HIPPA Privacy Rule Policies

Policies and Procedures **PRIVACY POLICIES AND PROCEDURES**	Policy # 3	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

This policy is designed to assure the timely development, implementation, modification and retention of documented Privacy Policies and Procedures related to 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 develop, implement, modify (when needed or appropriate) and retain Privacy Policies and Procedures and to assure that all of LifeMed ID's workforce members comply with those Privacy Policies and Procedures.

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

The Privacy Officer will be responsible for:

1. Developing LifeMed ID's Privacy and Breach Notification Policies and Procedures in coordination with LifeMed ID's management and legal counsel. Refer to: Privacy Policy #1: Privacy Office Assignment and Responsibilities.

2. Monitoring and assuring that any necessary revisions are made to LifeMed ID's Privacy and Breach Notification Policies and Procedures in a timely manner following changes in state or federal laws or HIPAA Regulations. Refer to: Privacy Policy #1: Privacy Officer Assignment and Responsibilities.

3. Monitoring and assuring that any necessary revisions are made to LifeMed ID's Privacy and Breach Notification Policies and Procedures in a timely manner following changes in LifeMed ID's organization, operations or technology capabilities and, as needed, following a Security Incident and/or an impermissible use or disclosure of PHI. Refer to: Privacy Policy #1: Privacy Officer Assignment and Responsibilities, Privacy Policy #28: Reporting Impermissible Uses and Disclosures, Violations, Mitigation and Sanctions.

4. Ensuring that any modifications in LifeMed ID's Privacy and Breach Notification Policies and Procedures are consistent with the applicable terms of LifeMed ID's Business Associate Agreements, LifeMed ID's contracts with its customers and/or the Notice of Privacy Practices of LifeMed ID's customers.

5. Ensuring that LifeMed ID's Privacy and Breach Notification Policies and Procedures are in written or electronic form, and available to appropriate LifeMed ID workforce members.

6. Ensuring versioning control and retention of LifeMed ID's Privacy and Breach Notification Policies and Procedures for at least six (6) years from the date of creation or date of last use, whichever is later.

7. Conducting periodic assessments of compliance with LifeMed ID's Privacy and Breach Notification Policies and Procedures, and making LifeMed ID's management aware of any known or potential problems that will be addressed. Refer to: Privacy Policy #1: Privacy Office Assignment and Responsibilities.

8. Ensuring the development and provision of LifeMed ID's initial and ongoing privacy training for workforce members, including orientation for new workforce members and updates for current workforce members periodically and when necessary. Refer to: Privacy Policy #2: Privacy Training Requirements.

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. §164.530(i) Policies and Procedures.

(1) Standard: *Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.*

(2) Standard: *Changes to policies and procedures.*

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in §164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with §164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: *Changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by §164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with §164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.*

(4) Implementation specifications: *Changes to privacy practices stated in the notice.*

(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by §164.520(b)(3) to state the changed practice and make the revised notice available as required by §164.520(c). The covered

entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under §164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)–(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) Implementation specification: *Changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by §164.520, provided that:*

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

45 C.F.R. §164.530(j) Documentation.

A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(iv) Maintain documentation sufficient to meet its burden of proof under §164.414(b).

(2) Implementation specification: *Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.*

References

Internal

1. Privacy Policy #1, Privacy Officer Assignment and Responsibilities
2. Privacy Policy #2, Privacy Training Requirements
3. 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