HIPPA Privacy Rule Policies

Policies and Procedures **SAFEGUARDS**	Policy # 4	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To establish workplace controls required of all LifeMed ID's workforce members to ensure adherence to privacy requirements in keeping with LifeMed ID's obligations to maintain the privacy of Protected Health Information (PHI) in accordance with state and federal privacy laws, HIPAA Regulations and LifeMed ID's contracts with its customers.

Policy

It is the policy of LifeMed ID to protect PHI and to ensure that reasonable safeguards are implemented, that all workforce members are trained on and follow documented policies and procedures to prevent intentional or unintentional impermissible use or disclosure of PHI in accordance with state and federal privacy laws, HIPAA Regulations and LifeMed ID's contracts with its customers.

All workforce members must comply with this policy. Violations of this policy will result in disciplinary action based on the seriousness of the offense or other factors. Disciplinary action may include written warning, suspension, or termination.

Definitions

"Customer" is an entity from which LifeMed ID receives PHI subject to a Business Associate Agreement (or other written agreement with the entity) in compliance with the HIPAA Regulations and approved by LifeMed ID's legal counsel.

For definitions of other capitalized terms or phrases, please refer to: *HIPAA-HITECH Privacy and Security Glossary*.

Procedures

1. Privacy Requirements. LifeMed ID's Privacy Officer is responsible for developing and maintaining complete, up-to-date Privacy Policies and Procedures, ensuring that all LifeMed ID's workforce members are trained and sanctions are appropriately applied for non-compliance. Refer to: Privacy Policy #1: Privacy Officer Assignment and Responsibilities and Privacy Policy #2: Privacy Training Requirements.

2. Electronic PHI (ePHI) Safeguards. LifeMed ID's Security Officer is responsible for ensuring that the safeguards described in the HIPAA Security Rule for ePHI are documented in LifeMed ID's Security Policies and Procedures, that all applicable workforce members are trained and have implemented these safeguards, and that sanctions are applied for non-compliance. In addition, the Security Officer is responsible for ensuring that proper safeguards for devices not covered by the HIPAA Security Rule that create, maintain, store or transmit ePHI are documented and implemented (e.g. smartphone, flash drives and email). Refer to LifeMed ID's Security Policies and Procedures.

3. Paper and Oral PHI Safeguards. LifeMed ID's Privacy Officer is responsible for ensuring that the safeguards for written and oral PHI are documented in LifeMed ID's Privacy Policies and Procedures and that all applicable workforce members are trained and have implemented these requirements, and that sanctions may be applied for non-compliance.

    a. Written PHI safeguards include, but are not limited to, the proper handling, filing, storing, transporting and disposal of paper files, faxes, reports, authorizations, prescriptions, appointments, schedules, etc.

    b. Oral PHI safeguards include, but are not limited to, verification of caller identification, content of voice messages, communications among workforce members, communications with patients, announcements, etc.

    c. Safeguards for telecommuter workforce members include, but are not limited to, transporting PHI, computer use by family members, password management and time-outs, securing paper files and reports, phone discussion confidentiality, cell phone use, etc.

4. Facility Safeguards. LifeMed ID's is responsible for ensuring that safeguards for facility access and workplace safeguards are documented and that all applicable workforce members are trained and have implemented these requirements. Some examples include, but are not limited to, the following:

    a. Identification Badges: All workforce members and visitors will wear identification badges prominently visible at all times.

        i. Identification badges will differentiate between employee, contractor, vendor, etc. in order to ensure limited access to the "minimum necessary" PHI depending on the responsibilities

of the workforce member or the purpose of the visit. Refer to: Privacy Policy #5: Minimum Necessary: Uses, Disclosures and Requests.

ii. Certain restricted areas that require special access will be under lock and key and only accessible by authorized workforce members. as approved by LifeMed ID's Privacy and Security Officers. Should an unauthorized person need to gain access to restricted areas, they will do so only if escorted by an authorized workforce member.

b. Visitors: Visitors will sign in, be issued a visitors' badge, be escorted by an authorized workforce member at all times and sign out upon leaving the facility.

c. Facility Tours: In addition to the above:

i. Prior to the commencement of any tour, visitors must sign a confidentiality agreement, indicating acknowledgement and agreement not to further use or disclose any inadvertent disclosure of PHI,

ii. Walk-through tours by visitors will be conducted in a manner that does not allow visitors to listen to or overhear telephonic or onsite discussions regarding PHI, and

iii. Visitors may not view computer screens containing PHI or encounter PHI in any other manner.

d. Keys: Keys to sensitive areas that house PHI will be issued to authorized persons only upon approval by LifeMed ID's Privacy and/or Security Officers.

i. Sign-in and out logs for building maintenance to enter areas housing PHI will be maintained by LifeMed ID and will include the purpose of the maintenance,

ii. Workforce members will immediately report any attempt to enter a restricted area by unauthorized persons to the appropriate office.

e. Restricted Areas: Entries to restricted areas that are temporarily unlocked and/or propped open to allow moving of equipment, furniture, supplies, etc. will be continuously monitored by an authorized workforce member.

f. Paper Shredders: Sufficient number of paper shredders will be located in appropriate areas, for example, near fax and copy machines, and that shredders will be emptied as needed and by a reputable company.

g. File Cabinets: An appropriate number and location of lockable file cabinets and storage areas will be provided to those workforce members who need to protect PHI.

h. Other Facility Controls: All other facility security controls and safeguards as required in the HIPAA Security Rule will be in place.

i. Reporting: Workforce members will report to the appropriate office, any attempt by an unauthorized person to gain entrance to a restricted area.

5. Transporting PHI. LifeMed ID's workforce members are responsible for securing PHI in their possession during transit. This includes any and/or all of the following measures:

a. Store all forms of media containing PHI (paper format or encrypted electronic media} in a locked container.

b. Keep laptop, PDA or other Mobile Devices and all media containing PHI in personal possession during transport.

c. Avoid leaving laptops, PDA or other Mobile Devices unattended in public areas, especially airports.

d. Never leave laptops, PDA or other Mobile Devices or media containing PHI in luggage to be stored or transported via public transport.

e. Avoid leaving laptops, PDA or other Mobile Devices or media containing PHI in visible areas of an automobile; lock automobile doors when leaving the vehicle.

f. Workforce members working in home offices and other teleworker environments will assure that:

i. Visitors and family members do not have access to LifeMed ID's business computers or media containing PHI,

ii. PHI in any format is not visible to unauthorized viewers,

iii. ePHI is never stored on non-LifeMed ID-owned computers, laptops or computer readable storage media, and

iv. PHI in paper format is stored in locked file devoted to LifeMed ID's operations.

g. When ending a remote session on a LifeMed ID computer, the workforce member must wait for confirmation of the log-out command from the remotely connected LifeMed ID machine before leaving the work station.

Documentation

This version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, will be retained by LifeMed ID for a period of at least 6 years plus the current year from the date of creation or the date when last in effect, whichever is later.

Regulatory Authority

45 C.F.R. §164.500 Applicability.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

45 C.F.R. §164.530 Administrative requirements.

(c) (1) Standard: *Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.*

(2) (i) Implementation specification: *Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.*

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

45 C.F.R. §164.502 Uses and disclosures of protected health information: general rules.

(e) (1) Standard: *Disclosures to business associates.*

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, ~~or~~ receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) Implementation specification: *documentation. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e).*

45 C.F.R. §164.504 Uses and disclosures: Organizational requirements.

(e) (1) Standard: *Business associate contracts.*

(2) Implementation specifications: *Business associate contracts. A contract between the covered entity and a business associate must:*

(ii) Provide that the business associate will:

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

References

Internal

1. Privacy Policy #1, Privacy Office Assignment and Responsibilities
2. Privacy Policy #2, Privacy Training Requirements
3. Privacy Policy #5, Minimum Necessary, Uses, Disclosures and Requests

External

1. Omnibus Final Rule: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a1031c979126e6440b522063b7bba578&rgn=div5&view=text&node=45:1.0.1.3.78&idno=45%20