Bloomberg Law Reports® Health Law

Heath Information Security: Complying With Federal Breach Notification Requirements as a Newly Regulated Entity

Contributed by Nancy L. Perkins, Arnold & Porter LLP

On February 22, 2010, the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) will commence enforcement of new regulations[1] implementing the security breach notification requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[2] According to a recent survey of entities subject to the new regulations, approximately 25 percent of health care providers are unaware of their obligations under the new HHS rule, and an even greater percentage of their "business associates" – service providers such as data management companies, billing services companies, and laboratory analysts – do not realize they too are directly subject to the new rules.[3] Even more striking, as few as 40 percent of those surveyed are not aware of the FTC's rule, which applies to vendors of "personal health records" (PHRs), "PHR related entities," and service providers of such vendors/entities.[4]

As described in a prior article focusing primarily on the HHS rule,[5] entities subject to either agency's rule face significant new obligations in the event of a breach of the security of health information under their control. When a breach occurs, regulated 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 requires considerable work, including establishing written policies and procedures and training staff. This article focuses on its scope and specific standards of the FTC regulation, including the timing and content requirements for the notices to individuals and others.

The possibility of a data security breach within healthcare organizations should not be underestimated. Indeed, according to a recent survey, 80 percent of healthcare-related entities has had one or more breaches of security involving the loss of patient health information.[6] Of those that had a data security breach, 33 percent reported that more than 90 percent of the data involved was electronic health information stored on databases.[7] This underscores how critical it is for entities subject to the HHS and/or FTC rules to take all possible steps to improve their data security protection policies and procedures, and to be ready to comply with the breach notification rules in the event those policies and procedures prove insufficient. Both HHS and the FTC have authority to impose heavy penalties for violations of their respective rules, ranging from $100 to $50,000 per violation (up to $1.5 million within a single year). Moreover, state attorneys general also can seek damages through civil actions on behalf of state residents, with potential recoveries of as much as $100 per violation or $25,000 for all violations of a particular requirement during a single calendar year.

To whom does the FTC rule apply?

The FTC rule applies to all PHR "vendors," "PHR related entities," and "third party service providers." A PHR is an "electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." The FTC rule defines a PHR "vendor" as "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains" a PHR. Typical examples of PHR vendors are websites such as WebMD, Google Health, and Microsoft's HealthVault, which allow individuals to set up on-line, private records of their health information and to update, monitor, and track the progression of diseases, dietary changes, use of medications, etc. Key to the definition of a PHR is its limitation to *electronic* records maintained "by or primarily for the *individual.*" Paper records and electronic records maintained by an entity for its own business use (such as insurance records held by an insurer), are not "PHRs" under the FTC rule.

A "PHR related entity" is an entity that: (1) offers products or services through the website of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals PHRs; or (3) accesses information in a personal health record or sends information to a personal health record. A web-based application that helps consumers manage medications, or an entity that advertises drugs or devices online, is a PHR-related entity. PHR-related entities also include online applications through which individuals connect devices such as blood pressure cuffs, blood glucose monitors, or other types of devices that allow them to track their health status or progress in treating certain conditions, such as a weight-tracking or online medication program that extracts information from PHRs. In addition, Internet search engines that appear on PHR websites are PHR-related entities and, to the extent they collect unsecured PHR identifiable health information at those websites, they are subject to the FTC's breach notification rule.

A "third party service provider" under the FTC rule is "an entity that (1) provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR-related entity in connection with a product or service offered by that entity; and (2) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services." These types of entities are akin to business associates of "covered entities" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to whom the HHS breach notification rule applies. Third party service providers include, for example, entities that provide data storage, billing, debt collection, or accounting services to vendor of PHRs or a PHR-related entity, to the extent that in providing such services they have access to individually identifiable health information.

The FTC takes the position that any foreign PHR vendors, PHR-related entities, or third-party service providers that maintain information for U.S. citizens or residents are subject to its rule, as well as U.S.-based entities that meet any of these definitions. The FTC also deems non-profit organizations and other entities outside

the scope of its traditional jurisdiction under the Federal Trade Commission Act to be subject to the rule to the extent they act as PHR vendors, PHR-related entities, or third-party service providers.

What information is subject to the FTC's breach notification requirements?

Pursuant to the HITECH Act, the FTC rule specifically limits its breach notification requirements to breaches involving "unsecured PHR identifiable health information" in a PHR.

"PHR identifiable health information" means any health information that: (1) is provided by or on behalf of an individual; and (2) identifies or could be used to identify an individual. However, because the FTC rule requires notifications of breaches only to the extent information is in a PHR, and PHRs by definition are electronic records, the rule's breach notification requirements apply only to electronic information.

PHR identifiable health information is "unsecured" unless it is properly encrypted or destroyed. As specified in a Guidance issued by HHS in April 2009,[8] 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 the confidentiality of the process or key must not have been breached. Data that have been encrypted in accordance with the methods verified by the National Institute of Standards and Technology (NIST)[9] meet this standard of transformation. To be destroyed, PHR identifiable health information must be "cleared, purged or destroyed" consistent with the NIST standards. Because active PHRs must be accessible for individual viewing, they will necessarily be "unsecured."

What constitutes a breach of the security of PHR identifiable health information?

Although some instances involving disclosure of health information would very obviously be considered breaches of the security of the information, other, less obvious circumstances also may constitute breaches under the FTC rule. The rule defines a "breach of security," with respect to unsecured PHR identifiable health information of an individual in a personal health record, as any "acquisition of such information without the authorization of the individual." The term "acquisition," therefore, is a key one. Although it is not separately defined in the FTC rule, "acquisition" is distinguished from "access" for purposes of the rule. Specifically, access to information in this context means the *ability* to view or read information, whereas acquisition of information means the actual act of viewing the information.

For example, a breach of security would *not* be deemed to have occurred if an employee of a PHR vendor, PHR-related entity, or service provider were to inadvertently open an individual's PHR (gaining access) but then quickly logged out of the PHR without reading, using, or disclosing any of the data in it. In this case, the employee would not be deemed to have acquired anything in the PHR. If, however, the employee did read any identifiable information in the PHR, or disclosed the

information to others, there would have been an acquisition of the information for purposes of the rule and, thus, a breach that would be subject to notification.

Although only unauthorized *acquisition* of unsecured PHR identifiable health information constitutes a breach, the FTC will *presume* that there has been an unauthorized acquisition in the event of unauthorized access to unsecured PHR identifiable health information, unless the vendor of personal health records, PHR related entity, or third party service provider involved with the incident can produce "reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." To rebut this presumption, it is incumbent upon the entity involved to document that, despite a compromise of PHR security, no actual viewing of PHR identifiable health information occurred.

The FTC is likely to be quite strict, but not unreasonable, about what it takes to rebut this presumption. For example, an employer would not be required to provide notification of a breach if the employer could show that an employee who opened a PHR without authorization followed company policies by reporting such access to his or her supervisor and affirming that he or she did not read or share the data, and that the employer conducted a reasonable investigation to corroborate the employee's version of events.

Likewise, if an employee lost a laptop outside the workplace or other private area, the presumption would be that the information was impermissibly acquired, but if the employer could show that the laptop was recovered, and a forensic analysis proved that files were never opened, altered, transferred, or otherwise compromised, that would serve to rebut the presumption. However, if an employee were accidentally to send an e-mail containing PHR identifiable health information to multiple recipients, there would likely be no way to rebut the presumption of acquisition, even if the employee immediately recalled the e-mail and asked the recipients to delete it. According to the FTC, in the context of widely distributed e-mail, there can be no reasonable expectation that no one acquired the information.

Must notifications be provided even if the breach poses no risk of harm?

Yes, under the FTC rule, although not under the HHS rule. HHS included in its rule a "risk of harm" threshold for required notifications. For entities subject to the HHS rule, there is no requirement for notification of a compromise of the security of an individual's information unless the incident "poses a significant risk of financial, reputational, or other harm to the individual." This standard, which is not part of the HITECH Act itself, is highly controversial and its inclusion in the HHS rule was opposed by privacy advocates as well as certain Members of Congress. The FTC was urged by many industry representatives to adopt such a standard, but refused to do so. According to the FTC, "harm in the context of health information may be different from harm in the context of financial information," and that the former, but generally not the latter, can cause irreversible damage. "Because health information is so sensitive," the FTC designed its standard for breach notification to "give companies the appropriate incentive to implement policies to safeguard such highly-sensitive information."[10]

How soon must notice be provided after a breach occurs?

In all cases, notices are to be provided as soon as practicable, within certain outer limits from the date a security breach is discovered.

- *Notices to the FTC*. If a breach involves information on more than 500 individuals, the PHR vendor or PHR-related entity experiencing the breach (or whose service provider experienced the breach) must notify the FTC within 10 business days. If the breach involves information on less than 500 individuals, it can be notified to the FTC as part of an annual log describing all of the PHR vendor or PHR-related entity's reportable security breaches in the prior year.
- *Notices to Individuals*. Each individual whose involved a security breach must be notified of the breach without "unreasonable delay," and in any event within no more than 60 days after the responsible PHR vendor or PHR related entity discovered the breach. The burden is on the regulated entity to demonstrate why any delay in notification was reasonable.[11]
- *Notice to the media*. If more than 500 individuals are affected in a particular state or smaller jurisdiction (e.g., a county, city, or town), the responsible PHR vendor or PHR related entity must notify prominent media outlets serving that area no later than 60 days after discovering the breach, but without unreasonable delay during that time period.

To ensure compliance with these requirements, it is critical to understand when a breach is deemed to be "discovered." Under the FTC rule, a breach is discovered by a PHR vendor, PHR-related entity, or service provider as of the first day the breach is known or reasonably should have been known to that organization. And, for each PHR vendor, PHR-related entity, or service provider, its "knowledge" of a breach is deemed to include the knowledge of any of its employees, officers, or agents (other than the person committing the breach).

It may not always be obvious to a PHR vendor or PHR-related entity whether others with whom it deals are its agents. Under common law rules of agency, certain criteria render a person or entity an agent, which suggests that PHR vendors and PHR-related entities should consult with legal counsel, well before any breaches occur, to identify their agents. Service providers may themselves be agents of a PHR vendor or PHR-related entity and, as such, their knowledge of a security breach would be imputed to a PHR vendor or PHR-related entity irrespective of the notice they are required to provide to the vendor/entity. Thus, PHR vendors and PHR-related entities cannot necessarily wait for their service providers to notify them of security breaches for discovery timing purposes.

PHR vendors and PHR-related entities should establish, as soon as possible, special means for monitoring and communicating with those entities concerning data security. First, PHR vendors and PHR-related entities should ensure that each agent and/or service provider is aware that the vendor/entity is regulated by the FTC rule, which creates responsibilities that creates for the agent/service provider. Next, the PHR vendor or PHR-related entity should consider contractually binding the agent/service provider to provide notice of a security breach within a day or two after the agent/service provider learns of the breach. Although this cannot ensure

notification of all breaches of security of which the agent/service provider "reasonably should have been" aware, it can reduce the likelihood that the PHR vendor or PHR-related entity will fail to fulfill its own notification obligations.

Notably, the maximum 60-day time period for notification to individuals and the media begins when an incident of unauthorized access to PHR identifiable health information is first known, not when (if later) it is determined that there was also unauthorized acquisition (and hence a breach). Thus, regulated entities must provide notice without reasonable delay, and in no event later than 60 days, after discovering an incident of unauthorized access, even if it may take days or weeks after that to investigate whether there actually was a security breach. It is the burden of the regulated entity to show that its notifications were provided without unreasonable delay, and therefore documenting all actions between the time of discovery of an incident of unauthorized access and the time of notification can be essential to avoid liability.

What must breach notifications contain and how should they be delivered?

Required notifications to individuals and the media must include: 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; and, a contact point for individuals to obtain more information.

Notices to individuals must be in plain language. The notice must be provided in writing by first-class mail to the individual's last-known address, unless the individual has opted to receive notice by e-mail. In circumstances where there are 10 or more individuals who cannot be reached after reasonable efforts to make contact, notice must be provided either by either a conspicuous posting on the website of the PHR vendor or PHR related entity's home page, or notice in major print or broadcast (TV or radio) media, for a period of 90 days. As the FTC has noted, because PHRs generally involve an online relationship with individuals, web postings may be a particularly well-suited method of substitute notice under its rule.

Notifications by service providers to PHR vendors and PHR-related entities 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.

Notices to the FTC are to be provided on a form available on the FTC website, www.ftc.gov.

Does the FTC rule preempt state breach notification requirements?

The FTC 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 FTC'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 FTC rule, or requires that certain information be presented or described in a certain way, so long as it is possible to comply with both the federal and state requirements, the FTC considers there to be no conflict between them and, thus, no preemption. Accordingly, if a state breach notification law requires a notice to contain, for example, contact information for consumer reporting agencies, or warnings to monitor credit reports, PR vendors and PHR related entities must comply with the state requirements irrespective of the FTC rule.

What steps should regulated entities take to be ready to comply by February?

The first and most important step entities subject to either the FTC rule can take to avoid the requirement to provide breach notifications is to prevent security breaches from occurring at all. Besides encrypting electronic identifiable health information wherever possible, regulated entities should undertake regular audits of their policies and procedures used to protect such information in accordance with the standards such as the HIPAA Security Rule.

In addition, regulated entities should commence immediately to develop notification protocols, including procedures for the particular types of required notifications, ensuring that contact information for individuals exists and is up-to-date, and drafting sample notifications to individuals, the government, and media. As discussed above, alerting business associates and agents of their notification requirements under the new rules also is critical to prevent lack of awareness of security breaches from precluding timely notification. In the event of a breach, regulated entities will not be excused for delay in notification on the ground that such related entity relationships and contact procedures had not previously been formalized. Finally, training of all employees with access to identifiable health information regarding their security obligations is essential to ensure compliance with the new rules.

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) (HHS rule); Health Breach Notification Rule, 74 Fed. Reg. 42,962 (to be codified at 16 C.F.R. Part 318) (FTC rule).

[2] Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

[3] 2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security (Nov. 2009) at 9,*available at* http://www.himssanalytics.org/docs/ID_Experts_111509.pdf.

[4] *Id.*

[5] *See* Nancy L. Perkins, *New Federal Rules on Notifications of Breaches of Health Information Security: What Do They Mean for the Healthcare Industry?*, Bloomberg Law Reports: Health Law, Nov. 2009.

[6] Ponemon Institute, *Electronic Health Information at Risk: A Study of IT Practitioners* (Oct. 15, 2009), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Electronic%20Health%20Information%20at%20Risk%20FINAL%201.pdf, at 5–6.

[7] *Id.* at 6.

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

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

[10] 74 Fed. Reg. at 42,966.

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