

Legislative Brief

Breach Notification for Unsecured PHI: HHS Interim Final Rule



On August 24, 2009, the Office of Civil Rights (OCR) issued an interim final rule (Breach Notification Rule) to require notification of breaches of unsecured Protected Health Information (PHI). OCR is the part of the Department of Health and Human Services (HHS) responsible for enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. The Breach Notification Rule applies to breaches of unsecured PHI that occur on or after **September 23, 2009**.

This issue of the Wine Sergi & Co, LLC Legislative Brief describes the background and main points of the Breach Notification Rule.

Background

HITECH Act Requirements

HHS was directed to issue the Breach Notification Rule by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was part of the American Recovery and Reinvestment Act of 2009. The breach notification provisions of the HITECH Act apply to HIPAA Covered Entities and Business Associates that access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHI.

The HITECH Act requires HIPAA Covered Entities to provide notification to affected individuals and to HHS following the discovery of a breach of unsecured PHI. In some cases, Covered Entities must also notify the media. In the case of a breach of unsecured PHI by a Covered Entity's Business Associate, the Business Associate must notify the Covered Entity of the breach. The Act also requires HHS to post on its website a list of Covered Entities that experience breaches of unsecured PHI that involve more than 500 individuals.

What is a Breach?

The HITECH Act defines a "breach" to mean the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information.

There are some exceptions to this definition:

- Disclosures where the recipient of the information would not reasonably have been able 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.

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 issued guidance on April 17, 2009 that described **encryption** and **destruction** as the two technologies and methodologies for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals. The Breach Notification Rule updates that guidance. The guidance is available at www.hhs.gov/ocr/privacy/.

NOTE: 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 Rule applies only to unsecured PHI.

Legislative Brief

Breach Notification for Unsecured PHI: HHS Interim Final Rule

Definitions

The Breach Notification Rule provides some additional information with respect to the definition of “breach” described above. The Rule states that a breach will compromise the security or privacy of PHI if it poses a significant risk of financial, reputational or other harm to the individual. The Rule also clarifies that a use or disclosure of PHI that does not include certain identifying information such as name, address and identification numbers, along with date of birth and zip code, does not compromise the security or privacy of the 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, Web site 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 Web site or must publish 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 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.

Legislative Brief

Breach Notification for Unsecured PHI: HHS Interim Final Rule

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. For 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 Web site. For breaches involving less 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 provide notification to HHS of the breaches that occurred during the year.

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 notification required under the Breach Notification Rule 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 Rule into their administrative duties under the HIPAA Privacy and Security Rules. For example, Covered Entities must implement policies and procedures that are designed to comply with the Breach Notification Rule and must train their workforce appropriately. 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.

Please contact your Wine Sergi & Co, LLC representative with any questions regarding the Breach Notification Rule.

This Wine Sergi & Co, LLC Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content © 2009 Zywave, Inc. Images © 2000 Getty Images, Inc. All rights reserved.

EAS 8/09