Legal Alert: Department of Health and Human Services Issues Breach Notification Rules for Unsecured Protected Health Information

9/2/2009

On August 24, 2009, the Department of Health and Human Services ("HHS") issued its interim final rule with regard to breach notification requirements for unsecured protected health information. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, which is part of the American Recovery and Reinvestment Act of 2009, HHS was required to issue interim final regulations regarding notification provisions in the event of a breach of unsecured protected health information. Generally, the HITECH Act requires HIPAA covered entities (i.e. health plans, health care providers who transmit certain transactions electronically and health care clearinghouses) to provide notification to affected individuals upon the discovery of a breach of unsecured protected health information. A notice is also required to be sent to a major media outlet if more than 500 individuals within a state or jurisdiction are impacted by the breach. Additionally, covered entities are required to notify HHS in the event of a breach of unsecured protected health information impacting 500 or more individuals.

When is notice required?

The notification requirements under the regulations are triggered only when there is a breach of unsecured protected health information. HHS previously issued guidance regarding when protected health information would be considered unsecured. Under this guidance, which is reiterated under the breach notification regulations, protected health information is considered secure if it has been encrypted or completely destroyed. The notification rule goes on to define a breach as the acquisition, access, use or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule and which compromises the security or privacy of the protected health information. The definition of a breach also includes three exceptions: (1) for unintentional access by a covered entity or business associate employee; (2) situations involving inadvertent disclosure from one covered entity or business associate employee to another similarly situated employee; or (3) where the recipient would not reasonably have been able to retain the information.

Essentially, there is a four-step process in which covered entities and business associates should engage to determine if there is a breach of unsecured protected health information triggering notification requirements:

Step 1 - Determine whether the PHI is unsecured (i.e. not encrypted nor destroyed);

Step 2 - Determine if the information was used or disclosed in a manner that would violate the HIPAA Privacy Rules;

Step 3 - Determine whether the impermissible use or disclosure compromises the security or privacy of the protected health information. HHS has said the security or privacy of PHI is compromised when there is a significant risk of financial, reputational or other harm to the individual. A risk assessment should be conducted to determine whether such harm has occurred; and

Step 4 - Determine whether the incident falls under one of the exceptions.

General Notice Requirements:

If there is a breach of unsecured protected health information, the covered entity must provide notice to the individual without unreasonable delay, but no later than 60 days after the discovery of the breach. Additionally, if a business associate discovers a breach of unsecured protected health information, it is required to notify the covered entity without unreasonable delay, but in no event later than 60 days after discovery of the breach. Under the regulations, a breach is considered discovered on the first day it becomes known to any member of the covered entity's or business associate's work force (or an agent of the covered entity or business associate), or the date it would have been known if the covered entity or business associate exercised reasonably diligence. HHS also notes that a business associate may be considered an agent of the covered entity. As such, the business associate's discovery of the breach could be imputed to the covered entity. Additionally, it is noted that the 60-day time period to provide notification is not a safe-harbor, but an outside limit. The notification should be provided as soon as reasonably practical but no later than 60 days.

The regulations require the notice to be written in plain language and contain all of the following information:

• a brief description of what happened;

• the types of protected health information involved;

• any steps the individual should take to protect themselves from further potential harm;

• a brief description of the actions the covered entity is taking to mitigate losses and prevent future breaches; and

• contact information for individuals to ask questions, which should include a toll-free number, e-mail address, website or postal address.

Notice to Individuals:

In the event of a breach of unsecured protected health information, notice meeting the requirements described above should be sent to the individual at their last known address or by e□mail, if the individual agrees to receive notice by e-mail. Notices to deceased individuals may be sent to their next-of-kin or a personal representative. All notices to individuals should meet

the timeframe and content requirements discussed above.

A substitute notice may be provided to individuals if the covered entity has insufficient or out-of-date contact information. If the breach involves fewer than 10 people, the substitute notice may be provided by phone, e-mail, or posting on the covered entity's website in lieu of a written notice sent to the last known address. If 10 or more individuals are involved in the breach, the covered entity must either post the notice on its home page for at least 90 days or provide notice in some major print or broadcast media that would likely reach the affected individuals.

Notice to the Media:

In addition to sending notices to the affected individuals, if the breach involves more than 500 residents of a state or smaller jurisdiction, the covered entity is required to send notification to prominent media outlets serving that state or jurisdiction. The notice to the media must meet the same content and timeframe requirements as notices to individuals. The notice to media is only triggered if there are more than 500 residents impacted of a particular state. So, if a total of 600 residents is impacted, and 300 are residents of one state and 300 are residents of another state, the media notice is not required. Finally, HHS clarifies that such notice may be provided to the media in the form of a press release.

Notice to the Department of Health and Human Services:

If there is a breach of unsecured protected health information involving fewer than 500 people, HHS requires the covered entity to maintain a log of such incidents and submit the log on an annual basis to HHS. The log is required to be submitted within 60 days after the end of the calendar year. For 2009, the log is only required to include breaches that occurred after the effective date of the interim final rule (i.e. September 23, 2009).

For a breach of unsecured protected health information involving 500 or more individuals, HHS requires the covered entity to notify HHS within 60 days of the breach. This notice applies regardless of where the impacted individuals reside. Unlike the media notice, which is only triggered if more than 500 impacted individuals reside in the same state, the notice to HHS applies even if there are fewer than 500 individuals who reside in a particular state as long as a total of 500 or more individuals are impacted. The notice to HHS is in addition to the individual notices that are required and any media notice that may be required. Instructions for the form and the content of the notice to HHS will be posted on the agency website. Additionally, HHS will post on its website the names of covered entities that report security breaches involving 500 or more individuals.

Effective Date and Enforcement Date:

The interim final rule on breach notification requirements was published August 24, 2009, and takes effect September 23, 2009. While HHS expects covered entities to fully comply with the breach notification rules as of the effective date, it has decided not to impose any sanctions for failure to provide the notifications required before 180 days from the date of publication of the interim final rule (i.e. February 22, 2010).

Action Items:

• Ensure that all PHI handled is secured according to HHS guidance (encrypted or destroyed) or ensure notice procedures are in place to comply

with the breach notification rules;

• Identify all business associates and agents with access to protected health information and ensure that agreements are updated with appropriate language to ensure compliance with breach notification rules;

• Update HIPAA training material to include training for breach notification requirements. Workforce members should be trained on the new notification procedures.

• Update your HIPAA policies and procedures manual to include policies and procedures related to breach notification requirements.

• Ensure an accurate and up-to-date security breach log is being maintained.

In addition to the breach notification rules described above, there are further amendments to the HIPAA Privacy and Security Rules under the HITECH Act. Please see our Legal Alert, Economic Stimulus Act Impacts HIPAA Requirements, dated February 23, 2009, for more information on these amendments.

If you have any questions regarding the breach notification rule or any of the other amendments to HIPAA under the HITECH Act, please contact Daniel T. Sulton at dsultan@fordharrison.com or any member of our Employee Benefits Group.