HIPPA Privacy Rule Policies

Policies and Procedures **PRIVACY OFFICER ASSIGNMENT AND RESPONSIBILITIES**	Policy # 1	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To assure the establishment of a Privacy Officer for the purpose of overseeing LifeMed ID's obligations to maintain the privacy of Protected Health Information (PHI) in accordance with state and federal privacy laws, the HIPAA Regulations and LifeMed ID's contracts with its customers.

Policy

It is policy of LifeMed ID to identify a Privacy Officer responsible for all LifeMed ID's privacy matters including Privacy and Breach Notification Policies and Procedures and for assuring that all of LifeMed ID's workforce members comply with such requirements.

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. Appointment of Privacy Officer. LifeMed ID will appoint To Be Determined as the LifeMed ID Privacy Officer to be responsible for ensuring compliance with privacy requirements throughout LifeMed ID
2. Responsibilities of Privacy Officer. The Privacy Officer will have the responsibilities set forth in Exhibit A which will include receiving complaints related to LifeMed ID's Privacy Policies and Procedures and practices.
3. Contacting the Privacy Officer. The Privacy Officer can be contacted via LifeMed ID's email at Catherine.Schulten@lifemedid.com twenty-four (24) hours a day, seven (7) days a week. Incident and

disclosure reports must be immediately completed using the form provided by the LifeMed ID Privacy Officer.

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.

Exhibit A: Responsibilities of the Privacy Officer

Purpose:

The Privacy Officer is responsible for LifeMed ID's compliance with state and federal privacy laws and the HIPAA Privacy and Breach Notification Rules and LifeMed ID's contracts with its customers.

Qualifications:

The Privacy Officer should be familiar with the day-to-day operations of LifeMed ID The Privacy Officer will have the ability to work well with LifeMed ID's management, legal counsel, customers, subcontractors, regulatory agencies and law enforcement officials. The Privacy Officer will require a strong, practical working knowledge of LifeMed ID's operations and of state and federal privacy laws and HIPAA Regulations.

Responsibilities:

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 and as required by LifeMed ID's contracts with its customers.

2. Investigating and maintaining a log of all reported incidents and follow-up related to LifeMed ID and/or LifeMed ID's Subcontractors. Refer to: Privacy Policy #28: Reporting Impermissible Uses and Disclosures, Violations, Mitigation and Sanctions and Privacy Policy #15: Uses By and Disclosures to Subcontractors and Third Parties.

3. Monitoring and communicating changes in privacy and breach notification laws and regulations and in customer requirements, and assuring that any necessary revisions are made to LifeMed ID's Privacy and Breach Notification Policies and Procedures in a timely manner.

4. Conducting periodic assessments of compliance with LifeMed ID's Privacy and Breach Notification Policies and Procedures, and making LifeMed ID management aware of any known or potential problems that will be addressed.

5. Participating in the identification of subcontractors that handle PHI on behalf of LifeMed ID and ensuring that appropriate agreements and safeguards are implemented and maintained between LifeMed ID and its vendors and subcontractors and as required by LifeMed ID's contracts with its customers. Refer to: Privacy Policy #15: Uses By and Disclosures to Subcontractors and Third Parties.

6. Investigating and following up, as appropriate, on requests for PHI disclosures assigned to the Privacy Officer. Refer to: Privacy Policy #14: Overview of Required and Permissible Uses and Disclosures, Privacy Policy #9: Request for Access, Privacy Policy #10: Amendments of Protected Health Information, and Privacy Policy #11: Accounting of Disclosures.

7. Determining whether a charge for an accounting of disclosures is appropriate, and, if so, the amount of such charge. Refer to: Privacy Policy #10: Accounting of Disclosures.

8. Maintaining, or ensuring the maintenance of, all documentation required by the HIPAA Privacy and Breach Notification Rules as outlined in LifeMed ID's Privacy and Breach Notification Policies and Procedures and as required by LifeMed ID's contracts with its customers.

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

10. Responding to an individual's concerns and complaints regarding LifeMed ID's Privacy Policies and Procedures. Refer to: Privacy Policy #29: Reporting and Responding to Privacy Complaints.

11. Responding to and coordinating LifeMed ID's response to privacy audits by customers and regulatory agencies and working with LifeMed ID's management to assure that appropriate actions are taken to resolve any problems.

12. Collaborating with LifeMed ID's Information Security and facilities departments and assisting in the development of appropriate administrative, physical and technical safeguards for the protection of PHI in LifeMed ID's care. Refer to: Privacy Policy #4: Safeguards.

13. Assisting LifeMed ID's human resources department in developing appropriate disciplinary measures when workforce members violate LifeMed ID's Privacy Policies and Procedures. Refer to: Privacy Policy #28: Reporting Impermissible Uses and Disclosures, Violations, Mitigation and Sanctions.

14. Cooperating with customers and state and federal agencies, including the DHHS Office for Civil Rights, in any and all compliance reviews or investigations.

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.

(a) **(1) Standard:** *Personnel designations.*

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by §164.520.

(2) Implementation specification: *Personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.*

(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.

(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.

(d) **(1) Standard:** *Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by*

this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) Implementation specification: *Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.*

(e) **(1) Standard:** *Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of §164.502(j) or paragraph (g)(2) of this section.*

(2) Implementation specification: *Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.*

(f) Standard: *Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.*

(g) Standard: *Refraining from intimidating or retaliatory acts. A covered entity—*

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in §160.316 of this subchapter.

(h) Standard: *Waiver of rights. A covered entity may not require individuals to waive their rights under §160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.*

(i) **(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.

(j) **(1) Standard:** *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 #2, Privacy Training Requirements
2. Privacy Policy #4, Safeguards
3. Privacy Policy #9, Request for Access
4. Privacy Policy #10, Amendments of Protected Health Information
5. Privacy Policy #11, Accounting of Disclosures
6. Privacy Policy #14, Required and Permissible Uses and Disclosures
7. Privacy Policy #15, Uses By and Disclosures to Subcontractors and Third Parties
8. Privacy Policy #28, Reporting Violations, Mitigation and Sanctions
9. Privacy Policy #29, Reporting and Responding to Privacy Complaints

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