Client Advisory

Katten
Katten Muchin Rosenman LLP

Health Care/Technology

August 31, 2009

HHS Issues Security Breach Notice Rule

On August 24, the Department of Health and Human Services ("HHS") published its rule (the "Rule") implementing the provisions of the HITECH Act[1] that require covered entities and their business associates to provide notice of breaches of unsecured protected health information ("PHI"). The Rule contains key information about what constitutes a "breach," how to determine if breach notification is required (or not), and how to create a compliant breach notification process. It also updates the earlier HHS guidance document (the "Guidance") specifying encryption and destruction as the two technologies and methodologies for rendering PHI "secure"—such that breach notification requirements can be avoided altogether.

The Rule applies to breaches occurring on or after September 23, 2009. Therefore, *it is critical that covered entities and their business associates waste no time in implementing security breach detection and notification programs that incorporate the provisions of the Rule (or alternatively, ensure that all PHI is "secured" in accordance with the updated Guidance)*. In recognition of the time it will take covered entities and their business associates to put in place such programs or secure their PHI, HHS will not impose sanctions for failure to provide the required breach notifications for breaches that are discovered before February 22, 2010.

The Rule was issued as an interim final rule with request for comments. Comments are due on or before October 23, 2009.

Overview of the HHS Security Breach Notice Rule

The HITECH Act required HHS to issue regulations for breach notification by covered entities subject to HIPAA[2] and their business associates. The Rule sets forth requirements for notifying affected individuals, the media and the Secretary of HHS following a breach of unsecured PHI. Highlights of the Rule are summarized below. In a separate but related development, on August 25, the Federal Trade Commission ("FTC") published its final Health Breach Notification Rule, which applies to vendors of personal health records and their third party service providers for breaches of unsecured, individually identifiable health information.[3] Regardless of which set of breach notification regulations apply, all affected entities must use the Guidance, as updated below, to determine whether information was "unsecured."

[1] Health Information Technology for Economic and Clinical Health Act ("HITECH"), part of the American Recovery and Reinvestment Act of 2009 ("ARRA").

[2] Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

[3] The FTC's Health Breach Notification Rule is effective September 24, 2009, and full compliance is required by February 22, 2010. That Rule is not summarized here, although the HHS and the FTC took steps to harmonize their respective breach notification rules to the extent practicable.

If you have any questions regarding the Security Breach Notice Rule or how it may affect your business, please contact one of the Katten Muchin Rosenman LLP professionals listed below:

Megan Hardiman
312.902.5488 / megan.hardiman@kattenlaw.com

Sheila Sokolowski
312.902.5456 / sheila.sokolowski@kattenlaw.com

Leonard A. Ferber
312.902.5679 / leonard.ferber@kattenlaw.com

Tanya L. Curtis
312.902.5593 / tanya.curtis@kattenlaw.com

Michael R. Callahan
312.902.5634 / michael.callahan@kattenlaw.com

Tara Goff Kamradt
312.902.5502 / tara.kamradt@kattenlaw.com

What Is a "Breach" of Unsecured PHI?

Covered entities and their business associates must provide notice of breaches of unsecured PHI. The HITECH Act defines "breach" as the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Regulations which compromises the security or privacy of the PHI. The Rule clarifies several important points about what constitutes a "breach."

a. The "Harm" Threshold

Under the Rule, not all violations of the Privacy Rule will be "breaches" triggering notification. Rather, notification is required only if: (1) there has been a violation of the Privacy Rule, *and* (2) the violation is one that compromises the security or privacy of the PHI. The Rule clarifies that a violation of the Privacy Regulations "compromises the security or privacy of PHI" *only if it poses a significant risk of financial, reputational or other harm to the individual*.

b. Conducting a Risk Assessment

To determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure, covered entities and business associates will need to perform a risk assessment. A variety of factors can be considered, such as (1) to whom the information is disclosed; (2) whether immediate steps were taken to mitigate the harm; (3) whether impermissibly disclosed PHI was returned prior to its being accessed; and (4) the type and amount of information disclosed. HHS has suggested that covered entities may want to review OMB Memorandum M-07-16 for examples of the types of factors to consider.

Example: A covered entity improperly discloses PHI that merely includes the name of an individual and the fact that he received services from a hospital. Depending on the facts, the covered entity may determine that this disclosure does *not* constitute a significant risk of financial or reputational harm to the individual. However, if the disclosure indicates the type of services (oncology) or a specialized facility (substance abuse), or if the PHI includes information that increases the risk of identity theft (such as social security number, account number or mother's maiden name), then there is a higher risk that the Privacy Rule violation compromised the security or privacy of the information.

Note: Covered entities and business associates bear the burden of proving that no breach has occurred because the impermissible use or disclosure did not pose a significant risk of harm. For this reason, it is critical that covered entities and business associates adequately document and retain their risk assessments.

c. New Exception for Limited Data Sets that Also Exclude Dates of Birth and Zip Codes

In the Rule, HHS declines to recognize "limited data sets" as a method of rendering PHI "secure," due to the potential risk of re-identification of this information. However, HHS does recognize that a covered entity or business associate may (depending on the facts) determine that the risk of identifying a particular individual is so small that an impermissible use or disclosure of a limited data set poses no significant risk of harm to any individuals. Furthermore, the Rule also sets forth a narrow exception under which use or disclosure of PHI as part of a limited data set *that also excludes dates of birth and zip codes*, does not compromise the security or privacy of the PHI.

d. Other Exceptions to Breach

As provided for in the HITECH Act, there are three exceptions to the definition of "breach." HHS provides a number of clarifications of terms used in the exceptions.

- With regard to the first exception—unintentional acquisition, access or use of PHI by employees or persons acting under authority of a covered entity or business associate—the Rule modifies the statutory language to use "workforce members" instead of employees. HHS clarifies that in determining whether a person is acting "under the authority of a covered entity or business associate," one should consider whether the person was acting on its behalf at the time of

the inadvertent acquisition, access or use. Additionally, HHS clarifies that the person must not further use or disclose in a manner not permitted under the Privacy Rule.

Example: A billing employee receives and opens a misdirected email from a nurse containing PHI about a patient, but then notices that he or she was not the intended recipient, alerts the sender of the email that it has been misdirected and deletes the email. Provided that the billing employee did not further use or disclose the PHI, this would not be a breach and would not require notification because the billing employee unintentionally accessed the PHI, and his access of the information was done in good faith and within the scope of authority.

- With regard to the second exception—inadvertent disclosure by a person authorized to access PHI to similarly situated individuals at the same facility—HHS clarifies that a "similarly situated individual" is one who is authorized to access PHI (whether or not authorized to access the same types of PHI). HHS also clarifies that "same facility" means the same covered entity, business associate or organized health care arrangement in which the covered entity participates. HHS also states that if a covered entity has multiple locations across the country, then the exception would apply even if the disclosure was made by a workforce member to a physician with staff privileges at a facility in another state.
- With regard to the third exception—disclosure to an unauthorized person not reasonably able to retain the PHI—HHS clarifies that a covered entity or business associate need only have a "good faith belief" that the unauthorized person would not have been able to reasonably retain the information disclosed. An example of a disclosure that fits this exception would be a nurse who mistakenly hands a patient discharge instructions for another patient, but then quickly realizes her mistake and recovers the instructions from the patient before they could have been read.

Note: Covered entities and business associates that rely on an exception must adequately document in the risk assessment why the impermissible use or disclosure fits an exception.

Discovery of Breach and Timeliness of Notification

- Breaches are treated as discovered when known by the covered entity, or when by exercising reasonable diligence, the breach would have been known by any person who is a workforce member or agent of the covered entity.
- Similarly, breaches are treated as discovered when known by the business associate, or when by exercising reasonable diligence, the breach would have been known by any person who is a workforce member or agent of the business associate.
- HHS clarifies that "reasonable diligence," with respect to both covered entities and business associates, means the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."
- Furthermore, if a business associate is acting as an agent of a covered entity, then the business associate's discovery of the breach is imputed to the covered entity and the covered entity must provide notification of the breach based on the time the business associate discovers the breach. However, HHS clarifies that where a business associate is acting as an independent contractor and not an agent of the covered entity, the covered entity must provide notification based on the time the business associate notifies the covered entity.
- Apart from a delay requested by a law enforcement official, which must be documented if requested orally, covered entities must provide individual notifications of a breach "without unreasonable delay" and no later than 60 days after discovery of the breach. HHS cautions that it may be unreasonable delay to wait until the 60th day to provide notification. For example, if a covered entity has the information necessary to provide notification to individuals at 10 days but waits until the 60th day to send the notification, it would constitute unreasonable delay.
- Business associates must notify covered entities of reportable breaches without unreasonable delay, and no later than 60 days from the date the business associate discovers the breach or should have discovered it using reasonable diligence. HHS clarifies that, to the extent possible, business associates must provide covered entities with the identity of each affected individual.

***Note**: Covered entities should ensure that their workforce members and other agents are adequately trained in the importance of timely reporting of privacy and security incidents and the consequences of failing to do so. Covered entities and business associates should implement reasonable systems for discovery and efficient investigation of breaches. Business associate agreements should consider breach notification timing and procedures.*

Content of Notice Requirements; Notice Procedures

The notice must be written in plain language and, to the extent possible, include the following elements:

- A brief description of what happened, including the date of the breach and the discovery of the breach, if known
- A description of the ***types*** of unsecured PHI involved in the breach, but not a listing of the actual PHI that was breached
- Any steps individuals should take to protect themselves from harm resulting from the breach
- A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individual and protect against further breaches
- Contact procedures for individuals to ask questions, including a toll-free number, email address, website or postal address

Generally, notice of a breach to the individual is to be provided by first-class mail at the last known address of the individual, though email may be used provided the individual has agreed.

In the event a covered entity does not have sufficient contact information for an individual, substitute notice may, depending on the number of affected individuals, be provided through telephone or other means, posting on the covered entity's homepage or through the appropriate print or broadcast media. Specific requirements for each of these alternatives are set forth in the Rule.

In the event the breach affects 500 or more residents of a state or jurisdiction, a covered entity must provide notice to the prominent media outlets serving that state or jurisdiction, and may do so in the form of a press release.

In the event the breach affects 500 or more individuals, regardless of their residence, the covered entity must notify the Secretary of HHS immediately. For this purpose, HHS interprets "immediately" to require that notice be sent to the Secretary concurrently with notification to the individual. For breaches affecting fewer that 500 individuals, the covered entity must maintain a log of such breaches and submit the log to the Secretary of HHS annually.

Contrary state law is preempted by these breach notification regulations and HHS is soliciting comments in this area. However, HHS notes that often it will be possible to issue a single notification that complies with both state and federal law.

***Note**: Covered entities and business associates need to develop the notice form and related procedures. Notice form and breach discovery, investigation and notification policies and procedures need to consider applicable state as well as federal breach notification provisions. Covered entities and business associates should retain documentation sufficient to demonstrate that the requisite notifications were made.*

Updates to Guidance on Securing PHI

Section 13402(h) of the HITECH Act defines "unsecured PHI" as "PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance," and provides that the guidance must specify the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. Covered entities and business associates that implement the specified technologies and methodologies with respect to PHI are not required to provide notice in the event of breach of such PHI as the PHI is not considered to be "unsecured." The Secretary initially

issued this Guidance on April 17, 2009, specifying encryption and destruction as the technologies and methodologies of rendering PHI unusable, unreadable or indecipherable to unauthorized individuals such that breach notification is not required. In response to comments, HHS has issued an updated Guidance. Highlights include the following:

- In response to apparent public confusion, HHS emphasizes that the Guidance does not impose any new requirement on covered entities to encrypt all PHI. A covered entity may be in compliance with HIPAA's Security Rule even if it reasonably decides not to encrypt electronic PHI, but instead to use a comparable method to safeguard the information. However, a covered entity that wishes to ensure breach notification is not required in the event of a breach of electronic PHI would need to encrypt that PHI in accordance with the Guidance.
- Clarification of the terms "data in motion," "data in use" and "data at rest."
- Entities subject to the separate FTC Health Breach Notification Rule (such as vendors of PHRs and their third party service provider) must also use the HHS Guidance to determine whether the information subject to a breach was "unsecured" and, therefore, whether breach notification is required.
- In response to comments requesting that access controls be included in the Guidance, HHS confirms that, despite their benefits, access controls do not meet the statutory standard of rendering PHI unusable, unreadable or indecipherable to unauthorized individuals.
- Redaction is expressly excluded as a means of data destruction. However, HHS notes that a loss or theft of information that has been redacted may not require notification under the Rule either because the information is not PHI (as with de-identified information) or because (depending on the facts) the redacted information does not compromise the security or privacy of the information and thus is not a breach as defined.
- Clarification that covered entities and business associates should keep encryption keys on a separate device from the data they encrypt or decrypt.