A Timely Analysis of Legal Developments

ASAP®

In This Issue:

August 2009

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), one small legislative portion of the massive economic stimulus bill enacted on February 17, 2009, mandates that employers and health care providers provide notice of any "breach" of "unsecured" protected health information (PHI) to affected individuals; the U.S. Department of Health and Human Services (HHS); and, in certain circumstances, "prominent media outlets." The quoted terms and many others in the HITECH Act are either undefined or raise a multitude of unanswered questions. HHS has recently published interim final regulations and accompanying commentary that clarify many of the Act's ambiguities.

Employers and Health Care Providers Receive New Guidance on HIPAA Security Breach Notification

By Philip L. Gordon

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), one small legislative portion of the massive economic stimulus bill enacted on February 17, 2009, mandates that employers and health care providers provide notice of any "breach" of "unsecured" protected health information (PHI) to affected individuals; the U.S. Department of Health and Human Services (HHS); and, in certain circumstances, "prominent media outlets." The quoted terms and many others in the HITECH Act are either undefined or raise a multitude of unanswered questions. On August 24, 2009, HHS published in the Federal Register interim final regulations and accompanying commentary that clarify many of the Act's ambiguities.

Notably, the Federal Register publication triggers two key deadlines. Commencing September 23, 2009, employers and health care providers ("covered entities") will be required to comply with the Act's security breach notification requirements. However, because HHS has announced a 180-day enforcement grace period, the more important date is February 22, 2010. Employers and health care providers who discover a security breach after that date and fail to provide the required notices may be targeted for an enforcement action.

As explained below, covered entities have much to accomplish during the grace period. They will need to digest the new requirements, revise existing HIPAA policies and procedures and develop new ones, put in place a security incident response plan, train employees, confer with business associates about security breach response, and negotiate modifications to existing business associate agreements.

What Triggers an Obligation to Notify?

To determine whether a security breach triggering HIPAA notification requirements has occurred, covered entities will need to work through the following questions:

1. **Did the incident involve protected health information (PHI)?** Significantly, most health information in the possession of employers is *not* PHI. For employers,

PHI is limited to individually identifiable health information created or received by, or on behalf of, a group health, dental or vision plan; health care reimbursement flexible spending account; pharmacy benefits plan; employee assistance program; or long-term care plan. Health information related to leave requests, accommodation requests, and workers' compensation as well as health information created or received by an in-house medical provider are *not* PHI. Covered health care providers — those who use HIPAA-mandated codes to bill insurers and government health programs for services — and employers in their capacity as the administrator of a HIPAA-covered plan should bear in mind that PHI includes demographic information associated with a health record, such as Social Security number, date of birth, and even an e-mail address.

2. **Was the PHI "unsecured"?** HHS has defined *unsecured* to mean PHI that has not been: (a) encrypted consistent with standards set by the National Institute for Standards and Technology; or (b) destroyed in a manner that renders the information irrecoverable, such as shredding for paper records. Thus, while HIPAA does not require the use of encryption, encrypting PHI can reduce the risk that a covered entity will be required to provide notice of a security breach.
3. **Did the incident involve a use or disclosure of unsecured PHI that violated the HIPAA Privacy Rule?** HHS has defined *breach* to mean a use or disclosure of unsecured PHI in violation of the HIPAA Privacy Rule. The Privacy Rule establishes an elaborate framework for permissible uses and disclosures of PHI. As a general rule, PHI may not be used or disclosed without the individual's prior written authorization. However, the Privacy Rule contains a laundry list of exceptions to this general rule. Consequently, covered entities often may be required to scrutinize the Privacy Rule to determine whether a breach occurred.
4. **Does the Privacy Rule violation fall within one of the exceptions to the notification requirements?** HHS has carved several, relatively narrow situations from the notification obligation: (a) when a workforce member authorized to access PHI inadvertently accesses PHI that is not within the scope of the authorization — for example, when a benefits administrator responsible for certain divisions of a large corporation inadvertently reviews PHI for employees of a division that is not assigned to her; (b) when a workforce member authorized to access PHI inadvertently discloses PHI to another workforce member who also is authorized to access PHI and works at the same facility — for example, when a doctor inadvertently gives a patient chart to a nurse who is not responsible for the doctor's patients; and (c) when the covered entity has a good faith belief that the recipient of an unauthorized disclosure of PHI would not have reasonably been able to retain the information — for example, when a payroll administrator's employee informs the employer that she received an e-mail with a spreadsheet containing health plan information but deleted it as soon as she realized that the e-mail was intended for the employer's health plan administrator.
5. **Does the Privacy Rule violation pose a significant risk of financial, reputational or other harm to the individual?** In making this risk assessment, the employer or health care provider should, according to HHS' commentary, consider the following non-exclusive list of factors: (a) who impermissibly used the information or to whom was the information impermissibly disclosed; (b) the type and amount of PHI disclosed; and (c) any steps taken that mitigate the potential harm to the individual. The risk assessment must be documented if it results in a decision not to provide notice, because the breach does not pose a significant risk of harm.

Who Must Be Notified?

The covered entity must notify each affected individual. When the recipient is an unemancipated minor, the notice should be sent to the minor's parent. If the covered entity knows that an affected individual is deceased, the covered entity should send the notice to the next of kin or personal representative, if known, and contact information is available.

If the breach involves 500 or more individuals, the covered entity must notify HHS contemporaneously with notifying affected individuals. Significantly, HHS will post information from these notices on its website, exposing the covered entity making the report to a greater risk of litigation and adverse publicity. Breaches involving fewer than 500 individuals must be logged and the log must be submitted to HHS no later than March 1 of the following calendar year.

If the breach involves 500 or more individuals from a state or jurisdiction, the covered entity must notify "prominent media outlets serving

the state or jurisdiction" contemporaneously with notifying affected individuals. The regulations do not define the quoted phrase, but HHS commented that the appropriate media outlet could be a citywide newspaper if all affected individuals reside within city limits but would be a statewide newspaper or television news program if affected individuals are more dispersed. The notice can take the form of a press release. Notably, the HITECH Act authorizes state attorneys general to enforce HIPAA. Consequently, to the extent the media outlet publicizes the breach, this notice raises the risk of an enforcement action by the attorney general's office.

When Must Notice Be Delivered?

Unless law enforcement asks the covered entity to delay notice, notice must be provided as soon as reasonably possible and without unreasonable delay, but in no event more than 60 days after discovery of the incident. The time spent investigating an incident to determine whether a breach, in fact, has occurred counts against the 60-day time limit.

Discovery occurs when any person who is a "workforce member" or agent of the covered entity (other than the responsible person) knows of the incident. The Privacy Rule broadly defines *workforce member* to include "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." As a result, the 60-day period for delivering notice could start to run before anyone in management is aware of the incident. To address this issue, covered entities should consider implementing reasonable systems for discovering a breach and train workforce members on how to identify and report a possible security breach.

HIPAA uses the term *business associate* to describe third-party agents who create or receive PHI on the covered entity's behalf. The regulation requires that business associates notify the covered entity of any breach and provide the identity of affected individuals. The regulations, however, do not specify a time frame and do not require that the business associate provide other information which the covered entity most likely will need to fulfill its notice obligation. As a result, the covered entity should address those matters in its vendor agreements, known in HIPAA parlance as "business associate agreements."

Discovery of a breach can occur even when no one knows of the incident if the incident would have been known to the covered entity through the exercise of reasonable diligence. HHS interprets the term *reasonable diligence* to mean "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." Under this definition, the 60-day notice period would run if, for example an employee failed to report a lost or stolen laptop containing unsecured PHI.

A statement by law enforcement that complying with any of the notice requirements would impede a criminal investigation or undermine national security tolls the 60-day notice period. A written request tolls the notice period for the duration of the requested delay. An oral request tolls the notice period for no more than 30 days unless followed by a written request for a longer delay. The covered entity must document the oral request.

What Must the Notice Say?

The regulations identify five subject matters that must be addressed in the notice:

1. A brief description of what happened, including the date of the breach and the date that the breach was discovered, if known;
2. The types of unsecured PHI involved in the breach, *e.g.*, Social Security number, date of birth, diagnosis;
3. Steps affected individuals can take to reduce the risk of harm from the breach;
4. A brief description of the covered entity's investigation, efforts to mitigate harm to affected individuals, and steps taken to prevent a recurrence; and
5. Contact information for obtaining additional information.

The regulations do not require that a covered entity offer any particular service to assist affected individuals, such as credit monitoring or fraud resolution services. The Privacy Rule does, however, require that each covered entity take reasonable steps to mitigate the harmful effects of an unauthorized use or disclosure of PHI. In some circumstances, the covered entity may need to offer services to affected individuals to comply with this mitigation requirement. Even when offering such services is not required, the covered entity may need to do so to maintain good employee or customer relations.

How Must the Notice Be Delivered?

Except in limited circumstances, the covered entity must send the notice by first-class mail to the affected individual's last-known mailing address. If ten or more notices are returned as undeliverable, the covered entity must prominently post the notice, or a hyperlink to the notice, on its website. The notice must remain posted for at least 90 days and include a toll-free number where callers can learn whether the breach compromised their PHI.

Interplay with State Security Breach Notification Laws

Forty-four states and the District of Columbia have enacted security breach notification laws that are similar to, but can very materially from, HIPAA's new security breach notification requirements. HHS has opined that the HIPAA requirements do *not* preempt state notice law and has stated that covered entities will be required to comply with both sets of laws when both are applicable.

Next Steps for Covered Entities

Given the requirements of notice to HHS and to prominent media outlets for larger breaches, a compromise of unsecured PHI — whether by an employer, a healthcare provider, or a business associate — could result in bad publicity and potentially costly litigation. To reduce these risks covered entities should consider accomplishing the following before the enforcement grace period expires on February 22, 2010:

- Create a security breach response plan or update the existing plan.
- Implement systems for detecting a security breach.
- Train workforce members on their role in responding to a security breach.
- Negotiate amendments to business associate agreement to address security breaches.
- Revise HIPAA policies and procedures regarding training, complaints, sanctions, non-retaliation, non-waiver of rights, as may be necessary, to address the security breach regulations.
- Update address lists for patients and/or plan participants to reduce the number of returned notices in the event of a breach.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and Chair of Littler Mendelson's Privacy & Data Protection Practice Group. He maintains a blog on employment related privacy issues at http://privacyblog.littler.com. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com.