[Alerts and Updates]

Compliance with New HIPAA and FTC Health Breach Notification Rules: What Healthcare Entities and Businesses Need to Know

August 28, 2009

On August 24, 2009, the U.S. Department of Health and Human Services ("HHS") published an interim final rule amending Health Insurance Portability and Accountability ("HIPAA") regulations by adding provisions that require notice to patients and others of a "breach," or disclosure of unsecured protected health information ("PHI"), by HIPAA-covered entities and business associates (the "HIPAA Rule").[1] A day later, the Federal Trade Commission published the Health Breach Notification Rule to address breach notification by personal health-records vendors (the "FTC Rule").[2] These rules implement portions of the federal "stimulus package," known as the American Recovery and Reinvestment Act of 2009 ("ARRA"), which was passed by Congress on February 17, 2009.

This Alert discusses the HIPAA Rule and the FTC Rule, and their significant elements. The HIPAA Rule is effective on September 23, 2009, although HHS will be accepting comments through October 23, 2009. These comments may be useful to HHS and to the public in further understanding the HIPAA Rule's implementation. Furthermore, HHS has indicated, in the explanatory preamble to the HIPAA Rule, that, relying on an ambiguity in ARRA, it will not impose sanctions for failure to comply with the HIPAA Rule prior to February 22, 2010. The FTC Rule is effective on September 24, 2009, and full compliance is required by February 22, 2010.

In general, the HIPAA Rule requires that a HIPAA-covered entity (a healthcare provider, payor or clearinghouse) notify an individual when unsecured PHI has been improperly disclosed. The entity must also notify HHS regarding confirmed breaches, either through an annual report or sooner, depending on the number of individuals affected. In some instances, media must also be notified. The HIPAA Rule specifies the content of the notice. Integral components of the HIPAA Rule are definitions of "unsecured PHI" and "breach," which *exclude* unauthorized uses and disclosures that do *not* violate the HIPAA Rule and do *not* significantly harm an individual. The HIPAA Rule and its preamble reveal a new twist in HHS's perspective on when, for notice purposes, a business associate is acting as an agent, as opposed to an independent contractor—a potentially confusing aspect of the HIPAA Rule.

Significant Definitions and Analysis

"Unsecured PHI"

"Unsecured PHI" is PHI (generally, information in any form that concerns the health of an individual) that is *not* rendered "unusable, unreadable, or indecipherable" through the use of a "technology or methodology," specified by HHS in its guidance. The guidance listed the two acceptable technologies and methodologies for rendering PHI secure—encryption and destruction—and included specific definitions for each. For instance, paper, film or other hard-copy media are considered "destroyed" only if they are shredded or altered so that they cannot be read or otherwise reconstructed, and redaction is specifically excluded as a mode of destruction. Thus, PHI that has not been encrypted or destroyed—and is subsequently disclosed—would be subject to the HIPAA Rule's notice provisions. Information technology staff and consultants may want to carefully review the HHS guidance, which is available in the *Federal Register* and on the HHS website, for additional requirements concerning encryption and destruction.

It is important to note that the data-protection standards recognized under the HIPAA Rule (encryption and destruction) are different from the data-protection standards articulated under the HIPAA Security Rule and the HIPAA Privacy Rule. The Security Rule requires that covered entities protect *electronic* PHI by satisfying a number of general standards. The Privacy Rule requires

that covered entities apply reasonable safeguards to all PHI. Thus, even PHI that was protected in accordance with the Privacy and Security Rules, such as by use of firewalls, but was breached under the terms of the new HIPAA Rule, would have to be reported.

"Breach"

Although the definition of "unsecured PHI" is broad, the definition of "breach" somewhat limits the situations when notice must be provided. When PHI is improperly disclosed, a covered entity or business associate should perform a specific analysis to determine whether a breach requiring notification has occurred:

1. A breach occurs only if the following elements are present in the situation: (a) there has been an "unauthorized" access, use or disclosure of PHI, which violates the HIPAA Privacy Rule; and (b) the disclosure "compromises the security or privacy" of the PHI," which means that it "poses a significant risk of financial, reputational, or other harm to the individual."
2. A breach does not occur if the PHI is part of a "limited data set," *and* does not include ZIP codes or dates of birth. A limited data set is a collection of PHI that excludes some but not all identifying PHI (*e.g.*, names, addresses), and is used for research, public health or operational purposes.
3. A breach does not include (a) any "unintentional" acquisition, access or use of PHI by a workforce member or individual acting under the authority of the covered entity or business associate that is made in good faith, within the course or scope of employment or other professional relationship, *and* is not further used or disclosed in an unlawful manner under the HIPAA Privacy Rule; (b) an "inadvertent" disclosure to another authorized person at the same covered entity, business associate or organized healthcare arrangement, and the PHI is not further used or disclosed in an unlawful manner under the HIPAA Privacy Rule; and (c) a disclosure where the covered entity or business associate had a good-faith belief that the unauthorized person to whom the information was disclosed would not reasonably be able to "retain" such information.

Determining Whether a Breach of Unsecured PHI Has Occurred

In practical terms, how can a covered entity or business associate determine whether a breach has occurred?

- First, it should determine whether there has been a violation of the HIPAA Privacy Rule. An incidental disclosure of PHI, as permitted under the Privacy Rule, would not constitute a breach.
- Second, if a HIPAA Privacy Rule violation has occurred, the entity should perform a *risk assessment* to determine whether the event poses a *significant* risk of financial, reputational or other harm to the individual. If a laptop were lost and later recovered, and it was determined that the PHI on the laptop posed minimal risk of harm to the individual, or the laptop had not been used during the time it was lost, then no breach would have occurred. The risk assessment should also consider whether the PHI at issue was part of a limited data set and also included ZIP codes or dates of birth; if not, there likely is no significant risk of harm to the individual posed by any disclosure.
- Finally, the entity should determine whether an exception applies. Here are some examples, as provided in the explanatory preamble to the HIPAA Rule:
    - A billing employee mistakenly receives an email from a clinician that contains PHI. The employee deletes the email and alerts the clinician. The first exception ("unintentional" access") applies.

- A physician inadvertently sends an email containing PHI to a nurse at the same hospital regarding the wrong patient. The physician and the nurse are both authorized to access the PHI. The second exception ("inadvertent access") applies.
- A hospital sends an explanation of benefits to the wrong individuals. Some are returned as undeliverable. The third exception (no ability to "retain" unsecured PHI) applies.

It is important to note that the burden is on the covered entity or business associate, through documentation or otherwise, to show that no breach has occurred or that an exception applies.

Notification

Timing

If it is determined that a breach has occurred, the covered entity should notify the individual who is the subject of the breach of unsecured PHI *without unreasonable delay*, but in no case later than 60 days after discovery. The 60-day period begins on the day that the covered entity (including its workforce and other agents) first knew or, *with reasonable diligence*, should have known about the breach. The 60-day rule is designed to allow for a reasonable amount of time to perform an investigation, but the entity should not wait to perform its investigation or notify the individual until the end of the 60-day period.

In determining whether a covered entity acted without unreasonable delay, HHS will consider whether the breach was known to an agent of the covered entity—which could include a business associate. The agent's knowledge of the breach is attributed to the covered entity, and the 60-day period begins with the timing of the agent's knowledge.

A potentially thorny aspect of the HIPAA Rule is whether a business associate is acting as an agent or as an independent contractor. In general terms, an agent steps into the principal's shoes to perform an act under the principal's scope of authority (*e.g.*, billing); an independent contractor performs an independent activity on behalf of the principal (*e.g.*, data analysis). One way to navigate this issue may be to impose strict notice time frames in business associate agreements.

The Notice

Notice must be made by First-Class mail, unless the individual (or next of kin) has agreed to electronic notice; however, if the contact information is insufficient or out-of-date and the individual is still living, the entity must provide for "substitute notice." Substitute notice is based on the circumstances and the number of individuals affected (*e.g.*, if under 10 individuals, notice may be made by phone; if over 10 individuals, more "conspicuous" notice is required, such as on the provider's website with a toll-free number, active for three months to provide more information).

The notice must include a brief description of the breach, the type of information disclosed, any steps the individual should take (*e.g.*, notifying the police), the steps taken to investigate and mitigate the breach, and contact procedures. The notice should not contain sensitive information, such as the type of medical treatment that happened to be disclosed.

When the breach involves more than 500 persons, the covered entity must notify HHS, per instructions to be posted on the HHS website. When the breach involves more than 500 residents of a particular state or "jurisdiction" (an area within a city), the covered entity must notify prominent media outlets without unreasonable delay, but no later than 60 days following discovery of

the breach. The notice must describe the breach according to the same content requirements for individual notices. The covered entity must keep a log of all breaches involving less than 500 individuals, and notify HHS annually.

Business Associates

For the business associate, like the covered entity, the beginning of the HIPAA Rule's timing requirements is tied to the day that the breach was actually known or should have been known with reasonable diligence. If the business associate is acting as an agent of the covered entity, discovery of the breach by the business associate is imputed to the covered entity, so that the covered entity's time frame for notifying the individual begins on the day that the breach was discovered by the business associate. If the business associate is acting as an independent contractor, it must notify the covered entity without unreasonable delay, but in no case later than 60 days, after discovery of the breach, at which time the covered entity's duties are triggered.

The business associate must also provide specified information, including the names of the individuals whose information was breached, to the covered entity. The covered entity and the business associate may determine which entity is in the best position to issue the notice to the individual. HHS discourages multiple notices to consumers.

Administrative Obligations

The HIPAA administrative obligations applicable to covered entities—including training, workforce sanctions, a complaint procedure, refraining from retaliatory acts, no waiver of rights, amendment of policies and procedures, and documentation—should be amended to take into account the HIPAA Rule. In addition, under the HIPAA Rule, business associates must undertake these same administrative obligations. The covered entity or the business associate should be able to demonstrate that, with respect to any event, no breach occurred or that proper notice was made.

The FTC Rule

The FTC Rule outlines requirements for vendors of personal health records ("PHRs") and PHR-related entities to notify their customers of any breach of unsecured, individually identifiable health information. These entities include vendors of online applications that interact with PHRs, "such as blood pressure cuffs, blood glucose monitors, or other devices," whose readings consumers can upload into their personal health record. For such entities, ARRA requires HHS to study—in consultation with the FTC—potential privacy, security and breach notification requirements, and to submit a report to Congress containing recommendations within one year of enactment of ARRA. In the interim, ARRA includes temporary requirements, to be enforced by the FTC, that specify the timing, method and contents of the breach notice to consumers in the event of a security breach.

Under the FTC Rule, "breach of security" is defined as the acquisition of unsecured PHI of an individual in a PHR without the authorization of the individual. A breach of security is presumed "when there is unauthorized access to data . . . unless the entity that experienced the breach 'has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.'" Similar to entities covered by the HIPAA Rule, entities covered by the FTC Rule may rely on encryption and destruction to demonstrate that PHI is secure. In the event of a breach, vendors must contact the FTC and the consumer directly, or if the breach is experienced by the vendor's service provider, it must notify the vendor, which then must notify the consumer and the FTC. As with the HIPAA Rule, if the breach affects 500 or more people, the FTC Rule requires that the media, in addition to the consumer, should be notified. Breach notices must be given "without unreasonable delay" and in no case later than 60 calendar days after discovering the breach. However, unlike the HIPAA Rule, the entity is required to notify the FTC

within 10 business days of the breach. Entities that do not properly notify consumers of the breach may be subject to civil penalties.

When a vendor provides PHRs under a business associate arrangement as well as independently to consumers, and a breach occurs that affects both sets of PHRs, the vendor is permitted to issue the same notice to all affected individuals, pursuant to the HIPAA Rule notice requirements, assuming that the covered entity has given the vendor/business associate the authority to issue the notice to its affected individuals.

Final Words

The HIPAA Rule and FTC Rule are part of a larger initiative, begun with the passage of HIPAA in 1996 through ARRA, to integrate advanced technology into the healthcare system. Both rules address consumers' concerns about the use of their healthcare information. Governed by deadlines imposed by ARRA—but recognizing the significant, unfunded burdens on affected entities—HHS and the FTC will not pursue enforcement under a de facto six-month grace period. Nevertheless, with effective dates less than one month away, entities should act promptly to ensure compliance and to draft comments on the HIPAA Rule—as comments are due by October 23, 2009.

For Further Information

If you have any questions about this Alert or would like more information, please contact Lisa W. Clark, any of the attorneys in our Health Law Practice Group or the attorney in the firm with whom you are regularly in contact.

Notes

1. Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42739 (Aug. 24, 2009).
2. Health Breach Notification Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009).