HIPPA & HITECH Breach Notification Rule Policies

Policies and Procedures **BREACH NOTIFICATION REQUIREMENTS**	Policy # 3	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To describe the process for the timely and complete notification requirements following the discovery of a Breach in accordance with state and federal laws and consistent with 45 C.F.R. §164.404 Notification to Individuals, §164.406 Notification to the Media, §164.408 Notification to the Secretary, §164.410 Notification by a Business Associate and §164.412 Law Enforcement Delay.

Policy

LifeMed ID is committed to complying with the notification requirements following the discovery of an impermissible and unauthorized breach of unsecured Protected Health Information (PHI). LifeMed ID will ensure that notifications are made to individuals whose PHI or Personally Identifiable Information (PII) has been breached as required by the Breach Notification Rule.

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*.

Overview

1. LifeMed ID's Privacy Officer is responsible for this policy and providing all guidance related to breach notifications in close consultation with the LifeMed ID's legal counsel.

2. In the case of a Breach of unsecured PHI or PII, LifeMed ID will provide the notifications required by both state and federal regulations within the required timeframes. State Law Preemption Exception: in general, State laws that go above and beyond the requirements of the HIPAA-HITECH Privacy or Breach Notification Rules are in addition to federal requirements and LifeMed ID must adhere to the strictest of those rules.

3. LifeMed ID's Vendor Contracting Officer, in consultation with the Privacy Officer, will ensure that all Business Associate (BA) and/or subcontractor contracts include specific requirements in compliance with breach notification requirements for:

    a. Policy and procedures for prompt notification to LifeMed ID and other requirements in compliance with state and federal regulations

    b. Workforce training, and

    c. Workforce sanctions for non-compliance.

4. In the event of a Breach of unsecured PHI or PII, LifeMed ID's Privacy Officer, in consultation with LifeMed ID's legal counsel, and in conjunction with LifeMed ID's donor, public and/or investor relations when appropriate, will oversee the notification of each individual whose unsecured PHI has been or is reasonably believed to have been breached, the Secretary and in some cases, appropriate major media outlets.

Procedures

1. In the event of a Breach by LifeMed ID or a BA or subcontractor of LifeMed ID [see Breach Notification Policy #2, Breach Risk Assessment], the Privacy Officer, in conjunction with LifeMed ID's legal counsel, will research state notification requirements and complete the following notification requirements, in addition to any more stringent state requirements than those that follow:

    a. Timeliness of Notification: Individual notifications will be provided without unreasonable delay and in no case later than 60 days following the discovery (Refer to definition of "discovery" in Definitions for Breach Notification Requirements) of a Breach unless:

        1) If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Privacy Officer shall:

i. If the statement is in writing, delay such notification, notice, or posting for the time period specified by the official; or

ii. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

b. Content of Notification: Notifications will include, to the extent possible,

1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known,

2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

c. Method of Notification: Individual Notice

1) The Privacy Officer will provide individual written notice(s) by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically and has not withdrawn that agreement.

2) If urgent notification is deemed necessary due to possible imminent misuse of the PHI, the Privacy Officer may additionally call the affected individual(s).

3) If the individual is deceased, the Privacy Officer will provide written notice(s) by first class mail to the address of the next of kin or Personal Representative of the individual, if available.

4) If LifeMed ID has insufficient or out-of-date contact information for 10 or more individuals, the Privacy Officer will provide substitute individual notice by either:

   i. Posting the notice on the home page of its web site for at least 90 days or

   ii. Providing notice in major print or broadcast media where the affected individuals likely reside.

   iii. In either case, the notices will include a toll-free phone number, active for at least 90 days, where an individual can be informed about the Breach.

d. Media Notice: If the Breach affects more than 500 residents of a State or jurisdiction, in addition to notifying the affected individuals, the Privacy Officer will provide notice, most likely in the form of a press release, to prominent media outlets serving the State or jurisdiction.

1) Timeliness of Notification: As with the individual notice(s), this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a Breach, subject to the same law enforcement delay requirements, and will include the same information required for the individual notice(s) unless State Law specifies otherwise.

e. Notice to the Secretary

1) Timeliness of Notification:

i. If a Breach affects 500 or more individuals, the Privacy Officer will notify the Secretary without unreasonable delay and in no case later than 60 days following a Breach, subject to the same law enforcement delay requirements.

ii. If a Breach affects fewer than 500 individuals, the Privacy Officer will maintain a log of Breaches and will provide notification to the Secretary of such Breaches occurring during the preceding calendar year, no later than 60 days after the end of the calendar year in which the Breaches occurred.

2) Content of Notification: The Privacy Officer will notify the Secretary by filling out and electronically submitting a Breach report form on the HHS website. (Refer to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)

f. Notification to State Authorities: The Privacy Officer will determine if the Breach meets additional reporting obligation under applicable State regulations that are not preempted by federal requirements and will comply with those reporting requirements, subject to the same law enforcement delay requirements.

g. Update Breach Log: The Privacy Officer will maintain the Breach Log with any new information uncovered in the investigation including the date of the Breach, the date of discovery, the number of persons affected, the source of the Breach (e.g. BA, Workforce member, etc.), the circumstances of the Breach, breach risk assessment, sanctions if applied, disposition of the breached information, mitigating actions to reduce chances of another Breach, notification details and dates.

h. Mitigation and Remediation Required Activities: (Refer to Breach Notification Policy #2, Breach Risk Assessment)

Regulatory Authority

§164.404 Notification to individuals.

(a) Standard

(1) *General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.*

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) Implementation specification: Timeliness of notification. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: *Content of notification*

(1) Elements. The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(2) Plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language.

(d) Implementation specifications: *Methods of individual notification. The notification required by paragraph (a) of this section shall be provided in the following form:*

(1) Written notice. (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) Additional notice in urgent situations. In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

§164.406 Notification to the media.

(a) Standard. *For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.*

(b) Implementation specification: *Timeliness of notification. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.*

(c) Implementation specifications: *Content of notification. The notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).*

§164.408 Notification to the Secretary.

(a) Standard. *A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.*

(b) Implementation specifications: *Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.*

(c) Implementation specifications: *Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.*

§164.410 Notification by a business associate.

(a) Standard.

(1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

(b) Implementation specifications: *Timeliness of notification. Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.*

(c) Implementation specifications: *Content of notification.*

(1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(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.

§164.412 Law enforcement delay.

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

References

Internal

1. Breach Notification Policy #2, Breach Risk Assessment

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

2. Instructions for Submitting Notice of a Breach to the Secretary: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html