Proskauer

HHS and FTC Announce New Breach Notification Rules for Unsecured Protected Health Information

September 2009

On August 24 and 25, 2009, the Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC"), respectively published rules on when and how covered entities regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and vendors of personal health records ("PHR") must notify individuals of security breaches concerning their unsecured protected health information ("PHI"). With its rule, HHS also provided guidance on securing PHI through "encryption" and "destruction" measures. While compliance with these security measures is not required, conformance to the guidance offers a relative safe harbor for covered entities and vendors in the event of a security breach.

In general, the HHS interim final rule (*74 Fed. Reg. 42740*, to be codified at 45 CFR pts. 160, 164) applies to HIPAA-covered entities and their business associates, while the FTC rule (*74 Fed. Reg. 42962*, to be codified at 16 CFR pt. 318) applies to PHR vendors, such as Google Health and Microsoft's Health Vault and their third-party service providers. Both rules implement provisions of the American Recovery and Reinvestment Act of 2009 ("ARRA"), the large economic stimulus bill signed into law by President Obama on February 17, 2009.

The HHS Rule

HSS issued its interim final rule pursuant to the Health Information Technology for Economic and Clinical Health Act ("HITECH"), a part of ARRA. HITECH's prescriptive language gave HHS little discretion in how to implement the statute. Thus, the HHS interim final rule closely mirrors the statutory language. HHS offers one major point of clarification, however, by including a "risk of harm" threshold, which allows a covered entity to consider the potential harm of a security breach to affected individuals before triggering the notification requirements. This threshold is discussed in more detail below.

The HHS rule requires HIPAA-covered entities to provide affected individuals with timely notice (i.e., no later than 60 days) upon the discovery of a breach of their "unsecured" PHI. Generally, a covered entity is subject to the HHS notification obligations when:

(1) an individual's PHI has been breached; (2) the PHI was "unsecured"; and (3) such breach poses significant risk of financial, reputational or other harm to the individual. These elements are also discussed in more detail below.

The HHS regulations mandate that notice include certain information, including a brief description of the event that led to the breach, the specific PHI involved, and the steps affected individuals should take to protect themselves from further harm. In cases where such a breach involves more than 500 individuals, the covered entity is required to notify the media as well as the HHS Secretary. Breaches involving fewer than 500 individuals must be reported to the HHS Secretary on annual basis. Business associates of covered entities (e.g., third-party administrators, pharmacy benefit managers) also are required to notify a related covered entity upon the discovery of a breach of unsecured PHI. The covered entity then must provide the affected persons with notice.

The existing business associate contract requirements already mandate that business associates notify covered entities of security incidents and unauthorized uses and disclosures. These requirements should be broad enough to include notification of breaches of unsecured PHI, as contemplated by HITECH and the HHS regulations. However, covered entities may wish to modify or expand these contractual notice obligations so as to ensure that covered entities can comply with the details of their regulatory obligations to notify individuals (as well as HHS and, as applicable, the media). Covered entities also may want to modify such agreements to ensure that business associates cover the costs of the required notice to individuals and media, as applicable.

Breach

A breach is generally defined as the unauthorized acquisition, access, use or disclosure of protected health information that violates HIPAA's Privacy Rule and compromises the PHI's security or privacy.

HHS provides for three exceptions to the definition of "breach." These are:

1) the unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the covered entity or business associate (*e.g.,* a nurse mistakenly sends a billing employee an e-mail containing a patient's PHI);

2) the inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate; and

3) disclosures in which an unauthorized recipient would not reasonably have been able to retain the PHI (e.g., if a covered entity mistakenly sends a explanation of benefits to the wrong individual, which is then returned by the Post Office, unopened, as undeliverable).

Encryption, Destruction Guidance

Since notice must only be provided for breaches of “unsecured” PHI, there is no obligation to provide notice for breaches of “secured” PHI. To qualify as secured, a covered entity must use a technology or methodology specified by the Secretary of HHS to safeguard the PHI so that it is “unusable, unreadable, or indecipherable to unauthorized individuals.” The interim final rule repeats guidance issued by HHS in April 2009 (74 R 19006). The guidance specifies the HIPAA Security Rule’s encryption standard as the appropriate methodology for safeguarding electronic PHI (as well as PHR-identifiable health information). Hard copy PHI, such as paper, film or other media, must be shredded or destroyed so that the PHI cannot be read or otherwise reconstructed. Redaction is specifically excluded as a means of destruction.

Although HIPAA’s Security Rule requires covered entities to safeguard electronic PHI, encryption is not required; rather, encryption is one of the Security Rule standards that are characterized as “addressable” rather than “required.” Comparable alternatives such as firewalls and access controls are also acceptable. However, if a covered entity chooses to encrypt PHI pursuant to this new HHS guidance, the PHI shall be considered “secure” for purposes of the breach notification rule. If a breach of that encrypted PHI is later discovered, then the covered entity is not required to provide notice since the information will not be considered “unsecured.” In this sense, encryption undertaken in conformance with the HHS guidance works as a safe harbor from the breach notification requirements of the interim rule.

Risk of Harm Threshold

As mentioned above, the preamble to the interim final rule recognizes that the HITECH statute encompasses a “harm threshold,” which limits notification to situations where it is reasonably necessary. Thus, the HHS rule clarifies that unauthorized use or disclosure of PHI only constitutes a breach if it “poses a significant risk of financial, reputational, or other harm to the individual.” In order to determine if such a risk exists, covered entities and business associates are required to perform a risk assessment. This harm threshold aligns the HHS regulation with many existing state breach notification laws, where risk of harm is also a key element in triggering notice.

In performing the risk assessment mentioned above, HHS notes that covered entities should consider a number of factors, including:

- who impermissibly used or to whom the information was impermissibly disclosed (e.g., the risk of harm is reduced if the PHI was disclosed to or used by another HIPAA-covered entity, such as a physician's office);
- the type, amount and sensitivity of the PHI involved (e.g., if the disclosed PHI merely included a name and that he or she received services from a hospital, then it would likely not constitute a significant financial, or reputational risk (although it would violate the HIPAA privacy rule); and
- whether the covered entity has taken immediate steps to mitigate the situation (e.g., received satisfactory assurances, through a confidentiality agreement or other similar means, that the recipient would destroy the PHI and not further compromise its privacy); and
- whether the impermissibly disclosed PHI was returned prior to being improperly accessed (e.g., a stolen laptop is recovered and forensic analysis shows the PHI was not accessed or compromised).

Covered entities and business associates must document their risk assessment process so that they can demonstrate, if necessary, that the impermissible use or disclosure did not pose a significant risk of harm to the individual. HHS also notes that any risk assessment should be fact-specific, and reminds covered entities and their business associates that "many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of the risk of reputational harm – especially in light of fears about employment discrimination."

Effective Date

Although the HHS regulations are technically effective 30 days after publication (*i.e.,* September 23, 2009), HHS stated it would not impose sanctions for noncompliance until February 22, 2010. This will allow covered entities and their business associates time to implement compliance measures.

The FTC Rule

The FTC final rule addresses entities that offer services to store individuals' health information online, as well as service providers of these entities. Although the rule does not apply to HIPAA-covered entities or their business associates, it does apply to entities that heretofore have been beyond the FTC's jurisdiction, such as nonprofit organizations.

The FTC's notification rule only applies to breaches of "unsecured" PHR, defined as identifiable PHR information "that is not protected through the use of technology or methodology specified by the Secretary of [HHS]." As discussed above, HHS has identified encryption and destruction as the appropriate means for securing such information. Therefore, like the HIPAA-covered entities regulated by the HHS rule, PHR vendors may seek safe harbor from the notice requirements by encrypting PHR.

Personal health records vendors, as well as "PHR-related entities," are required to notify affected individuals upon the discovery of a "breach of security" of unsecured PHR identifiable health information. The FTC defines "PHR- related entities" as entities that (1) offer products or services through a PHR vendor's website, (2) offers products or services through the web sites of HIPAA-covered entities that offer individuals' PHRs, or (3) access information in PHR or send information to a PHR. These may include web-based applications that help consumers manage medications, a web site offering online personalized health checklists or even a brick-and-mortar company advertising dietary supplements online.

The FTC regulations require PHR vendors to notify affected customers following the discovery of a "breach of security" concerning a customer's PHR. More specifically, a "breach of security" is defined as the unauthorized acquisition of an individual's unsecured PHR-identifiable health information. Examples include the theft of a laptop containing unsecured PHR, unauthorized downloading of such records by an employee, or remote copying of PHR by a hacker.

The FTC rule presumes that where there has been unauthorized access (i.e., the opportunity to view data), there also has been unauthorized acquisition (*i.e.,* the actual viewing or reading of data). This presumption is rebuttable, however, if the vendor "has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." For example, if an employee inadvertently accesses a customer's PHR, but logs off without reading, using or disclosing such data, then no breach of security has occurred.

As in the HHS rule, a PHR vendor must provide an individual with prompt notice upon discovery of a security breach. The notice must include pertinent information such as a description of what happened, the type of PHR involved, and steps the individual can take to protect themselves from further harm. In the case of a breach involving 500 or more people, entities must notify the media. Likewise, a third party service provider must notify the relevant vendor or PHR-related entity upon discovery of a security breach; in turn, the vendor or PHR-related entity must notify the affected individual.

There is one critical difference between the HHS and FTC regulations: the FTC's final rule does not include a risk of harm threshold. Therefore, even where a PHR vendor might reasonably conclude that a security breach presents a small risk of harm to a consumer, the vendor is still required to notify the affected individual. The FTC noted that its standard does take harm into account, given that, as described above, entities can rebut a presumption of harmful acquisition of PHR. However, because of the sensitivity of health information, the FTC believes "the standard for notification must give companies the appropriate incentive" to safeguard such information.

Effective Date

The FTC's notification requirements are effective September 23, 2009 (i.e., 30 days from publication). In the preamble to the final rule, however, the FTC stated it would not begin enforcing the notification standards until February 22, 2010.

Closing Thoughts

Both HIPAA-covered entities and vendors of personal health records should begin putting policies and procedures in place to comply with the standards articulated by the HHS and the FTC rules. Covered entities, PHR vendors and PHR-related entities also should consider encrypting personal health records pursuant to HHS guidance. Such encryption will provide entities with safe harbor-like protection in the event of a security breach to unsecured PHR. HIPAA-covered entities also may want to revisit contracts with business associates in light of the HHS notification requirements.

Proskauer Rose LLP is closely monitoring developments in connection with the HHS and FTC security breach requirements. If you have further questions concerning either agency's requirements, please contact either Rick Zall at 212.969.3945, Sara Krauss at 212.969.3049 or Harris Danow at 212.969.3723.