Until now, the loss or theft of protected health information rarely resulted in notice to consumers. Very few state data security breach notification laws encompass medical information. The Health Insurance Portability and Accountability Act ("HIPAA") merely required an "accounting" of such events to a patient upon the patient's request.

All that has changed. Congress, in enacting the Health Information Technology for Economic and Clinical Health Act ("HITECH"), imposed breach notification obligations on many of the individuals and business entities that receive, create, or maintain patients' individually identifiable health information. Pursuant to HITECH, on Aug. 17, the Federal Trade Commission ("FTC") issued its Health Breach Notification Rule, governing the breach notification obligations of three new categories of entity: "vendors of personal health records," "PHR related entities" and "third party service providers."

Although the rule is effective Sept. 24, 2009 (applying to breaches of security that are discovered on or after Sept. 24, 2009), the FTC will use its enforcement discretion to refrain from bringing an enforcement action for failure to provide the required notifications for breaches that are discovered before Feb. 22, 2010. The FTC expects regulated entities to use this time to come into full compliance with the
rule, which ushers in a very rapid, very public breach disclosure regime for entities suffering the loss or theft of personal health records.

In addition to the FTC regulations, the Department of Health & Human Services ("HHS") has issued similar regulations that set forth the security breach notification obligations of HIPAA-covered entities and business associates. Although the framework of the two regulations are similar in nature, each regulation merits separate discussion in light of the distinct entities each regulation governs. Reed Smith will discuss the HHS regulation, as well as the manner in which the FTC and HHS regulations interrelate, in a forthcoming memorandum.

Who will be impacted by the rule?

Under the FTC's rule, a "vendor of personal health records" is an entity other than a HIPAA-covered entity or business associate "that offers or maintains a personal health record." In turn, the regulations define a "personal health record," or "PHR," as 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." "PHR identifiable health information" is defined as "individually identifiable health information [as defined under HIPAA], and with respect to an individual, information (1) [t]hat is provided by or on behalf of the individual; and (2) [t]hat identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."

In its news release accompanying the rule, the FTC describes vendors of PHRs as companies that "provide online repositories that people can use to keep track of their health information." The definition of "vendors of PHR," however, leaves much room for confusion. For example, many employers (that are not HIPAA covered entities or business associates) maintain electronic files that contain identifiable health information pertaining to employees. Is such information managed "primarily for the individual," making such an employer a vendor of PHRs? Case-by-case determinations will need to be made as to which business processes subject companies to the FTC's rule on breach notification.

The new rule defines the other regulated entity classifications in an equally complex manner. A "PHR related entity" is one that:

- Offers products or services through the website of a vendor of personal health records
- Offers products or services through the websites of HIPAA-covered entities that offer individuals personal health records, or
- Accesses information in a personal health record or sends information to a personal health record

The effect of the third prong of this definition may lead to a very broad application of the FTC's new rule, and thereby foist security breach notification obligations onto many businesses that otherwise would not have needed to comply. In an attempt to clarify the types of businesses that will be classified as a PHR-related entity, the FTC has stated that PHR-related entities include a web-based application that helps consumers manage medications, a website offering an online personalized health
checklist, and a brick-and-mortar company advertising dietary supplements online.

The third category of regulated entities under the rule, "third party service provider," is defined as an entity that (a) provides services to a vendor of PHRs, or to a PHR-related entity in connection with the offering or maintenance of a PHR; and (b) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services. According to the FTC, examples of a third-party service provider include entities that provide billing, debt collection, or data storage services to vendors of PHRs or PHR-related entities.

What counts as a "breach of security"?

Vendors of PHRs, PHR-related entities, and third-party service providers will have an obligation, once the rule is effective, to notify consumers upon any "breach of security" of unsecured identifiable health information that is in a PHR. Under the rule, "breach of security" is defined as the "acquisition of [unsecured identifiable health information that is in a personal health record] without the authorization of the individual." A non-exhaustive list of events that fall within the definition would include misuse of records by an employee, theft and loss of a laptop containing such records, or remote intrusion into an electronic database by a hacker.

Do companies have to provide notice of the loss or theft of encrypted information?

Note that the rule applies only to "unsecured" information. PHRs that are "secured" using a technology or method specified by HHS guidelines will not give rise to notification obligations, even if acquired by unauthorized parties.

Is the loss or theft of paper records included under the rule?

No, per the text of the HITECH Act, only electronic records are covered for vendors of PHRs, PHR-related entities, and third-party service providers. As such, the FTC regulations do not apply to paper records.

What does the notice have to say?

The notice must include a description of what happened, the date of the breach, date of discovery of the breach, the types of unsecured PHI involved, steps the individual should take, steps the entity took or is taking to investigate and/or mitigate, and contact procedures for individuals with more questions.

To whom must the notice be provided?

The rule requires vendors and PHR-related entities to notify the consumer directly. Third-party service providers must notify the vendor or PHR-related entity for which it provides services.

How long do companies have to provide notice?

All notifications required by the rule must be made "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security."
Does the company sending notice need to notify anyone other than the consumer?

Depending on the nature of the breach, yes. If a breach involves the records of more than 500 residents of a state or jurisdiction, notice must be provided to "prominent media outlets serving" that state or jurisdiction. If the breach involves the records of more than 500 people total, the entity providing notice must notify the FTC. The FTC will notify HHS, which will post an announcement to its website.

What happens if the party sending notices does not have current addresses?

The rule imposes publication notice requirements unlike anything in the state data security breach notification laws. If the vendor's contact information for 10 or more consumers is out-of-date, the vendor must resort to publication notice. This entails a "conspicuous posting for a period of 90 days on its website" or notice "in major print or broadcast media."

What does a company do when the facts surrounding the potential breach are unclear?

In many instances, companies facing a potential breach can ascertain only that someone gained unauthorized access to their records, but are unable to tell what, if anything, was actually viewed. In these situations, the FTC has commented that the definition of a security breach includes a rebuttable presumption of unauthorized acquisition, such that absent "reliable evidence showing that there has not been or could not reasonably have been" unauthorized reading, use, or disclosure of the information, it will be presumed that unauthorized acquisition of the data in question has occurred.

Does the rule's standard for notification take risk of harm into account?

The rule provides specific exemptions for certain instances of data theft, loss, or unauthorized access where risk of harm is minimal. For example, no notice is required where the data has been encrypted per the methodology set forth by HHS, provided that the encryption key remains secure. To take another example, notice is not required under the rule in the case of inadvertent unauthorized access by a company's employee if: (1) the employee follows company policies by reporting the incident to the company; (2) the employee affirms that he did not read or share the data; and (3) the company conducts a reasonable investigation to corroborate the employee's version of events.

The FTC cites to this latter exemption as evidence that the rule's "standard does take harm into account." But the FTC goes on to note that "harm in the context of health information may be different from harm in the context of financial information," and that, "[b]ecause health information is so sensitive, the Commission believes the standard for notification must give companies the appropriate incentive to implement policies to safeguard such highly sensitive information."

Does the rule require notification even when the information discloses no
connection to a health condition or health care transaction?

The HITECH Act left considerable room for debate as to what constitutes a PHR. For example, in its proposed security breach notification rule, the FTC took the position that the regulations would cover a security breach of a database containing names and credit card information, "even if no other information was included." Many commenting on the proposed rule commented that the loss or theft of a database that evidences no connection to health conditions or health care services should not require consumer notice. The FTC changed its mind in light of this commentary, and provided in its final rule that "[t]he Commission is persuaded that name and credit card information alone is not PHR identifiable health information. However, as noted above, if the disclosure of credit card information identifies an individual as a customer of a vendor of personal health records or related entity associated with a particular health condition, that information would constitute 'PHR identifiable health information.'"

Who will enforce the FTC's rule?

The HITECH Act grants a broad enforcement authority to the FTC. Entities that are typically beyond the agency's jurisdiction under FTC Act § 5 are subject to the final rule. This includes nonprofits and educational institutions, so long as they qualify as entities regulated by the rule. The HITECH Act also authorizes the FTC's commencement of an action to recover civil penalties for violations of up to $10,000 for each violation of the rule.

© Copyright 2019 Reed Smith. All rights reserved.