Privacy Policy - Breach Notification

Policy Purpose

Organization takes the privacy and integrity of an individual's personal health information seriously. Organization also has legal responsibilities to protect PHI under HIPAA, to determine when there is a reportable breach of an individual's PHI and to make appropriate and timely notifications following a breach.

The purpose of this Breach Notification Policy is to meet Organization's responsibilities and to provide guidance to Organization workforce members regarding making required notifications when a Breach determination has been made under Privacy Policy - Breach Determination.

This policy establishes guidelines for Organization to

- Make, or assure the appropriate Covered entity or Business associate makes, appropriate notifications to individuals impacted by a Breach;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate notifications to federal and state authorities if required by the details of the Breach determination;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate notifications to media if the findings of the Breach determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of Breach notifications.

Policy Description

This policy establishes guidelines for Organization to

- Make, or assure the appropriate Covered entity or Business associate makes, appropriate timely notifications to individuals impacted by a Breach;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate timely notifications to federal and state authorities if required by the details of the Breach determination including reporting of breaches involving less than 500 individuals in a single state or geographic region to HHS electronically on an annual basis by March 1 (or February 29th in a Leap year) of the year following the Breach;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate timely notifications to media if the findings of the Breach determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice if required or desired;
- Ascertain and meet any more stringent applicable contractual notification requirements; and
- Document compliance with the requirements of this policy.

Following the determination of a breach under Privacy Policy - HIPAA incident Reporting and Response and Breach Determination Organization will determine what external notifications are required or should be made (i.e., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.), develop appropriate content for the notices, reports and postings, and communicate each notification, report or positing according to the procedures and requirements set forth below.

Procedures

Privacy and Security Officers Shall Direct all Notifications but may Appropriately Delegate Activities

With input from the Compliance Officer and others at their discretion, Organization’s Privacy and Security Officers will direct all activities required under this policy including the wording of any Individual Notices, HHS filings, communications required by contract, Media notices, and scripts (including escalation processes) for any telephone inquiries. Legal representation will be utilized if desired by the Privacy or Security Officer or at the direction of anyone on the senior leadership team of the Organization. The Privacy and Security Officer may delegate responsibilities as appropriate but remain responsible for the implementation of Breach Notification Policy requirements. This delegation includes allowing either another responsible Covered entity or a responsible Business associate to make the notifications. Organization remains responsible for assuring all requirements have been met by the delegated entity or individual. For responsibilities of Business associates, please refer to Privacy Policy - Business Associates for more information.

Organization will Determine Notification Requirements based on the findings of the Breach Incident Investigation.

Organization will use the Number of Individuals Involved to Determine Appropriate Notifications and Timing.

Individual Notification: If the number of individuals impacted by a breach is known to be less than 500, Organization will follow the notification Procedures set forth below for the timing and content of Individual Notification and Notification to HHS.

500 or More: If the number of individuals affected by the Breach is known to be 500 residents of a State or jurisdiction, Organization will provide notification to Prominent media outlets serving the State and regional area where the impacted individuals reside and follow the notification Procedures set forth below for the timing and content of Media Notice, HHS and Notification for Breaches Affecting more than 500 individuals.

If the number of individuals is uncertain, Organization must use reasonable efforts to estimate the number of affected individuals and document its methods. Organization shall use this estimate to determine the number of individuals affected for determining appropriate notification procedures. Should further information or investigation prove the estimate to be incorrect, Organization must update any previous notifications or reports made using that estimate if the method or content of the Notice is materially different due to the change.

See Chart below for Summary of Requirements. Details of Appropriate Notice, Timing, Content and Means appear below the summary chart.

IF	Notification To	Timing*	Content	Means of Notice

Number of Individuals impacted is less than 500	Each person individually	Without unreasonable delay and in no case later than 60 days following discovery of breach	In plain language A. A brief breach description, including date and the date of B. types of unsecured PHI that were involved C. steps the individual should take to protect themselves D. what the organization is doing to investigate, mitigate harm to individuals, and to protect against further Breaches; and E. Contact procedures	In writing by first class mail or by email if the affected individual has consented to such notice. Additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice Substitute notice**
	HHS	no later than 60 days after the end of the calendar year in which the Breaches were discovered (March 1 or February 29th in a leap year).	In addition to content required for individual notice, Information Required on Current HHS report includes Entity Contact, BA Contact if Occurred at BA, Number of individuals impacted, safeguards placed prior to breach, mitigation efforts, safeguards placed after breach, number of individuals impacted	Completion of online form on the HHS website

Number of Individuals Impacted is greater than 500 in any State or jurisdiction	Prominent Media Outlet serving the areas where impacted individuals reside	without unreasonable delay and in no case later than 60 days following the discovery of a Breach	In plain language: a. A brief breach description, including date and the date of b. types of unsecured PHI that were involved c. steps the individual should take to protect themselves d. what the organization is doing to investigate, mitigate harm to individuals, and to protect against further Breaches; and e. Contact procedures	Contact media and provide information to be included in publication
	HHS	without unreasonable delay and in no case later than 60 days following the discovery of a Breach	In addition to content required for media notice, Information Required on Current HHS report includes Entity Contact, BA Contact if Occurred at BA, Number of individuals impacted, safeguards placed prior to breach, mitigation efforts, safeguards placed after breach, number of individuals impacted	Completion of online form on the HHS website

*Subject to Law Enforcement requests for delay

**Substitute notice may be used in some situations for individuals, see policy for details.

Timing

1. Organization will provide Individual notice without unreasonable delay and in no case later than 60 days following the discovery of a Breach. The Organization may also provide additional notice in urgent situations because of possible imminent misuse of the PHI.
2. Organization will provide Media Notice, when required, without unreasonable delay and in no case later than 60 days following the discovery of a Breach.
3. Organization will provide HHS notice by completing a web report form on the following timeline:
    - If 500 or more individual residents of a State or jurisdiction are affected, Organization will complete the HHS notification without unreasonable delay and in no case later than 60 days following the discovery of a Breach.
    - If fewer than 500 individuals are affected, Organization will notify HHS of each Breach no later than 60 days after the end of the calendar year in which the Breaches were discovered (March 1 or February 29th in a leap year).

Discovery of Breach:

A breach of PHI shall be treated as “discovered” as of the first day the breach is known to the Organization, or, by exercising reasonable diligence would have been known to the Organization (includes breaches by Organization’s Business associates). The Organization shall be deemed to have knowledge of a breach if such breach is known or if by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or an agent of the Organization (i.e., a Business associate acting as an agent of the Organization).

Delays in Timing Permitted: Law Enforcement Delay

When Organization is notified by a law enforcement official that a notification, notice or posting required for a Breach would either impede a criminal investigation or damage national security, Organization may delay the notification, notice or posting for a) a period of time specified by the law enforcement official in writing or b) for the requested amount of time not to exceed 30 days from the date of an oral request for delay from a law enforcement official. Organization will extend the original 30-day delay imposed by an oral request if a law enforcement official makes a later request in writing prior to the expiration of the initial delay request. Any such oral or written request must be documented by Organization and the record preserved.

Workforce members should also refer to Privacy Policy - Verification of Identity and Authority when processing any law enforcement request for delay.

Content and Means of Notifications and Postings

At a minimum the content of reports, notifications and notices required by law for breaches of the privacy or security of PHI in any form must include the information set forth below and must be communicated by the means indicated:

Individual Notice: Means of Communication

In writing by first class mail or by email if the affected individual has consented to such notice. Reference the Sample Breach Notification format for all Individual Notice. If the Organization desires to send additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice but not as a substitute for it.

Substitute Individual Notice

When Organization has insufficient contact information for ten or greater affected individuals, Organization will give notice by posting notice for 90 days on the company website or by publication in major print or broadcast media in the area where the affected individuals likely reside.

When Organization has insufficient contact information for fewer than ten affected individuals it may give notice to those individuals by alternative written notice, by telephone or other reasonable means.

Individual Notice: Content

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 the individual should take to protect themselves from potential harm resulting from the Breach;
4. A brief description of what the Organization is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Media Notice Means of Communication and Content

For Media Notices the following information should be included and the Notice must include enough information for an individual to determine whether their information may have been disclosed, what they should do if it was and who to contact for more information:

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 the individual should take to protect themselves from potential harm resulting from the Breach;
4. A brief description of what the Organization is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Means of Notifying HHS

For a Breach Affecting 500 or More individuals Organization will timely complete a Notice utilizing the form on the HHS website (https://OCRportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true). For a Breach Affecting less than 500 Individuals Organization will timely file (within 60 days of the end of the calendar year in which the Breach occurred) a Notice utilizing the form on the HHS website (https://OCRportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true).

Reliance on Others to Provide Notification

Organization will determine any contractual obligations related to the PHI. If allowable, Organization may choose to rely upon notifications given by a business associate for the Breach notifications required. Organization will request copies of any notifications to its individuals, the public and HHS if Organization’s individual’s information was breached.

Record Keeping

Organization must keep records concerning all notifications, notices and postings made separately for each Breach reported. This includes any reports, notices or postings made by any other party on which Organization relied for its own notice to individuals, agencies, authorities, or media. These records must be kept for a minimum of six years following the provision of the notice, report or posting. If desired, utilize the Breach Notification Documentation Job Aid to record the details for recordkeeping.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.404 *Notification to Individuals*

45 CFR 164.406 *Notification to the Media*

45 CFR 164.408 *Notification to the Secretary*

45 CFR 164.410 *Notification by a Business Associate*

45 CFR 164.412 *Law Enforcement Delay*

45 CFR 164.414 *Administrative Requirements and Burden of Proof*

45 CFR 164.530 *Administrative Requirements*