*NOSIG*2*4

Signature of Patient or Personal Representative

Date

Print Name

Personal Representative's Title