HIPPA & HITECH Breach Notification Rule Policies

Policies and Procedures **ADMINISTRATIVE REQUIREMENTS**	Policy # 1	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To describe the processes associated with ensuring that LifeMed ID complies with the administrative requirements (associated with the Privacy Rule: 45 C.F.R. §164.530 (b)- Training, (d) Complaints, (e) Sanctions, (g) Refraining from intimidating or retaliatory acts, (h) Waiver of Rights, (i) Policies and Procedures, and (j) Documentation) as they relate to, and are required by, the Breach Notification Rule.

Policy

It is LifeMed ID's policy that LifeMed ID's workforce members are aware of and comply with the administrative requirements associated with breach identification and notification in compliance with state and federal law and consistent with 45 C.F.R. §164.414.

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

For definitions of capitalized terms or phrases, please refer to *HIPAA-HITECH Privacy and Security Glossary* and *Definitions for Breach Notification Requirements*.

Procedures

1. Responsibility: LifeMed ID's Privacy Officer is responsible for ensuring compliance with the administrative requirements of the Breach Notification Rule and for providing all guidance and

determinations related to reported incidences in close consultation with LifeMed ID's legal counsel.

2. Training: The Privacy Officer or designee is responsible for ensuring the development and provision of a training program for all aspects of the Breach Notification Rule for all applicable workforce members, upon hire and periodically, but no less frequently than annually, as well as providing updates following significant changes in regulatory requirements, organization, operations, or other material changes to LifeMed ID's policies and procedures that impact their job functions and/or responsibilities. A log will be maintained by the Privacy Officer or designee of all workforce members who have participated in applicable training. Failure of a workforce member to participate in training may result in termination.

3. Complaints: LifeMed ID's Privacy Officer or designee is responsible for ensuring that complaints or concerns expressed by workforce members or others about LifeMed ID's privacy or breach practices are taken seriously and that LifeMed ID's workforce members have access to a Complaint Form, which can be obtained from LifeMed ID's Privacy Officer. This, in turn, is submitted to LifeMed ID's Privacy Officer. Other means and methods to register a complaint will be made available and communicated to such individuals including the ability to speak directly to LifeMed ID's Privacy Officer or corresponding directly with the Department of Health and Human Services (DHHS).

    a. LifeMed ID's Privacy Officer will promptly investigate any privacy-related or breach-related complaint with appropriate LifeMed ID's management and document findings and disposition, if any.

    b. If the complaint is justified, the Privacy Officer will oversee the implementation of prompt action to ensure that similar problems do not arise in the future.

    c. If updates to policies and procedures are required, or changes to LifeMed ID's Notice of Privacy Practices, the Privacy Officer will ensure timely and appropriate updates and training occur.

    d. If the investigation results in a determination that Protected Health Information (PHI) has been improperly disclosed (See Breach Notification Policy #2, Breach Risk Assessment),

the Privacy Officer will take steps to mitigate any harm associated with future or ongoing disclosure, including the destruction or return of the PHI.

e. Once the matter is resolved, the Privacy Officer, in consultation with legal counsel, will follow notification requirements see (See Breach Notification Policy #3, Breach Notification) and may respond to the Individual or other persons who complained.

4. Sanctions. Human Resources in consultation with LifeMed ID's Privacy Officer will establish a range of sanctions that may be imposed if LifeMed ID's breach notification policies and procedures are violated. Disciplinary action will be commensurate with the severity of the violation, the intent, the existence of previous violations and the degree of potential harm. Sanctions may range from warnings and further training in the event the workforce member was not aware of policy requirements, to immediate termination in the event of a knowing and intentional violation. The Human Resources Department is responsible for ensuring that all appropriate workforce members are made aware of the disciplinary actions and sanctions that may be imposed for non-compliance with LifeMed ID's Privacy and Security policies and procedures. Additionally, federal and state privacy and/or breach notification laws may impose civil and criminal penalties including fines and imprisonment for violations of the law.

5. Refraining from Intimidating or Retaliatory Acts. It is not a violation of LifeMed ID's policies for a LifeMed ID workforce member to file a complaint with the secretary of DHHS; testify, assist, or participate in an investigation or compliance review of LifeMed ID's breach notification policies; or oppose any act made unlawful by the federal privacy regulations, provided the workforce member has a good faith belief that LifeMed ID's action being opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the federal breach notification regulations. Sanctions will not be imposed based on such actions. No person filing or assisting in the investigation of a compliant shall be retaliated against or subject to intimidation of any kind.

6. Waiver of Rights. LifeMed ID will not require anyone to waive their rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

7. Policies and Procedures. LifeMed ID's Privacy Officer is responsible for ensuring the development, implementation and maintenance of appropriate and reasonably designed policies and procedures related to Breach Notification Rule requirements. The Privacy Officer will ensure that appropriate and timely changes to these policies and procedures due to changes in law, technology, organizational structure or services will be documented and approved by management, and made accessible and trained to LifeMed ID's workforce members.

8. Documentation. LifeMed ID's Privacy Officer is responsible for ensuring all required documentation associated with training, sanctions, complaints, investigations, mitigation activities, breach risk assessment, and policies and procedures are maintained for six (6) years.

Regulatory Authority

§164.414 Administrative requirements and burden of proof.

*(a) Administrative requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart**

***§164.530**

(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.

(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.*

(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. Policy #2, Breach Risk Assessment
2. Policy #3, Breach Notification

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