HITECH Breach Notification Interim Final Rule

HHS issued regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached.

These “breach notification” regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The regulations, developed by the Office of Civil Rights OCR for the Department of Health and Human Services, require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

These regulations ensure that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care.

Part II
Department of Health and Human Services
45 CFR Parts 160 and 164
Breach Notification for Unsecured
Protected Health Information; Interim Final Rule

https://www.govinfo.gov/content/pkg/FR-2009-08-24/pdf/E9-20169.pdf

---

DEPARTMENT OF HEALTH AND HUMAN SERVICES

45 CFR Parts 160 and 164

Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

---

Template: Health Information Privacy and Security Breach Notification Letter

DISCLAIMER

This tool is intended to serve as a guide and does not seek to dictate content and format or disavow other content and format advice.

This federal rule1 requires the breach message to be presented at an appropriate reading level and in clear language and syntax. To ensure the letter is adequate to be helpful, no length constraints are directed. However it should not include extraneous material detracting from the message.

The letter is approached in three stages:

1. Required elements must be addressed in a customized manner according to situational circumstances:

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 the individual should take to protect themselves from potential harm resulting from the breach

D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches

E. 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

2. Elements for customized inclusion if appropriate:

A. Recommendations that the individual contact his or her credit card company and information about how to contact the credit bureaus and obtain credit monitoring services (if credit card information was breached)

B. Information about steps the covered entity is taking to retrieve the breached information, such as filing a police report (if a suspected theft of unsecured protected health information occurred)

C. Information about steps the covered entity is taking to improve security to prevent future similar breaches

D. Information about sanctions the covered entity imposed on workforce members involved in the breach

3. Required or desired elements to be identified by the responsible healthcare organization according to specific state laws, applicable federal regulations, and organizational policy.

Italics are used in the template document to indicate variables—those areas needing an organization's substitution of specific facts, choices, options, and special considerations. Additional content may be further required or desired depending on setting, state, federal, and organization nuances specified in number three above.

All HIPAA covered entities must familiarize themselves with the HIPAA breach notification requirements and develop a breach response plan that can be implemented as soon as a breach of unsecured protected health information is discovered.

While most HIPAA covered entities should understand the HIPAA breach notification requirements, organizations that have yet to experience a data breach may not have a good working knowledge of the requirements of the Breach Notification Rule. Vendors that have only just started serving healthcare clients may similarly be unsure of the reporting requirements and actions that must be taken following a breach.

The issuing of notifications following a breach of unencrypted protected health information is an important element of HIPAA compliance. The failure to comply with HIPAA breach notification requirements can result in a significant financial penalty. With this in mind, we have compiled a summary of the HIPAA breach notification requirements for covered entities and their business associates.

Summary of the HIPAA Breach Notification Requirements

The HIPAA Breach Notification Rule – 45 CFR §§ 164.400-414 – requires covered entities and their business associates to report breaches of electronic protected health information and physical copies of protected health information. A breach is defined as the acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA Rules.

HIPAA breaches include

- unauthorized access by employees as well as third parties,
- improper disclosures,
- the exposure of protected health information, and
- ransomware attacks.

Exceptions include:

- Breaches of secured protected health information such as encrypted data when the key to unlock the encryption has not been obtained;
- “any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a

business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure;"

- An inadvertent disclosure by a person who is authorized to access PHI, to another member of the workforce at the organization who is also authorized to access PHI;
- When the covered entity or business associate makes a disclosure and has a good faith belief that the information could not have been retained by the person to whom it was disclosed.

In the event of a reportable HIPAA breach being experienced, the HIPAA breach notification requirements are:

- Notify Individuals Impacted – or Potentially Impacted – by the Breach
- All individuals impacted by a data breach, who have had their protected health information accessed, acquired, used, or disclosed, must be notified of the breach.
- Breach notifications are also required for any individual who is reasonably believed to have been affected by the breach.

Breach notification letters must be sent within 60 days of the discovery of a breach unless a request to delay notifications has been made by law enforcement. In such cases, notifications should be sent as soon as that request has expired. While it is permissible to delay reporting of a breach to the HHS for breaches impacting fewer than 500 individuals (see below), that delay does not apply to notifications to breach victims.

Breach notification letters should be sent by first class mail to the last known address of breach victims, or by email if individuals have given authorization to be contacted electronically.

The HIPAA breach notification requirements for letters include

- writing in plain language,
- explaining what has happened,
- what information has been exposed/stolen,
- providing a brief explanation of what the covered entity is doing/has done in response to the breach to mitigate harm,
- providing a summary of the actions that will be taken to prevent future breaches, and

- giving instructions on how breach victims can limit harm.
- Breach victims should also be provided with a toll-free number to contact the breached entity for further information, together with a postal address and an email address.

Notify the Department of Health and Human Services

Notifications must be issued to the Secretary of the Department of Health and Human Services, via the Office for Civil Rights breach reporting tool.

The HIPAA breach notification requirements differ depending on how many individuals have been impacted by the breach.

- When the breach has impacted more than 500 individuals, the maximum permitted time for issuing the notification to the HHS is 60 days from the discovery of the breach, although breach notices should be issued without unnecessary delay.

- In the case of breaches impacting fewer than 500 individuals, HIPAA breach notification requirements are for notifications to be issued to the HHS within 60 days of the end of the calendar year in which the breach was discovered.

Notify the Media

HIPAA breach notification requirements include issuing a notice to the media. Many covered entities that have experienced a breach of protected health information notify the HHS, relevant state attorneys general, and the patients and health plan members impacted by the breach, but fail to issue a media notice – a violation of the HIPAA Breach Notification Rule.

A breach of unsecured protected health information impacting more than 500 individuals must be reported to prominent media outlets in the states and jurisdictions where the breach victims reside – See 45 CFR §§ 164.406. This is an important requirement, as up-to-date contact information may not be held on all breach victims. By notifying the media, it will help to ensure that all breach victims are made aware of the potential exposure of their sensitive information. As with the notifications to the HHS and breach victims, the media notification must be issued within 60 days of the discovery of the breach.

Post a Substitute Breach Notice on the Home Page of the Breach Entity's Website

In the event that up-to-date contact information is not held on 10 or more individuals that have been impacted by the breach, the covered entity is required to upload a substitute breach notice to their website and link to the notice from the home page. The link to the breach notice should be displayed prominently and should remain on the website for a period of 90 consecutive days. In cases where fewer than 10 individuals' contact information is not up-to-date, alternative means can be used for the substitute notice, such as a written notice or notification by telephone.

Data Breaches Experienced by HIPAA Business Associates

Business associates of HIPAA-covered entities must also comply with the HIPAA breach notification requirements and can be fined directly by the HHS' Office for Civil Rights and state attorneys general for a HIPAA Breach Notification Rule violation.

Any breach of unsecured protected health information must be reported to the covered entity within 60 days of the discovery of a breach. While this is the absolute deadline, business associates must not delay notification unnecessarily. Unnecessarily delaying notifications is a violation of the HIPAA Breach Notification Rule.

It is usually the covered entity that will issue breach notifications to affected individuals, so any breach notification will need to be accompanied with details of the individuals impacted. It is a good practice to issue a breach notification to a covered entity rapidly, and to provide further information on the individuals impacted once the investigation has been completed. Under the terms of a HIPAA-compliant Business Associate Agreement (BAA), a business associate may be required to issue breach notifications to affected individuals.

Timeline for Issuing Breach Notifications

Breach notifications should be issued as soon as possible and no later than 60 days after the discovery of the breach, except when a delay is requested by law enforcement. Investigating a breach of protected health information can take some time, but once all the necessary information has been obtained to allow breach notifications to be sent they should be mailed.

HIPAA-covered entities must not delay sending breach notification letters. It is possible to receive a HIPAA violation penalty for delaying notifications, even if they are sent

within 60 days of the discovery of the breach. There have been several recent cases of HIPAA breach notification requirements not being followed within the appropriate time frame, which can potentially result in financial penalties.

State Breach Notification Laws May Be Stricter than HIPAA

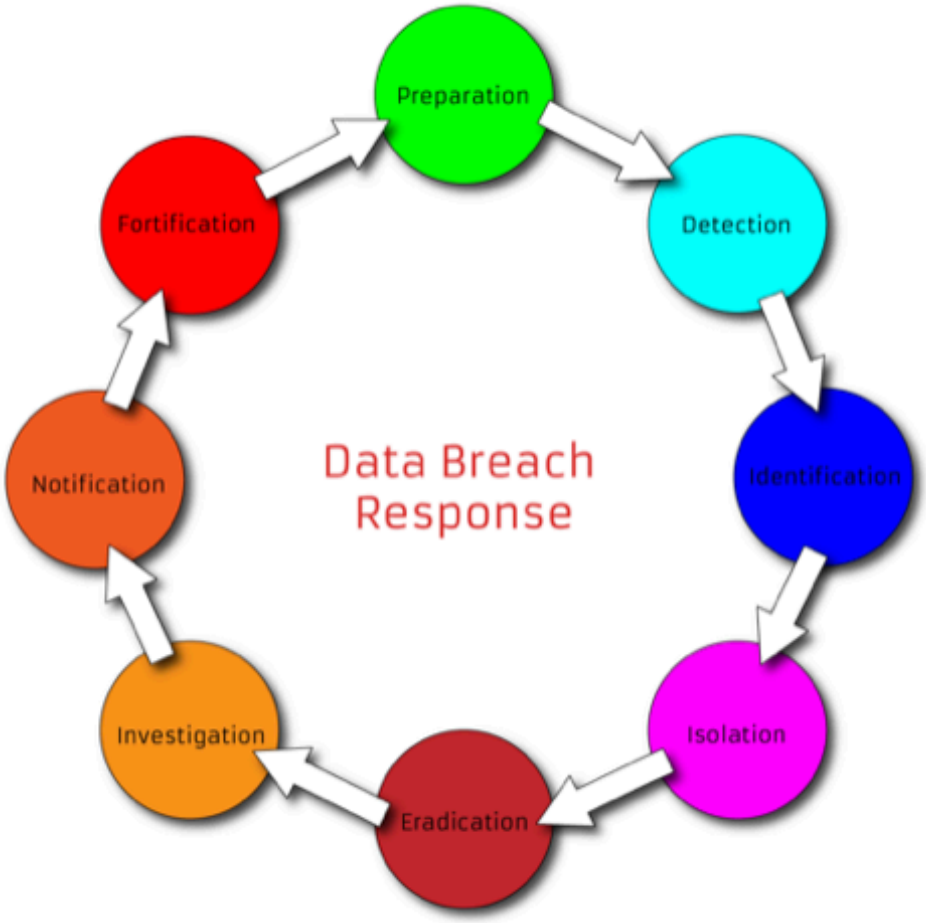
U.S. states have their own breach notification laws. Typically, notifications must be issued to breach victims promptly and a notice also submitted to the state attorney general's office. Some states require breach notifications to be issued well within the HIPAA deadline.

Delaying breach notifications until the 60-day limit of HIPAA could well see state laws violated, leading to financial penalties from state attorneys general. State laws frequently change so it is important to keep up to date on breach notification laws in the states in which you operate.

Penalties for Violations of HIPAA Breach Notification Requirements

HIPAA covered entities must ensure the HIPAA breach notification requirements are followed or they risk incurring financial penalties from state attorneys general and the HHS' Office for Civil Rights.

In 2017, Presense Health became the first HIPAA-covered entity to settle a case with the Office for Civil Rights solely for a HIPAA Breach Notification Rule violation – after it exceeded the 60-day maximum time frame for issuing breach notifications. Presense Health took three months from the discovery of the breach to issue notifications – A delay that cost the health system $475,000. The maximum penalty for a HIPAA Breach Notification Rule violation is $1,500,000, or more if the delay is for more than 12 months.



Responding to a Healthcare Data BreachSource: HIPAA JOURNAL

https://www.hipaajournal.com/wp-content/uploads/2015/10/how-to-respond-to-a-healthcare-data-breach.png

> *However, the damage caused by malware and hackers can be severely restricted. Damage limitation is the name of the game, and preparation is key.*
>
> *When hackers break through the security perimeter, or when malware is discovered, you must be able to act immediately. You must therefore develop and test a data breach response plan.*

1. Preparation

It is essential that protections are put in place to prevent a cyberattack, but a security perimeter breach is still likely to occur. When that happens all staff members must know their roles and responsibilities. Your breach response plan needs to be actioned immediately. In order to prevent problems, your response plan must be tried and tested.

2. Detection

Hackers may already be inside your network. Malware may have been installed. It is essential that networks are routinely, and regularly scanned for potential breaches. The sooner a security breach is discovered, the less damage is likely to be caused. Law enforcement agencies must also be notified rapidly. Their input may influence your breach response.

3. Identification

Who is the perpetrator? Where is the attack coming from? What are you dealing with? Why has access been gained? It is essential to know thy enemy in order to determine the best method for isolating and neutralizing the threat.

4. Isolation

Shut down all compromised systems to contain an attack or malware infection. It is essential to stop data access rapidly, and prevent the exfiltration of PHI/PHI. The initial point of attack may not be the only part of a system that has been compromised. Check all systems/ equipment and determine if others areas of the network have also been compromised.

5. Eradication

Even if access to data has been gained, it may not be too late to prevent information from being exfiltrated, but before access/infections are eradicated, ensure a data backup has been performed. Data loss must be prevented. A thorough system disinfection must then take place. Back doors must be found and shut down.

6. Investigation

A forensic data analysis should be conducted to find out exactly how data were exposed and the extent of an attack. Seek help from external data security experts and take the opportunity to perform a thorough risk assessment to identify new security vulnerabilities that may exist.

9. Preparation

After suffering a data breach you must prepare for subsequent attacks. Assess what elements of your breach response worked well, and what didn't. Make improvements, develop new policies as necessary, and test those policies and procedures to ensure they work in practice.

7. Notification

You have 60 days to issue breach notification letters to victims and to report the security breach to the OCR but do not delay the breach response unnecessarily. State attorneys general must also be notified. Make sure you are aware of the timescales for doing so, state by state. Fast issuing of notifications can reduce the fallout from a data breach.

8. Fortification

Data security defenses must be fortified, and all security holes plugged. Government regulatory bodies will expect to see security vulnerabilities addressed rapidly following a breach of PHI. A data breach may not warrant a HIPAA fine, but a failure to address security risks will.

Sample HIPAA Breach Notification Letter

[Patient Name] [Patient Address]

Dear [Patient]:

We are sending this letter to you as part of [Provider]'s commitment to patient privacy. We take patient privacy very seriously, and it is important to us that you are made fully aware of a potential privacy issue. We have learned that your personal information, including name, address, _____, _____, and _____, may have been compromised. On [give date of discovery], it was discovered that [describe incident and give date of breach]. We reported the incident to the police because theft may have been involved [if applicable]. However, we have not received any indication that the information has been accessed or used by an unauthorized individual.

[Describe steps patient should take to protect themselves:]

We are keenly aware of how important your personal information is to you. If you choose, as a measure of added security, we are offering one year of credit monitoring and reporting services at no cost to you. This service is performed through [Vendor], an organization that watches for and reports to you unusual credit activity, such as creating new accounts in your name. [Vendor] will also request that the three credit bureaus place a "Fraud Alert" on your credit report. If you would like to receive this service, please respond yes by _____ or _____.

We understand that this may pose an inconvenience to you. We sincerely apologize and regret that this situation has occurred. [Provider] is committed to providing quality care, including protecting your personal information, and we want to assure you that we have policies and procedures to protect your privacy.

If you want to take advantage of the free credit monitoring service, or if you have any questions, please contact [Phone Number].

Sincerely,