HIPPA Privacy Rule Policies

Policies and Procedures **DISCLOSURES, VIOLATIONS, MITIGATION AND SANCTIONS**	Policy # 28	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To describe the processes associated with reporting impermissible uses and disclosures of Protected Health Information (PHI), violations of the HIPAA Privacy Rule or LifeMed ID's Privacy Policies and Procedures, activities to remediate and mitigate future harm, and the circumstances under which sanctions may be imposed against a workforce members who violates the LifeMed ID's Privacy Policies and Procedures 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 that impermissible uses and disclosures of PHI, violations of the HIPAA Privacy Rule or LifeMed ID's Privacy Policies and Procedures are identified and addressed promptly, that appropriate measures are taken to mitigate any further impermissible use or disclosure and/or any unauthorized modification or destruction of PHI in order to reduce the possibility of harm or re-occurrence and that appropriate sanctions are imposed.

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. Examples of Impermissible Use or Disclosure of PHI. Examples of impermissible uses or disclosures of PHI that must be reported may include, but are not limited to, the following:
   a. Sharing PHI for purposes other than delivery of LifeMed ID's contractual services,
   b. Disclosure of PHI to individuals or workforce members without permission,

c. Emails containing PHI sent to an incorrect recipient,
d. Emails containing PHI sent to the correct recipient via an unsecure route,
e. Fulfillment errors resulting in PHI sent to an unintended recipient,
f. Fulfillment reports lost or missing in the mail (including U.S. Mail, Fed-Ex, UPS, etc.),
g. Facsimile errors resulting in PHI sent to an unintended recipient,
h. Voice mails containing PHI on a phone without permission,
i. Lost or stolen portable media containing PHI, such as laptops, flash drives, iPads or iPhones, or
j. Lost or stolen unsecured PHI, such as in paper faxes, records, notes, prescriptions, patient logs, visitor sign-in logs that include patient names.

2. Responsibility for Reporting Suspected or Confirmed Incidents of Impermissible Use or Disclosure of PHI.

   a. When a LifeMed ID workforce member suspects that PHI may have been used or disclosed in violation of HIPAA Regulations or any of LifeMed ID's Privacy or Security Policies or Procedures or customer contracts, the workforce member must notify a supervisor and/or the Privacy Office. Any supervisor receiving such a report will submit an incident report immediately to the Privacy Office by accessing and completing the form located at: {URL}.
   b. If the disclosure involves a breach of security as outlined in LifeMed ID's Security Policies and Procedures, the Privacy Officer will forward the report to LifeMed ID's Security Office.
   c. The LifeMed ID Privacy Officer and Security Officer, if applicable, will follow-up and/or investigate each suspected or confirmed incident reported on an incident report form in a manner that complies with LifeMed ID's internal standard operating procedures on investigation and reporting.

3. Responsibility of the LifeMed ID Privacy Officer or Designee. Upon receipt of notice of a potential impermissible use or disclosure, the Privacy Officer, with the advice of legal counsel if necessary, will:

   a. Immediately notify the Security Office if the potential impermissible use or disclosure pertains to a Security Incident (as outlined in LifeMed ID's Security Policies and Procedures),
   b. Initiate a triage process to determine if it is, indeed, an incident and whether further investigation should be initiated,
   c. Follow-up and/or investigate each suspected or confirmed incident reported on an incident report form in a manner that complies with LifeMed ID's internal standard operating procedures on investigation and reporting,
   d. Conduct, or oversee the conduct of, a detailed investigation of the circumstances associated with the use or disclosure including the collection of all relevant data for analysis,
   e. Immediately notify LifeMed ID's legal counsel of confirmed cases of impermissible uses or disclosure or other violations of state or federal privacy laws or HIPAA Regulations and provide updates as necessary or appropriate,
   f. In consultation with legal counsel:
   i. Determine whether the use or disclosure is a violation of the HIPAA Regulations or LifeMed ID's Privacy or Security Policies and Procedures and/or customer contractual requirements,
   ii. Determine whether notification is required under the HIPAA Breach Notification Rule or your Breach Notification Policies and Procedures or your customer's contract, and
   iii. If disclosure is required, the Privacy Officer or designee will follow the requirements for notification outlined in the customer contract, LifeMed ID's Breach Notification Policies and Procedures and by federal or state laws and the HIPAA Regulations,

g. Immediately begin an identification process of the affected individuals and the information that was used or disclosed,
h. Ensure the development and implementation of a remediation or corrective action plan that may include changes to facility access, data access, training material, and/or suspension or termination of a workforce member to reduce the possibility of a reoccurrence of the incident,
i. Implement activities to mitigate any harm associated with future impermissible use or disclosure of the PHI, such as verification of destruction or return of the PHI and:

i. Take reasonable steps to ensure no further use or disclosure of any unsecured PHI,
ii. Oversee the development and implementation of any required corrective action plan(s) to avoid a reoccurrence, and
iii. Determine with legal counsel the "probability of compromise" with respect to LifeMed ID's breach risk assessment policy *(*Refer to: *Breach Notification Policy #2: Breach Risk Assessment)*.

j. Monitor and/or audit to ensure the mitigation and remediation plans are implemented and effective,
k. If the terms of a Business Associate Agreement have been violated, comply with the requirements set forth in *Privacy Policy #15: Uses By and Disclosures to Subcontractors and Third Parties*.
l. Notify management when appropriate,
m. Determine the need to notify other internal or external stakeholders,
n. Determine the need to bring in external experts,
o. Notify LifeMed ID's leadership of any potential or expected sanctions that may need to be applied,
p. Identify any needed changes to LifeMed ID's Privacy Policies and Procedures and develop a plan to update them,
q. Communicate to the privacy training coordinator any changes to be included in upcoming training classes,
r. Document all pertinent and required information including the details and resolution of a reported suspected or confirmed incident or violation.

4. Sanctions.
    a. LifeMed ID's leadership, in consultation with the Privacy Officer, will establish a range of sanctions that may be imposed if LifeMed ID's Privacy Policies and Procedures are violated.
    b. Disciplinary action will be commensurate with the severity of the violation, the intent, the existence of previous violations and the degree of potential harm.
    c. 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 an intentional violation.
    d. All LifeMed ID's workforce members will be made aware of the disciplinary actions and sanctions that may be imposed by LifeMed ID as well as any civil or criminal penalties, including fines or imprisonment, that may be imposed for violations of state or federal privacy laws or HIPAA Regulations
5. No Sanctions Based on Whistleblowing or Complaints.
    a. It is not a violation of LifeMed ID's Privacy Policies and Procedures for a workforce member to disclose PHI to a Health Oversight Agency, Public Health Authority, or other appropriate entity in the good faith belief that LifeMed ID has engaged in unlawful conduct, violated professional or clinical standards, or

potentially endangered individuals, workforce member, or the public. Sanctions will not be imposed based on such disclosures.

b. It is not a violation of LifeMed ID's Privacy Policies and Procedures for a 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 Privacy Policies and Procedures, or oppose any act made unlawful by HIPAA 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 HIPAA Privacy Rule. Sanctions will not be imposed based on such actions.

c. It is not a violation of LifeMed ID's Privacy Policies and Procedures for a workforce member who is the victim of a criminal act to disclose information about the suspected perpetrator to a law enforcement agency, as long as the officer or agency's identity and authority has been verified and documented and the "minimum necessary" information to carry out the purpose is disclosed. Refer to: *Privacy Policy #5: Minimum Necessary: Uses, Disclosures and Requests* and *Privacy Policy #27: Verification of Identity and Authority*. Sanctions will not be imposed on such actions.

6. Accounting of Disclosure. LifeMed ID's Privacy Office will maintain a file of all impermissible uses or disclosures and other violations, as required by the customer contract and *Privacy Policy #11: Accounting of Disclosures*.

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. §164.502 Uses and disclosures of protected health information: general rules.

(j) Standard: *Disclosures by whistleblowers and workforce member crime victims*

(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in §164.512(f)(2)(i).

45 C.F.R. §164.504 Uses and disclosures: Organizational requirements.

e) **(1) Standard:** *Business associate contracts.*

(2) Implementation specifications: Business associate contracts. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity...

(ii) Provide that the business associate will:

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

45 C.F.R. §164.530 Administrative requirements.

(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.*

45 C.F.R. §164.410 Notification by a business associate.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

References

Internal

1. Breach Notification Policy #2, Breach Risk Assessment
2. Privacy Policy #5, Minimum Necessary: Uses, Disclosures and Requests
3. Privacy Policy #11, Accounting of Disclosures
4. Privacy Policy #15, Uses By and Disclosures to Subcontractors and Third Parties
5. Privacy Policy #27, Verification of Identify and Authority

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