HIPPA Privacy Rule Policies

Policies and Procedures **PRIVACY TRAINING REQUIREMENTS**	Policy # 2	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To describe LifeMed ID's privacy training requirements for all workforce members 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 provide appropriate privacy training for all workforce members to assure that they understand the privacy requirements established under contracts with customers and under state and federal privacy laws and HIPAA Regulations.

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. Development of Privacy Training Program. The Privacy Officer or designee, is responsible for developing or arranging for privacy training for all workforce members, upon hire and periodically thereafter, but no less frequently than annually. The Privacy Officer, or designee, is also responsible for providing updates following significant regulatory changes or other material changes to LifeMed ID's Privacy Policies and Procedures that impact workforce members' job functions.

2. Privacy Training Method. Privacy training will be conducted in a manner that ensures that workforce members with common duties and responsibilities, and/or access levels and security clearance, attend

together so that more attention may be devoted to specific responsibilities and the privacy requirements related to such responsibilities.

3. Privacy Training for New Workforce Members. New workforce members will receive initial privacy training on Privacy Policies and Procedures within a reasonable period of time after joining LifeMed ID, and will not be allowed to access, use or disclose until they have received appropriate training.

4. Content. The initial privacy training will cover, at a minimum, the following basic matters:

   a. The history and purpose of federal privacy laws, including the HIPAA Regulations, and the legal responsibilities of LifeMed ID

   b. Individual privacy rights, including access and inspection, amendments, accountings of disclosures, requests for restrictions, and confidential communications; specific procedures will not be covered unless the workforce member will be responsible for assisting individuals or customer's with exercising these rights or are likely to receive request from individuals.

   c. Allowable internal uses and disclosures for Treatment, Payment, and Health Care Operations.

   d. "Minimum necessary" requirements for uses, disclosures and requests, with special attention given to how the workforce members will apply these requirements to their own duties and responsibilities.

   e. Internal safeguards within LifeMed ID, including administrative, physical, and technical safeguards to protect the security and integrity of PHI. Special attention will be given to the measures that will be taken by the workforce members with respect to their own duties and responsibilities.

   f. An introduction to LifeMed ID's Privacy Policies and Procedures, with special attention given to those policies that may be needed by the workforce members when carrying out their duties.

   g. Procedures for obtaining clarification of privacy requirements and for notifying the Privacy Officer or other appropriate persons in the event of a possible privacy breach. Refer to: Privacy Policy #28: Reporting Impermissible Uses and Disclosures, Violations, Mitigation and Sanctions.

   h. The penalties and consequences to LifeMed ID's and its workforce members and/or its customers and LifeMed ID's Subcontractors for violations of the HIPAA Regulations.

i. Disciplinary sanctions that will be imposed on a workforce member by LifeMed ID for non-compliance with the Privacy Policies and Procedures which may range from receiving a warning to being terminated. Refer to: Privacy Policy #28: Reporting Impermissible Uses and Disclosures, Violations, Mitigation and Sanctions.

5. Privacy Training Log. A log will be maintained by the Privacy Officer or designee, of all workforce members who have participated in privacy training. Failure by a workforce member to participate in privacy training may result in termination.

6. Collaboration. The Privacy Officer is responsible for oversight of privacy training through collaboration with business unit managers and trainers.

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.

(b) **(1) Standard:** *Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.*

(2) Implementation specifications: Training.

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

References

Internal

1. Privacy Policy #28, Reporting Violations, Mitigation and Sanctions

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