

SEPA Labs	Policy & Procedure HIPAA / PRIVACY SAFEGUARDING AND STORING PROTECTED HEALTH INFORMATION	FUNCTION
		NUMBER 1d
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

PURPOSE

The purpose of this policy is to provide guidelines for the safeguarding of Protected Health Information (“PHI”) in SEPA Labs and to limit unauthorized disclosures of PHI that is contained in a patient’s Laboratory 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 SEPA Labs 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 Laboratory Record. At the same time, SEPA Labs recognizes that easy access to all or part of a patient’s Laboratory Record by health care practitioners involved in a patient’s care is essential to ensure the efficient quality delivery of health care.

The Administrator / CEO is responsible for the security of all Laboratory Records. All staff members are responsible for the security of the active Laboratory Records at the work stations.

PROCEDURE

SEPA Labs Privacy Official and Administrator / CEO shall periodically monitor SEPA Labs’ compliance regarding its reasonable efforts to safeguard PHI.

Safeguards for Verbal Uses

These procedures shall be followed, if reasonable by SEPA Labs, 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. Clinical Review - Report meetings
 - b. Department Head or Managers meetings
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 have a “need to know” the information will be present at the meeting. (See the Policy “Minimum Necessary Uses and Disclosures.”)

SEPA Labs	Policy & Procedure HIPAA / PRIVACY SAFEGUARDING AND STORING PROTECTED HEALTH INFORMATION	FUNCTION
		NUMBER 1d
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

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.

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:

1. Active Laboratory Records shall be stored in an area that allows staff to access the records quickly and easily as needed.
2. Active Laboratory Records shall not be left unattended.
3. Only authorized staff shall review the Laboratory Records. All authorized staff reviewing Laboratory Records shall do so in accordance with the minimum necessary standards.
4. Laboratory 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 Laboratory Records:

1. Thinned and inactive Laboratory 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 Laboratory Records.
2. In the event that the confidentiality or security of PHI stored in an active or inactive Laboratory Record has been breached, SEPA Labs Privacy Official and Administrator shall be notified immediately.

SEPA Labs	Policy & Procedure HIPAA / PRIVACY SAFEGUARDING AND STORING PROTECTED HEALTH INFORMATION	FUNCTION
		NUMBER 1d
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

3. SEPA Labs procedure will be followed if Laboratory Records are missing.
4. In the event of a change in ownership of SEPA Labs, the Laboratory 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.

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 or terminals.
2. All users of computer equipment must have unique login and passwords.
3. Passwords shall be changed on a regular basis.
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 laboratory testing processes, diagnosis, payment or health care operations.
6. SEPA Labs 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, the Administrator / CEO or SEPA Labs 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.

SEPA Labs	Policy & Procedure HIPAA / PRIVACY SAFEGUARDING AND STORING PROTECTED HEALTH INFORMATION	FUNCTION
		NUMBER 1d
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

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 Laboratory Record and will not become part of the Laboratory Record (e.g., report sheets, shadow charts or files, 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.

Electronic:

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

(See the Policy “Destruction of Protected Health Information” for additional guidelines.)

SEPA
Labs

Policy & Procedure

HIPAA / PRIVACY
**SAFEGUARDING AND STORING
PROTECTED HEALTH INFORMATION**

FUNCTION

NUMBER

1d

PRIOR ISSUE

EFFECTIVE DATE

January 1, 2014

This page intentionally left blank.