



September 2009

EMPLOYEE BENEFITS & EXECUTIVE COMPENSATION UPDATE

New Health Information Breach Notification Requirements Effective September 23: Will You Be Ready?

As stated in our March 2009 bulletin (www.ThompsonHine.com/publications/publication1737.html), the American Recovery and Reinvestment Act of 2009, signed into law on February 17, 2009, changes the privacy and security requirements applicable to protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). On August 24, 2009, the Department of Health and Human Services (HHS) published final interim regulations on the requirements for notification upon a breach of "unsecured" PHI. These regulations apply to both covered entities (group health plans, certain health care providers and health care clearinghouses) and their business associates. The regulations are effective for breaches that occur on or after September 23, 2009; however, HHS will not impose sanctions for failure to provide the required notifications for breaches that are discovered before February 22, 2010.

Following is a summary of the regulations regarding the new requirements for notification if a "breach" of "unsecured" PHI occurs.

HAS A BREACH OCCURRED?

To determine whether a breach has occurred, the covered entity or business associate who committed the potential breach must take the following three steps:

- Verify whether there has been an acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rules. If there has been no breach of the HIPAA Privacy Rules, no notification is required.

Information that has been de-identified in accordance with the HIPAA Privacy Rules is not considered PHI, so a use or disclosure of the de-identified information would not generate a notice requirement.

- Determine whether the impermissible use or disclosure compromises the security or privacy of the PHI. In order for the privacy or security of PHI to be compromised, the impermissible use or disclosure must pose a significant risk of financial, reputational or other harm to the individual.

The covered entity or business associate must perform a risk analysis based on the specific facts of the situation. The facts considered and conclusions drawn must be documented and retained in the entity's HIPAA files for at least six years.

In determining whether there has been a compromise to the privacy or security of PHI, the covered entity or business associate should consider:

- Who impermissibly used the PHI or to whom the PHI was impermissibly disclosed; and



- The type and amount of PHI involved in the impermissible use or disclosure.

For example, a covered entity violates the HIPAA Privacy Rule if it improperly discloses PHI that merely includes the name of an individual and the fact that the individual received services from a hospital. However, that violation may not constitute a significant risk of financial or reputational harm to the individual. The risk of harm (and the likelihood of a breach) would be greater if the information indicates the types of services received or includes information that increases the likelihood of identity theft.

- Establish whether the incident falls under one of the following exceptions:
 - Unintentional acquisition, access or use of PHI by an employee or individual acting in good faith under the authority of a covered entity or business associate;
 - Inadvertent disclosure of PHI from one person authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate; and
 - Unauthorized disclosure in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

WHEN IS PHI UNSECURED?

PHI is considered unsecured if it is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption or destruction of the information as described in HHS guidance.

There is no requirement that a covered entity or business associate comply with the HHS standards for destruction and encryption. For example, a covered entity may reasonably choose to use firewalls and access controls to make PHI inaccessible for purposes of the HIPAA Security Rules. However, because the HHS standards are not used in this example, the PHI is considered unsecured and any breach of that PHI generates a notice requirement.

WHAT ARE THE REQUIRED NOTIFICATIONS?

If a covered entity or business associate determines that a breach of unsecured PHI has occurred, notification must be sent:

- To individuals affected by the breach of unsecured PHI;
- To the Secretary of HHS;
- To the media, in certain circumstances; and
- To the covered entities whose individuals are affected by the breach, if a business associate has committed the breach.



The covered entity is responsible for notifying the individual, even if the breach was committed by a business associate. However, covered entities and business associates may negotiate for the business associate to provide the notification.

Notification to Individuals

Covered entities must notify individuals as soon as reasonably possible and without unreasonable delay. The notification must not take place more than 60 calendar days after the date the breach is, or should have been, discovered unless a delay is necessary for certain law enforcement purposes.

Sixty calendar days is the maximum notification period, but may be an unreasonable delay. For example, if a covered entity has the information needed to send a notice 10 days after the breach, it is unreasonable for the covered entity to wait until the 60th day to send the notice.

The notification must be written in plain language and include:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach;
- A description of the **types** of unsecured PHI that were involved in the breach, if known (not the actual PHI that was breached);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity or business associate involved is doing to investigate the breach, to mitigate harm to individuals and to protect against further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number and email address, web site or postal address.

Notification must be provided in written form sent by first-class mail to the last known address of the individual or, if the individual has agreed to receive electronic notice, via email.

If a notice is undeliverable because the covered entity does not have current contact information for the individual, the covered entity must attempt to provide notice in another manner that is reasonably calculated to reach the individual. If there are fewer than 10 individuals for whom notices are undeliverable, the covered entity may provide telephone, email or other reasonable notice. However, if notices are undeliverable to more than 10 individuals, the covered entity must either post notice on its home page or provide notice in major print or broadcast media.

Notice that must be provided via the covered entity's web site or in major media must satisfy certain criteria.



Notification to the Secretary of HHS

Every breach of unsecured PHI must be reported to HHS. If a breach affects fewer than 500 individuals, the breach should be logged and submitted in an annual report within 60 days after the end of the year. If a breach affects at least 500 individuals, the breach should be reported to HHS at the same time notification is given to the affected individuals. Instructions on how to provide this notice will be provided on the HHS website at a later date.

Notification to the Media

If the unsecured PHI of more than 500 residents of any one state or smaller jurisdiction is, or is reasonably believed to have been, accessed, acquired or disclosed during such a breach, prominent media outlets in the state or jurisdiction must be notified. The information contained in the notice and the timing of the notice are the same as the notice to individuals impacted by the breach.

The media notification requirement is dependent upon the state or jurisdiction in which the affected individuals live. For example, if a breach affects 300 individuals who live in one state and 300 who live in another, immediate notification is required to HHS, but media notification is not required.

Where media notification is required, the type of media to which notice should be provided is dependent upon the geographic area in which the affected individuals live.

Notification to Covered Entities

Business associates are required to provide notice to any covered entities that may have individuals impacted by a breach. Such notice must be provided without unreasonable delay and in no case later than 60 days after the business associate discovers, or should have discovered, the breach. Business associates must provide covered entities with at least enough information to permit the covered entity to identify who may have been impacted by the breach and to provide the required notice to such individuals.

WHAT ACTIONS ARE REQUIRED OR RECOMMENDED?

- Covered entities and business associates must develop policies and procedures to identify and respond to potential breaches.

The current written HIPAA privacy policy must be updated to include these notification policies and procedures.

- Covered entities and their business associates should work together to:
 - Identify the persons within each organization who are responsible for providing (in the case of the business associate) and receiving (in the case of the covered entity) breach notifications;



- Create timelines for providing notice to the covered entity and establish the circumstances under which information will be provided prior to completion of the business associate's full investigation of the possible breach;
- Designate responsibility for notifying affected individuals; and
- Allocate costs and liabilities that may be incurred by the parties with regard to these rules.

Business associate agreements should be reviewed and modified, if necessary, to incorporate provisions consistent with these new rules.

- Covered entities and business associates must train their workforces on the policies and procedures for identifying and responding to potential breaches.

Covered entities and business associates should consider providing a refresher on the full scope of the organization's HIPAA privacy and security compliance if HIPAA privacy and security training has not taken place recently.

FOR MORE INFORMATION

If you would like more information about the HIPAA breach notification requirements, please contact your primary Thompson Hine Employee Benefits & Executive Compensation lawyer or email us at AskUs@ThompsonHine.com. For a list of our Employee Benefits & Executive Compensation lawyers, go to www.ThompsonHine.com/practices/Employee_Benefits_Executive_Compensation/lawyers/.

Thompson Hine sends bulletins as a service. If you do not wish to receive future bulletins, please email Heidi.Moreno@ThompsonHine.com with the phrase "Unsubscribe" as the subject line.

This advisory may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions. Some of the design images and photographs in this document may be of actors depicting fictional scenes.

© 2009 THOMPSON HINE LLP. ALL RIGHTS RESERVED.