



HIPAA Breach Notification Requirements

Background

Most employers know that the health plans they sponsor are subject to HIPAA Privacy and Security Rules and know that HIPAA applies in different ways depending on if an employer's plan is fully insured or self-funded. However, even small employers offering fully insured medical and dental plans, have significant HIPAA responsibilities if they offer a Section 125 health flexible spending account (HFSA) or a Health Reimbursement Account (HRA). HIPAA treats HFSA's and HRAs as self funded medical plans.

The American Recovery and Reinvestment Act (ARRA) passed in February 2009 contains a number of changes to HIPAA. One of the more significant new requirements is contained in a section of ARRA called The Health Information Technology for Economic and Clinical Health (HITECH) Act.

HITECH requires that when there has been a "breach" of unsecured Protected Health Information (PHI), covered entities must provide notification to affected individuals, the Department of Health and Human Services (HHS), and sometimes to the media. The Act also requires the HHS to develop a web site with a list of covered entities that experience breaches of unsecured PHI involving more than 500 individuals.

HHS published an interim final rule regarding the breach notification rules on Monday, August 24th, making the effective date of these regulations September 23rd, 2009. Considering the extremely short time between the publishing of the rules and their effective date, employers should review and update existing HIPAA policies to comply with these rules as soon as possible.

What is a Breach?

Definition of a Breach

HHS defines a breach as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI." (For clarity purposes this summary will refer simply to "uses" of PHI in place of the technical definition). For an incident to be considered a breach, it must be a violation of the HIPAA Privacy Rule. However, not all violations of the Privacy Rule will be breaches. HHS provides the example that violations of HIPAA administrative requirements, such as a lack of reasonable safeguards or a lack of training, do not themselves qualify as breaches, although such violations may lead to a breach.

The Act and regulations limit the definition of breach to a use or disclosure that "compromises the security or privacy" of the PHI. According to the HHS an incident must pose a significant risk of financial, reputational, or other harm to the individual to be considered a breach.

To determine if a use of PHI constitutes a breach, HHS instructs organizations to perform a risk assessment to determine if there is a significant risk of harm to the individual. In performing the risk assessment, covered entities and business associates should consider factors such as:

- Who impermissibly used or to whom was the information impermissibly disclosed?
- Did the entity take steps to mitigate an impermissible use or disclosure?
- Was the PHI is returned or recovered prior to it being accessed for an improper purpose?

HHS goes on to explain that "in performing a risk assessment, covered entities and business associates should also consider the type and amount of PHI involved in the impermissible use. If the nature of the PHI does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach."

Exceptions to a Breach

The Act also includes three exceptions to the definition of breach:

- (1) Unintentional use of PHI by an employee or individual acting under the authority of a covered entity or business associate;
- (2) Inadvertent disclosure of PHI from one person authorized to access PHI at a covered entity or business associate to another similarly situated person authorized to access PHI at the covered entity or business associate;
- (3) Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

HHS summarizes that covered entities and business associates will need to do the following to determine whether a breach occurred:

- First, the covered entity or business associate must determine whether there has been an impermissible use or disclosure of PHI under the Privacy Rule.
- Second, the covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the PHI. This occurs when there is a significant risk of financial, reputational, or other harm to the individual.
- Lastly, the covered entity or business associate may need to determine whether the incident falls under one of the exceptions to the breach definition.

Unsecured Protected Health Information

The Act defines “unsecured PHI” as “PHI that is not secured through the use of a technology or methodology specified by the (HHS) in guidance”. This guidance was issued on April 17, 2009, and later published in the Federal Register on April 27, 2009.

The guidance specified encryption and destruction as the technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable. Note that this rule does not require the use of encryption or destruction when dealing with all PHI; rather it provides a “safe harbor” from the notice requirement. For example, if properly encrypted PHI is lost, the entity is not required to comply with the breach notification requirements.

Notice Requirements

Notice to the Individual

A covered entity must notify each individual whose unsecured PHI has been breached. The breach is considered “discovered” as of the first day the breach is known by the covered entity. The notice must be sent “without unreasonable delay” but in no case later than 60 days after the discovery of the breach.

HHS points out that “Covered entities should ensure their workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.

The Act requires the notification to include, to the extent possible, the following elements:

- (1) A brief description of what happened, including the date of the breach;
- (2) A description of the types of unsecured PHI that were involved in the breach;
- (3) Any steps individuals should take to protect themselves from potential harm;
- (4) A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and
- (5) Contact information for individuals to ask questions.

The Act requires written notice be sent to the individual by first-class mail at the last known address. The notice may be sent by email only if the individual has previously agreed to receive electronic notices and such agreement has not been withdrawn.

If a covered entity does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, the covered entity must provide substitute notice for the unreachable individuals. If 10 or more individuals are involved, the covered entity must provide a substitute notice through either a conspicuous posting on the home page of its web site or conspicuous notice in major print or broadcast media.

Notice to the Media and HHS

If a breach involves more than 500 individuals in a state, the Act requires that notice be provided to prominent media outlets serving the area. Obviously, notification to the media creates significant PR issues, and there are a number of requirements regarding the form of this notice. Covered Entities are advised to seek professional assistance if faced with the prospect of notifying the media of this type of breach.

For breaches involving 500 or more individuals, the Act also requires covered entities to notify HHS immediately. For breaches involving less than 500 individuals, the Act requires a covered entity to maintain a log of such breaches and annually submit such log to the HHS.

Additional Requirements

Business Associates

The Act requires a business associate of a covered entity to notify the covered entity when it discovers a breach of PHI and requires business associates, to the extent possible, to provide covered entities with the identity of each individual whose PHI has been breached. Covered entities may wish to address the timing of the notification in their business associate contracts.

Administrative Requirements

The regulations require covered entities and business associates to develop and document policies and procedures related to these breach notification rules. HHS specifically lists a number of actions entities should take including:

- Train workforce members on, and have sanctions for failure to comply with, the organizations breach policies and procedures
- Permit individuals to file complaints regarding these policies or a failure to comply with them
- Refrain from intimidating or retaliatory acts

Finally HHS makes clear that, following an impermissible use or disclosure under the Privacy Rule, covered entities and business associates have the burden of demonstrating that all notifications were made as required.

Summary

While the Breach Notification Rules are getting the most attention, other changes to HIPAA this year include a number of technical changes and the requirement that HHS increase enforcement of HIPAA rules and regulations. At a minimum, employers should take these changes seriously and review and update existing HIPAA Privacy and Security policies including training employees responsible for the administration of the employer's health plans on the rules.

For more information contact W.J. Flynn and Associates, LLC at 651-287-2371 or bob.radecki@wjflynnandassociates.com.

While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept liability for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it. This publication is distributed on the understanding that the publisher is not engaged in rendering legal, accounting or other professional advice or services. Readers should always seek professional advice before entering into any commitments.