# Breach Notification Requirements for Unsecured PHI

The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to notify affected individuals following the discovery of a **breach of unsecured protected health information (PHI)**. Notification must also be provided to the Department of Health and Human Services (HHS), and, in some cases, to the media.

An impermissible use or disclosure of unsecured PHI is presumed to be a breach unless the covered entity demonstrates through a risk assessment that there is a **low probability** that the PHI has been compromised. “Unsecured PHI” is PHI that is not secured through the use of a technology or methodology specified by HHS. HHS has specified **encryption and destruction** as the two technologies and methodologies for securing PHI.

Covered entities should **review their HIPAA policies** to make sure that they address the breach notification requirements, including the factors that must be considered when determining whether a breach has occurred.

## LINKS AND RESOURCES

- HHS' final rule on the breach notification requirements
- HHS’ webpage on HIPAA’s breach notification requirements
- HHS' breach notification portal, which includes a list of covered entities that experience breaches of unsecured PHI that involve more than 500 individuals.

### Breach Notification

Following a breach of unsecured PHI, a covered entity must notify:

- The individuals whose PHI was accessed, acquired, used or disclosed due to the breach;
- HHS; and
- The media, for breaches involving more than 500 residents of a state or jurisdiction.

### Unsecured PHI

- The breach notification requirements only apply to unsecured PHI.
- Encryption and destruction are the two methods for securing PHI.
- If a covered entity (or business associate) has used encryption or destruction to secure PHI, the PHI is not considered unsecured.

## WHAT IS A BREACH?

The HITECH Act defines a “breach” as the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the information. There are three exceptions to this definition.

### Three Exceptions

- Disclosures where the recipient of the information would not reasonably have been able to retain the information;
- Certain unintentional acquisition, access or use of information by employees or others acting under the authority of a covered entity or business associate; and
- Certain inadvertent disclosures among people similarly authorized to access PHI at a business associate or covered entity.

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates through a **risk assessment** that there is a **low probability that the PHI has been compromised** (or one of the three exceptions to the definition of breach applies). The risk assessment must, at a minimum, take into account these factors:

- The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

If an evaluation of the factors fails to demonstrate that there is a low probability that PHI has been compromised, **breach notification is required**.

### WHAT IS UNSECURED PHI?

Under the HITECH Act, "unsecured PHI" is PHI that is not secured through the use of a technology or methodology specified by HHS in guidance. The HITECH Act directed that the HHS guidance should specify the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. HHS' guidance describes encryption and destruction as the two technologies and methodologies for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals.

Covered entities and business associates that implement the specified technologies and methodologies with respect to PHI are not required to provide notification in the event of a breach of that information because the information is not considered "unsecured PHI." The breach notification requirements apply only to unsecured PHI.

## NOTIFICATION TO INDIVIDUALS

### General Rule

If a covered entity discovers that it has experienced a breach of unsecured PHI, it must notify each individual whose unsecured PHI has been (or is reasonably believed by the covered entity to have been) accessed, acquired, used or disclosed as a result of the breach. The notice must be provided without unreasonable delay and in no case later than **60 calendar days** after the breach is discovered.

A breach is considered discovered on the first day that the covered entity knows about the breach, or would have known about it if it had been exercising reasonable diligence. The covered entity is deemed to know about the breach if an employee or agent (other than the person committing the breach) is aware of it.

### Content of Notice

The notice must be written in plain language and must contain the following information:

- A brief description of what happened, including the dates the breach occurred and was discovered, if known;
- A description of the types of unsecured PHI that were involved, such as names, Social Security numbers or other types of information;
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, mitigate harm to individuals and protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, website or postal address.

### Method of Notice

In general, notice must be provided in writing, by first-class mail to the individual's last known address. Notice can be sent electronically if the individual has agreed to electronic notice. If the individual is deceased, written notice should be provided to the next of kin or personal representative, if the covered entity has that person's address.

If written notice is not possible because of insufficient or out-of-date contact information for the individual, a substitute notice may be used. If the covered entity does not have contact information for a group of fewer than 10 individuals, the substitute notice may be provided by an alternate form of written notice, telephone or other means. If the group is 10 or more, the covered entity must conspicuously post the notice (including a toll-free number for questions) for 90 days on the home page of its website or must publish a conspicuous notice in major print or broadcast media in areas where affected individuals likely reside.

### Notice in Urgent Situation

In a case that requires urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide notice by telephone or other means.

### NOTIFICATION TO HHS

Covered entities must notify HHS of a breach of unsecured PHI. However, the notification required depends on the size of the group affected.

| | |
|---|---|
| Breaches involving fewer than 500 individuals | The covered entity must maintain a log or other documentation of the breaches. Within 60 days after the end of each calendar year, the covered entity must notify HHS of the breaches that occurred during the year. |
| Breaches involving 500 or more individuals | The notice must be provided at the same time as the notice to the individuals and in the manner specified on the HHS website. |

## NOTIFICATION TO THE MEDIA

If the breach of unsecured PHI involves more than **500 residents** of a state or jurisdiction, the covered entity must notify "prominent media outlets" that serve that area. The notice must include the same information as a notice to an individual. It must be provided without unreasonable delay and in no case later than 60 calendar days after the breach is discovered.

## NOTIFICATION BY A BUSINESS ASSOCIATE

If a business associate discovers a breach of unsecured PHI, it must notify the covered entity of the breach. Notification must be provided without unreasonable delay and no later than 60 calendar days after the breach is discovered. The notice must include, to the extent possible, the identification of each individual whose unsecured PHI has been affected. The business associate must also give the covered entity any information necessary to notify the individual of the breach.

## LAW ENFORCEMENT DELAY

There are instances where notification may have to be delayed due to law enforcement needs. For example, a law enforcement official may find that a required breach notification could impede a criminal investigation or cause damage to national security. If the official provides a written statement specifying the time for which a delay is required, the covered entity or business associate must delay the notice until the date specified. If the statement is made orally, the covered entity or business associate must document the statement (including the official's identity) and delay the notification temporarily, but no longer than 30 days. If a written statement is received later, the notice can be delayed as specified in the statement.

## ADMINISTRATIVE REQUIREMENTS

Covered entities must incorporate compliance with the breach notification requirements into their administrative duties under the HIPAA Privacy and Security Rules. Covered entities must also provide a complaint process and apply appropriate sanctions for failures to comply with its policies. Covered entities may not intimidate or retaliate against individuals for exercising their rights under the breach notification rule and may not require individuals to waive those rights.

Covered entities and business associates have the burden of demonstrating that all notifications were provided or that an impermissible use or disclosure did not constitute a breach, and must maintain documentation to meet the burden of proof.