Bloomberg Law Reports® Health Law

New Federal Rules on Notifications of Breaches of Health Information Security: What Do They Mean for the Healthcare Industry?

Contributed by Nancy L. Perkins, Arnold & Porter LLP

Under new regulations recently issued by the U.S. Department of Health and Human Services (HHS)[1] and the Federal Trade Commission (FTC)[2] to implement the Health Information Technology for Economic and Clinical Health Act (HITECH Act), health care providers, health plans, and vendors of "personal health records," as well as business associates of these entities, have significant new obligations in the event of a breach of the security of health information under their control.[3] When a breach occurs, these entities must investigate the nature, cause and effect of the breach and, depending on the circumstances, notify all affected individuals as well the federal government and, in some cases, the media. Being prepared to fulfill these obligations is no easy task and entities subject to the new rules need to anticipate the substantial efforts that may be required to implement the policies and procedures that will ensure compliance.

As required by the HITECH Act, the two agencies' respective regulations took effect in mid-September, 2009. However, recognizing the burdens entailed in becoming compliant, both HHS and the FTC have delayed their enforcement until February 2010. Nevertheless, entities subject to the rules face exposure for noncompliance now, because state attorneys general have authority to bring civil actions on behalf of state residents who allegedly have been harmed by violations of the HITECH Act, including the breach notification requirements. Attorneys general may seek injunctive relief, statutory damages, and attorneys fees, with damages potentially running as high as $100 per violation or $25,000 for all violations of an identical requirement or prohibition during a single calendar year. Thus, despite HHS's and the FTC's delayed enforcement policies, entities covered by the breach notification rules should act quickly to ensure their compliance as soon as possible.

This article discusses the HHS regulation. A future article will discuss the FTC's regulation. The HHS regulation is an "interim final rule" and was not previously issued in proposed form. Accordingly, consistent with federal requirements for "notice and comment" rulemaking, HHS invited comments on the rule from the public until October 23, 2009. Some of those comments, including some from Members of Congress, urge HHS to make the rule more strict. Regulated entities need to bear that in mind as they prepare their compliance policies and practices, as HHS may decide to tighten up some of the existing rule's flexibility.

What entities and information are subject to the new HHS rule?

The HHS rule applies to all "covered entities" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which includes health care providers that conduct insurance-related electronic transactions, health plans, and health care

clearinghouses. The rule also applies directly to covered entities' "business associates."

The HHS rule applies to any "unsecured" protected health information (PHI), which means any individually identifiable health information that is "unsecured." Electronic PHI is "unsecured" under the rule if it is neither properly encrypted nor destroyed. Any other form of PHI is "unsecured" unless it is destroyed.

As specified in a Guidance issued by HHS in April 2009, to be properly *encrypted*, the information must have been transformed, through the use of an algorithmic process, "into a form in which there is a low probability of assigning meaning without use of a confidential process or key," and such process or key has not been breached.[4] The encryption methods verified by the National Institute of Standards and Technology (NIST)[5] meet this standard.

To be *destroyed*, electronic PHI must be "cleared, purged or destroyed" consistent with standards set forth by NIST. To destroy PHI in paper form, the medium in which the information is contained must be shredded or otherwise destroyed such that the PHI "cannot be read or otherwise be reconstructed."

Safe Harbors

Encrypting or destroying PHI therefore provides a "safe harbor" from the HHS breach notification requirements. In addition, if PHI is stripped of all of the 16 "direct identifiers" that must be removed to create a "limited data set," as defined in the HIPAA Privacy Rule, as well as any date of birth and any zip code, breach notifications also are not required.[6] Although the PHI will still technically be "unsecured" for HITECH Act purposes even with these identifiers removed, HHS believes that an impermissible use or disclosure of this information does not "compromise the security or privacy" of the PHI, because such use or disclosure would pose a low level of risk. HHS has specifically emphasized that this is a narrow exception to the breach notification requirement and that if, for example, the information does not contain birth dates but does contain zip code information, or contains both birth dates and zip code information, the exception will not apply.

For many HIPAA covered entities and business associates, it will not be feasible to encrypt or destroy all the PHI they maintain, or to strip the PHI of all the identifiers that must be removed to enjoy the "safe harbor" described above. For such persons and entities, policies and procedures must be established so that timely and adequate breach notifications can be provided in conformity with the HHS rule.

What is a "breach" under the HHS rule?

The trigger for the application of the HITECH Act's breach notification requirements is a "breach" of data security, so it is critical to understand what constitutes such a breach. With three limited exceptions, a "breach" of the security of PHI is broadly defined to include any "acquisition, access, use, or disclosure" of PHI that violates the HIPAA Privacy Rule and poses a significant risk of financial, reputational, or other harm to the individual. Thus, when a covered entity or business associate learns of

an acquisition, access, use or disclosure of PHI that was not clearly authorized, it must determine whether there was a violation of the Privacy Rule; if so, whether any of the three exceptions applies, and if no exception applies, whether the violation threatened any harm to an individual whose PHI was involved.

Regulatory Exceptions

The three exceptions to the "breach" definition are narrow. They apply when:

- PHI is unintentionally accessed, acquired, or used by a member of the workforce of a HIPAA covered entity or business associate in a work-related context and in good faith, where there is no further use or disclosure of the PHI.
- PHI is inadvertently disclosed by one individual who rightfully has access to the PHI to another individual at the same covered entity, business associate, or organized health care arrangement who also has the right to access PHI, as long as there is no further use or disclosure of the PHI.
- PHI is disclosed by a covered entity or business associate to an unauthorized person but the covered entity or business associate has a "good faith belief" that such person would not reasonably have been able to retain the PHI.

The first two exceptions essentially clarify that PHI disclosures within a covered entity or business associate itself generally do not trigger a notification requirement. For example, under the first exception, if a covered entity's employee responsible for patient billing were to receive and open an e-mail containing a patient's PHI that was mistakenly sent to the employee and, upon noting that she was not the intended recipient, alerted the sender of the message that it was misdirected and then deleted the message, the disclosure would not constitute a "breach" under the HHS rule. Although there was an unauthorized disclosure, it was unintentional and the billing employee's actions with respect to the PHI were in good faith, within the scope of authority, and there was no further use or disclosure in a manner not permitted by the Privacy Rule.

A similar analysis would apply to the second exception. With respect to that exception, HHS has clarified that it is intended to apply where PHI is shared among persons who each have the right to access PHI, but not necessarily the same PHI.

The third exception embodies HHS's modification of the HITECH's provision stating that a "breach" does not include situations where "an unauthorized person to whom [PHI] is disclosed would not reasonably have been able to retain [the PHI]." In its breach notification rule, HHS added the "good faith belief" standard with respect to concluding that PHI could not reasonably have been retained. This means that covered entities and business associates can rely on the exception based on their fair judgment of the surrounding circumstances. For example, if a clinician were mistakenly to give one patient another patient's prescription information but quickly recognize the error and retrieve the information, the clinician could reasonably conclude that the patient could not have read or otherwise retained the information. In contrast, had the information been sent to the wrong patient by mail or e-mail, and not returned as undeliverable, it would not be reasonable to reach such a conclusion.

With respect to all three exceptions, the covered entity or business associate has the burden to prove that the exception applies. Thus, it is critical for covered entities and business associates, to the extent they seek to rely on any of these exceptions, to document the facts involved with any unauthorized disclosure of PHI and the bases for the conclusion that the disclosure did not constitute a security breach.

Significant Risk of Harm

Assuming none of the "breach" definition exceptions applies, a covered entity or business associate needs to determine if the unauthorized access or disclosure poses a "significant risk of harm" to any individual whose PHI was involved. The covered entity or business associate carries the burden to demonstrate that there is no such risk, and should carefully document the bases for any conclusions in that regard. Among the factors HHS has suggested should be considered in performing a risk assessment are:

- Who impermissibly used or accessed the PHI? Does the HIPAA Privacy Rule or the HIPAA Security Rule,[7] or any similar statutory or regulatory protections for data privacy, apply to such person(s)? If so, the risk of harm will likely be less than in cases where no such stringent protections apply.
- What type and amount of PHI was subject to disclosure? Was it just a name and fact of visiting a dentist, or was it a record of an abortion or a prescription for AIDs medication, for example? In the former case, it would likely be reasonable to conclude there is a very low or nonexistent risk of harm; in the latter, such a conclusion would almost certainly be unreasonable. (Notably, use or disclosure of more PHI than the minimum amount necessary for an authorized purpose may, without more, constitute a "breach" for purposes of the notification requirements.)
- Was the PHI returned before there was an opportunity for it to be accessed for an improper purpose? For example, was the PHI contained on a laptop computer that was lost or stolen but then recovered, and a forensic analysis shows the file containing the PHI was not opened or transferred, or was the PHI in a file that, although recovered intact, was left lying in the patient waiting room of a busy clinic for an entire afternoon?
- Were steps taken to mitigate risk of harm, such as obtaining satisfactory assurances from the unauthorized recipient of PHI that the PHI will not be retained or further used or disclosed? If a written confidentiality agreement is obtained that provides commitments to that effect, for example, it may be reasonable to conclude that there is little or no risk to the individual(s) whose PHI was involved.

Criticism of Risk of Harm Standard

The "risk of harm" standard in the HHS breach notification rule has drawn sharp criticism. In a formal comment letter on the HHS rule, six Members of the House of Representatives asserted that the HITECH Act "does not imply a harm standard."[8] According to these Representatives, when the HITECH Act was being drafted, House Members "specifically considered and rejected such a standard," and instead "passed legislation that has a black and white standard for notification. The Members are urging HHS "to revise or repeal the harm standard provision included in its interim final rule at the soonest appropriate opportunity."

Similar views have been expressed by certain privacy advocates in comment letters and otherwise.[9] Members of the health care industry, in contrast, strongly support the risk-of-harm standard, noting that such a standard has been endorsed by numerous state legislatures in their own their breach notification laws. Industry members also argue that the standard serves consumer's interests by preventing unnecessary and unwarranted anxiety to individuals caused by notifications of breaches that actually pose little or no risk of harm. In the industry's view, the time and resources devoted to such excessive notifications can better be channeled into improving technological and other means of strengthening measures to prevent breaches of security from occurring in the first place.

It remains to be seen how HHS will respond to these conflicting views. It seems reasonable to assume that the agency may seek to modify the standard in some respect, or at least to clarify the justification for retaining it. In the meantime, HIPAA covered entities and their business associates should prepare to adjust their compliance policies and procedures in the event that HHS might decide to eliminate the standard. Should that occur, the notification requirements would be applicable in virtually all instances of a disclosure of PHI in violation of the Privacy Rule that involves receipt of the information by any person or entity other than the covered entity or business associate responsible for the disclosure.

What is involved in providing breach notifications?

For HIPAA covered entities, there are several components to the breach notification requirements of the HITECH Act:

- *First*, a covered entity that experiences a breach must notify HHS *immediately*, unless the breach involves PHI regarding less than 500 individuals, in which case the covered entity may report it to HHS as part of an annual notification of all such security breaches in the prior year.
- *Second*, the covered entity must notify each individual whose PHI was involved without "unreasonable delay," and in any event within *no more than 60 days after discovering the breach*. The burden is on the covered entity to demonstrate why any delay in notification was "reasonable."[10]
- *Third*, if more than 500 individuals are affected in a particular area, the covered entity must notify prominent media outlets serving that area.

Required notifications to individuals and the media must include all of the following information:

- a brief description of what happened and what the covered entity is doing in response;
- a description of the type(s) of PHI involved;
- guidance on what affected individuals can do to protect against resulting harm;
- a contact point for individuals to obtain more information.

HHS will post on its website a list of each covered entity involved in a breach affecting more than 500 individuals, and must provide annual reports to Congress summarizing the statistics on all the breaches that occurred within the prior year.

Under the parallel breach notification requirements for HIPAA business associates, a business associate that discovers a security breach must notify the *covered entity* from which (or on behalf of which) the business associate obtained the PHI at issue. As with respect to covered entity notifications, business associate notifications must be made without "unreasonable delay" and in any event within 60 days of the date when the breach was discovered by the business associate, a member of its workforce, or any of its agents. The notification must include an identification of each affected individual, and also should describe the circumstances of the breach sufficiently to enable appropriate covered entity to undertake its required notifications, as described above, as well as any other protective measures, including possible modification or even termination of the business associate relationship.

Discovery of a Breach

The HHS rule deems a breach to be discovered by a covered entity as of the first day the breach is "known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity." Thus, a covered entity is not liable for failing to provide notification in cases where it was not aware of a breach, unless the covered entity would have been aware of the breach if it had exercised reasonable diligence. "Reasonable diligence" means the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."

The HHS rule imputes to a covered entity the knowledge of any member of the covered entity's workforce (other than the person committing the breach), as well as the knowledge of any agent of the covered entity. Thus, as soon as such workforce member knows or would, with reasonable diligence, have known of a security breach, the covered entity also "knows" of the breach. Whether a person or entity is an "agent" of a covered entity is to be determined under the federal common law of agency. Under that standard, some — but not likely all — business associates of covered entities will also be "agents" of the covered entity, which means a breach discovered by those particular business associates will be deemed "known" by the covered entity when they are discovered by the business associate, *not* when the business associate notifies the covered entity of them at some later time. This means that covered entities should undertake to determine, with the assistance of legal counsel, which of their business associates qualify as "agents" — and they should undertake this *before* they are faced with an actual data breach discovered by the business associate.

60-Day Notification Period

With respect to investigations of breaches for purposes of determining whether notifications are required, it is critical to understand that the maximum 60-day time period for notification begins when the incident is first *known*, *not when the investigation of the incident is complete*, even if it is initially unclear whether the

incident constitutes a breach under the HHS rule. Also important to recognize is that the duration of the investigation cannot take an "unreasonable" amount of time, because, as noted above, the HITECH Act requires notice to be provided without "unreasonable delay." Even though reasonable delay could potentially delay notice until 60 days after discovery of the breach by a covered entity (but no more), the 60 days is an outer limit and it may well be deemed "unreasonable" to wait that long — or possibly even half that long, depending on the circumstances. For example, if a covered entity has compiled the information necessary to provide notification to individuals on day 10 but waits until day 60 to send the notifications, it would constitute an unreasonable delay despite the fact that the covered entity has provided notification within 60 days. To ensure that any delay in notification can be justified, covered entities and business associates should document in detail the steps taken in the course of breach investigations, as it will be their burden to prove that the delay was not "unreasonable."

How Does the HHS Rule Relate to State Breach Notification Laws?

The HHS rule preempts *contrary* state breach notification laws, but not those that are substantively consistent with the rule. For example, if a state law requires notice of a security breach within 10 days after discovery of the breach, a covered entity's compliance with that law will be required despite the HHS's rule's allowance of a "reasonable delay" in notification of up to 60 days. Likewise, if a state law requires information to be included in a breach notification beyond what is required by the HHS rule, or requires that certain information be presented or described in a certain way, HHS considers there to be no conflict between the state law and its rule. In HHS's view, there is no preemption in this situation because covered entities can develop and provide a notice that satisfies both federal and state law.

What immediate steps should regulated entities take in response to the new rules?

The first and most important step covered entities and business associates can take to avoid the requirement to provide breach notifications is to prevent security breaches from occurring at all. That means encrypting electronic PHI wherever possible and implementing strict data retention procedures to ensure prompt destruction of such information not required to be maintained under applicable document retention laws. Next, regulated entities should undertake an audit of all of their policies and procedures used to protect electronic PHI in accordance with the HIPAA Security Rule, as well as the mechanisms by which they protect the privacy and security of such information in other forms.

In addition, recognizing the burdens of the requirements that must be adhered to in the event there is a security breach, regulated entities should commence immediately to develop notification protocols, including procedures for the particular types of required notifications. They should ensure that contact information for individuals exists and is up-to-date, and draft sample notifications to individuals, the government, and media. Covered entities also may want to amend their agreements with business associates to require particular notification procedures in the event the business associate experiences a security breach. In the event of a breach, regulated entities will not be excused for delay in notification on the ground that necessary

notice procedures had not previously been formalized. And of course, training of workforce members, as well as agents with access to PHI, will be critical to ensure compliance with the new HHS rule.

Nancy L. Perkins is a counsel in the Washington, D.C. law firm Arnold & Porter LLP. Ms. Perkins regularly advises clients on federal and state requirements for privacy and security of medical, financial, and electronic data. She has particular expertise in the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act, and their implementing regulations. She also has an extensive background in international law and advises clients on the rapidly developing framework for global protection of data privacy and security. Ms. Perkins can be reached at nancy.perkins@aporter.com.

---

[1] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (2009) (to be codified at 45 C.F.R. Parts 160 and 164).

[2] Health Breach Notification Rule, 74 Fed. Reg. 42,962 (to be codified at 16 C.F.R. Part 318).

[3] The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

[4] The HHS Guidance is published at 74 Fed. Reg. 19,006 (2009).

[5] The NIST standards are available at http://www.csrc.nist.gov/.

[6] The 16 "direct identifiers" are, with respect to both the subject of the information and all relatives, employers, and household members of that individual: (1) names; (2) postal address information, other than town or city, state, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) Social Security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license numbers; (11) vehicle identifiers and serial numbers, including license plate numbers; (12) device identifiers and serial numbers; (13) Web URLs; (14) IP address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

[7] Standards for Security of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subpart C.

[8] The Members' letter to Sebelius is available at http://energycommerce.house.gov/Press_111/20091001/sebelius_letter.pdf/.

[9] *See, e.g.*, Angela Moscaritolo, *Privacy groups blast new health care notification rule*, SC Magazine, Sep. 22, 2009, *available at* http://www.scmagazineus.com/Privacy-groups-blast-new- health-care-notification-rule/PrintArticle/149444/; *HHS guts health-care breach notification law, groups warn*, Computerworld, Sept. 23, 2009, *available at* http://www.infowatch.com/en/press/news/risks/2697/.

[10] Notification may (and should) be delayed at the request of law enforcement if it would impede a criminal investigation or undermine national security.