HIPPA & HITECH Breach Notification Rule Policies

Policies and Procedures **BREACH RICK ASSESSMENT**	Policy # 2	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To describe the follow-up processes from reports of incidents and complaints in order to identify, investigate, and determine the possibility of a breach and to document the details that support resulting decisions related to mitigation, remediation and notification consistent with state and federal privacy laws and in accordance with 45 C.F.R. §164.414(b) Burden of Proof.

Policy

It is LifeMed ID's policy to exercise reasonable diligence in connection with the discovery and investigation of any breach of unsecured Protected Health Information (PHI).

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. Upon a suspicion or knowledge of a privacy violation or security incident, an LifeMed ID workforce member will immediately notify the Privacy Officer of the incident as follows:

    a. Call and fill out an incident report available from the LifeMed ID Privacy Officer and submit to same including a brief description of what occurred, the date of the incident, the date on which

the incident was discovered, potentially number of records, and a description of the PHI or Personally Identifiable Information (PII) suspected to have been breached.

b. Will leave the environment and evidence unaltered, and

c. Will contact his/her supervisor or their designee assigned to investigate these types of situations and initiate mitigation procedures (refer to Privacy Policy #4, Reporting Violations, Mitigation and Sanctions).

2. The Privacy Officer will update the incident log and will execute the following steps in order to determine whether LifeMed ID has breach reporting obligations:

a. Determine <u>if the use or disclosure included unsecured PHI as defined by the Privacy Rule.</u> If the Privacy Officer determines that either:

i. the use or disclosure did not include PHI, or

ii. if the use or disclosure did include PHI, it was encrypted or otherwise "secured" (see Definitions for Breach Notification Requirements), or

iii. if the use or disclosure or use met one of the exclusions to the definition of a data breach, then he/she updates the incident log accordingly, enters the date that the incident was closed and determines if an update to procedures, and/or training and/or sanctions need to be considered.

b. If the Privacy Officer determines that the disclosure did include unsecured PHI and did not meet one of the exclusions, then he/she will proceed to step (c).

c. Determine <u>if the use or disclosure required an authorization or an opportunity to agree or object.</u> If the Privacy Officer, in consultation with the supervisor and LifeMed ID's legal counsel as appropriate, determines that the use or disclosure did not require an authorization or an opportunity to agree or object, then he/she updates the Incident Log accordingly and enters the date that the incident was closed. If the Privacy Officer determines that the disclosure did require authorization, then he/she will proceed to step (d).

d. Conduct a breach risk assessment. The Privacy Officer, in conjunction with legal counsel as appropriate, will conduct a "breach risk assessment" to determine whether or not there is a low probability that the PHI has been compromised based on at least the following factors:

   i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

   ii. The unauthorized person who used the PHI or to whom the disclosure was made;

   iii. Whether the PHI was actually acquired or viewed; and

   iv. The extent to which the risk to the PHI has been mitigated.

3. Following the Determination.

   a. If the Privacy Officer determines that the Incident does meet the threshold of low probability of compromise of PHI, then he/she updates the incident log documenting the risk assessment and decision, and enters the date that the incident was closed.

   b. If the Privacy Officer determines that the incident does not meet the threshold of low probability of compromise of the PHI, he/she determines that breach notification is required, documents the risk assessment and decision in the Incident Log and prepares for required notifications in accordance with the Breach Notification Rule and State regulations.

4. Mitigation. The Privacy Officer will immediately implement activities to mitigate any harm associated with future impermissible use of disclosure of the PHI, such as verification of destruction or return of the PHI.

5. Remediate. The Privacy Officer will oversee the development and implementation of a remediation plan that may include changes to facility access, data access, data security, policies and procedures, training material, and/or suspension or termination of a workforce member.

6. Updates to Policies & Procedures and LifeMed ID's Notice of Privacy Practices. If the cause of the incident or breach requires updating LifeMed ID's policies and procedures or Notice of Privacy Practices, the Privacy Officer will oversee the appropriate and timely activities to complete.

7. 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.

§164.414 Administrative requirements and burden of proof.

(a) **Burden of proof.** *In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at §164.402.*

References

Internal

1. Privacy Policy #4, 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