

“What keeps you up at night?”

Saul Ewing Health Law
Practice Group:

George W. Bodenger
Chair

HHS issues interim final rule on health data breaches

By Scott D. Patterson, Evan J. Foster and Bruce D. Armon

On August 24, 2009, the Department of Health and Human Services (“HHS”) officially published its much-anticipated **Interim Final Rule on Breach Notification for Unsecured Protected Health Information**: <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>. HHS issued the rule to comply with a deadline in the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, part of the American Recovery and Reinvestment Act of 2009 (“ARRA”).

Although the HHS Rule is nominally an “interim” final rule that includes a request for comments, it becomes effective 30 days after publication (**September 23, 2009**). All “covered entities” and “business associates” subject to HIPAA will need to pay immediate attention to compliance. This includes health care providers, health plans, health care clearinghouses, third party administrators, claims processors, billing companies, and other service providers who have access to protected health information (“PHI”) governed by HIPAA.

The Federal Trade Commission (“FTC”) issued a companion Health Breach Notification Rule the week before, which is the subject of a separate Saul Ewing Update, http://www.saul.com/common/publications/pdf_2098.pdf. Saul Ewing's original Update on the HIPAA-related provisions of the HITECH Act can be found at http://www.saul.com/common/publications/pdf_1875.pdf.

BASIC ELEMENTS OF THE HHS RULE

The HHS Rule requires covered entities to notify affected individuals and HHS (and sometimes the media) following the “discovery of a breach of unsecured [PHI].” Business associates of a covered entity have similar obligations to notify the covered entity of such a discovery, so that the covered entity can provide further notices. The HHS Rule and accompanying background text provide detailed definitions and explanations of the critical terms “discovery,” “breach,” and “unsecured.”

Compliance personnel will need to familiarize themselves with the details of the new rule and its accompanying background document in order to make correct decisions, document them correctly, and develop appropriate risk assessment and response procedures. The HHS Rule does not require notification with respect to every network intrusion or every HIPAA violation.

For example, an entity could violate the HIPAA Security Rule by storing PHI on a completely insecure network but be lucky enough never to have its unprotected data viewed by unauthorized persons. Conversely, notices may be required even though the covered entity and its business associates have done their best to comply with HIPAA, as when a network reasonably secured by a firewall in compliance with the HIPAA Security Rule is penetrated by an intruder.

“UNSECURED” PHI

Notification is only required with respect to a breach of *unsecured PHI*. Data that is not PHI is excluded. This exclusion follows existing HIPAA PHI definitions and exclusions. Examples of excluded categories include health data that has been fully “de-identified” for HIPAA purposes and data that is not treated as PHI even though it includes “individually identifiable health information,” such as employment records in the possession of an employer. However, data in a partially de-identified HIPAA “limited data set” is not automatically excluded, because of the theoretical risk of “re-identification” of an individual from the remaining data. If a limited data set is compromised, the risk of re-identification must be factored into the overall risk assessment that the compromised entity must perform, as discussed below under “Breach.”

The Rule also exempts data that has been “secured” through encryption or destruction conforming to HHS guidance on “technologies and methodologies that render [PHI] unusable, unreadable, or indecipherable to unauthorized individuals” (as originally promulgated in April 2009 and updated in the HHS Rule.) HHS makes it clear that it is not amending the HIPAA Security Rule to require encryption of all PHI. However, failure to encrypt means that the data will be considered “unsecured,” so that unauthorized access or use may result in a breach requiring notification. In contrast, encrypted data exposed through an identical event would be useless to the intruder, and would not trigger notification obligations.

“BREACH”

A “breach” is “the acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which

compromises the security or privacy of the [PHI].” A violation of the Privacy Rule amounting to a breach can be as seemingly minor as “disclosures that impermissibly involve more than the minimum necessary information.” However, HHS added a “harm” element to its definition of “compromises the security or privacy of the [PHI],” which substantially mitigates the threat that inconsequential disclosures will trigger notification requirements. There is no “breach” unless the event “poses a significant risk of financial, reputational or other harm to the individual.” Entities that experience potential breaches have the burden of establishing there is no “significant risk of harm,” which means conducting a properly documented risk assessment, taking into account what information was compromised, who may have seen it, and what the potential consequences could be for affected individuals.

Certain events are specifically excluded if they do not result in further unauthorized use or disclosure, such as (i) unintentional access by a “workforce member” acting in good faith and in the scope of his or her authority, (ii) inadvertent disclosure to another person authorized to access PHI at the same entity, or (iii) disclosure to a person who “would not reasonably have been able to retain such information.”

This leads to a three-step analysis described by HHS as follows:

Based on the above, we envision that covered entities and business associates will need to do the following to determine whether a breach occurred.

First, the covered entity or business associate must determine whether there has been an impermissible use or disclosure of protected health information under the Privacy Rule.

Second, the covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the protected health information. This occurs when there is a significant risk of financial, reputational, or other harm to the individual.

Lastly, the covered entity or business associate may need to determine whether the incident falls under one of the exceptions in paragraph (2) of the breach definition.

“What keeps you up at night?”

“DISCOVERY”

A breach is “discovered” when it is “known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent” of the entity. This means that even a low-level temporary employee’s knowledge may be imputed to the covered entity or business associate, starting the notification clock.

“Agent” is used in its ordinary common-law sense, meaning someone empowered to act on another’s behalf.

HHS makes the point that employers in relevant businesses should make a point of educating all of their personnel on the importance of communicating as soon as they become aware that health data held by the employer may have been compromised. The HHS Rule also specifically expands existing HIPAA training requirements to obligate every covered entity to “train all members of its workforce” with respect to the new requirements “as necessary and appropriate” for those members to carry out their job duties.

NOTICE

The HHS Rule requires a notice to be written in “plain English” and to include, at a minimum, descriptions of the following:

- What happened and when (without providing a roadmap for future attacks);
- The kinds of information that were compromised (and perhaps those that were not, for example, name and patient account number were exposed, but not Social Security number or diagnosis);
- Steps individuals should take to protect themselves from potential harm as a result of the breach;
- What the entity is doing to investigate and mitigate the breach, and to prevent further breaches; and
- Contact procedures for obtaining additional information.

Individuals are to be notified by mail (or by email if they have consented to email notification). Substitute methods of notice are prescribed if the contact information is insufficient or out of date. If the breach involves 10 or more individuals, substitute notice must include a “conspicuous posting” for 90 days on the entity’s

website or “conspicuous notice” in major media in relevant geographic areas, and a toll-free phone number for inquiries. If the breach involves more than **500** individuals in a single state or jurisdiction, the entity must notify “prominent media outlets” serving that state or jurisdiction. Notice must be given “without unreasonable delay” and in any event no more than **60 days** after discovery of the breach.

PREEMPTION

State data breach notification laws (currently on the books in 45 states) are only preempted to the extent that compliance with both is “impossible” or if the state law “stands as an obstacle” to the HHS Rule. In general, HHS expects that entities will be able to harmonize multiple obligations by combining disclosures into a single notification document. States can also require notices to be issued sooner than the HHS Rule would require without creating a conflict. This approach gives states considerable latitude to supplement HHS’s requirements, so compliance personnel must pay attention to their state obligations as well as their federal ones.

IMPACT ON HIPAA BUSINESS ASSOCIATE AGREEMENTS

The HHS Rule will undoubtedly trigger a burst of revisions to existing HIPAA business associate agreements and service contracts, much as the companion FTC Rule will result in additional compliance covenants in agreements between healthcare providers and vendors of personal health records. Covered entities will want contractual assurances that their business associates will comply with all of their obligations under the new rules. In addition, HHS’s background text encourages covered entities and business associates to collaborate to streamline the administrative effort involved in notifications, for instance by having the covered entity delegate notification management to a service provider that may be better equipped for those administrative tasks.

CONCLUSION

Entities that already have mechanisms in place for dealing with data breaches should easily be able to comply with the new HHS Rule by adapting existing procedures, contracts, and workforce

training programs. Entities that have been slower to awaken to the advent of data breach notification laws will need to come up to speed in a hurry. While the 30-day deadline does not mandate immediate operational changes, entities that fail to prepare may have to scramble to handle a data breach “without unreasonable delay” as the HHS Rule requires. The recent transfer of enforcement responsibilities for the HIPAA Security Rule to the HHS Office for Civil Rights, enforcement-related statements from the current Administration, and accompanying increases in enforcement budgets and staffing, strongly suggest that HIPAA enforcement on all fronts is likely to become more aggressive in coming months.

This Alert was written by Scott D. Patterson, Evan J. Foster and Bruce D. Armon, members of the firm's Health Law Practice Group. Scott can be reached at 610.251.5089 or spatterson@saul.com; Evan can be reached at 610.251.5762 or efoster@saul.com and Bruce can be reached at 215.972.7985 or barmon@saul.com. This publication has been prepared by the Health Law Practice Group for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute “Attorney Advertising.”

© 2009 Saul Ewing LLP, a Delaware Limited Liability Partnership.
ALL RIGHTS RESERVED.