Breach Notification Rule

The HIPAA Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI).

What is a "Breach"?

HIPAA defines a **"breach"** as, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI.

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised, based on a risk assessment of at least the following factors:

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

There are **three exceptions** to the HIPAA definition of breach:

1. The **unintentional** acquisition, access, or use of PHI made in good faith and within the scope of authority.
2. The **inadvertent** disclosure of PHI by a person authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate.
3. If the covered entity or business associate has a **good faith belief** that the unauthorized person to whom the disclosure was made would not have been able to retain the information.

Breach Notification Requirements

Following a breach of unsecured PHI, covered entities must provide notification of the breach to **affected individuals**, **HHS**, and, in certain circumstances, to **the media**. If a breach occurs at or by a business associate, the business associate must notify the covered entity **no later than 60 days** from the discovery of the breach.

Notice to Affected Individuals

Covered entities must notify affected individuals of the breach by first-class mail or by email, if the affected individual has agreed to receive such notices electronically. These individual notifications must be provided without unreasonable delay and in no case later than **60 days** following the discovery of a breach and must include, to the extent possible:

- A brief description of the breach;
- A description of the types of information that were involved in the breach;
- The steps affected individuals should take to protect themselves from potential harm;
- A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
- Contact information for the covered entity (or business associate, as applicable).

If the covered entity has insufficient or out-of-date contact information for **10 or more individuals**, the covered entity must post the notice on the home page of its website for at least 90 days **or** provide the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days, where individuals can learn if their information was involved in the breach.

If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate.

Notice to HHS

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the U.S. Department of Health and Human Services of breaches of unsecured PHI by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects **500 or more individuals**, covered entities must notify HHS without unreasonable delay—and in no case later than **60 days**—following the breach. Covered entities may notify HHS annually of breaches involving **fewer than 500 individuals**, no later than **60 days after the end of the calendar year** in which the breaches are discovered.

Notice to the Media

Covered entities that experience a breach affecting **more than 500 residents** of a State or jurisdiction are required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. This media notification must be provided without unreasonable delay and in no case later than **60 days** following the discovery of a breach, and must include the same information required for the notice to affected individuals (see above).

Administrative Requirements

Covered entities and business associates should **maintain documentation** that all required notifications of the use or disclosure of unsecured PHI were made, or alternatively, documentation to demonstrate that notification was not required.

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities **must** have in place written policies and procedures regarding breach notification, train employees on these policies and procedures, and develop and apply appropriate sanctions against workforce members who do not comply with them.

Click here for more information on the Breach Notification Rule.

Additional Information

- HHS Cyber-Attack Checklist