The HITECH Breach Notification Rules: Ensuring Compliance with the New Obligations

Co-authors Amy K. Fehn and Laura C. Range, Michigan Medical Law Report, Winter 2010

On February 17, 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009. In response to a mandate in the HITECH Act, the Department of Health and Human Services (HHS) issued an interim final rule with request for comments for Breach Notification for Unsecured Protected Health Information (the "Rule") on August 19, 2009.

The Rule establishes significant new notification obligations for covered entities and business associates that are subject to HIPAA. Specifically, the new regulations establish guidelines for determining when a breach of unsecured PHI occurs; dictates who must notify of such a breach and to whom notification must be made; and establishes the timeframe and contents of such notification.

The Rule became effective on September 23, 2009. However, HHS has requested additional comments that were due on October 23, 2009 and that may ultimately result in further modifications to the notification obligations.

Covered entities and business associates must be aware of the new obligations under the Rule and should begin taking steps immediately to ensure compliance. In addition, these entities must remain cognizant of additional changes and modifications that may develop and must be prepared to alter their compliance efforts with these additional potential changes in mind.

When Are the Notification Requirements Triggered?

The Rule only requires notification if the incident qualifies as a "breach" of unsecured PHI. The Rule defines "breach" as the "acquisition, access, use or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of [PHI]." Therefore, a use or disclosure that violates the HIPAA Privacy Rule is a prerequisite, and any uses or disclosures that do not violate the Privacy Rule cannot constitute a "breach" requiring notification under the Rule.

In addition, an incident will only qualify as a "breach" if it meets a certain "harm threshold." In other words, the use or disclosure must "pose a significant risk of financial, reputational, or other harm to the individual." To determine whether this harm threshold has been met, covered entities and business associates must conduct and document a fact specific "risk assessment." The risk assessment should take into account the following factors: (1) the identity of the entity or individual that impermissibly used the information or to whom the information was impermissibly disclosed; (2) the steps taken to mitigate harm and the immediacy with which such steps were taken; (3) whether the information was returned before being accessed; and (4) the type and amount of information disclosed.

Finally, the Rule also contains three statutory exceptions to the "breach" definition. These exceptions are as follows: 1) uses or disclosures by persons acting under the authority of the covered entity or

business associate that are made in good faith, that fall within the scope of the disclosing individual's authority, and that do not result in further violations of the HIPAA Privacy Rule; 2) inadvertent disclosures from one person authorized to access PHI to another person also authorized to access PHI within the same covered entity, business associate, or organized health care system; and 3) situations in which the covered entity or business associate has a good faith belief that an unauthorized person receiving the PHI could not reasonably have been able to retain the information.

What Are the Notification Requirements?

Individual Notice

In situations in which a covered entity or business associate has a reasonable belief that the breach involved an individual's PHI, the entity must provide written notice to each affected individual. Such notice must be provided without "unreasonable delay," but in no case later than sixty days after discovery of the breach. To the extent possible, the notice should include the following information: 1) a brief description of what happened; 2) the types of information that were involved in the breach; 3) steps that affected individuals should take to protect themselves from potential harm; 4) a description of what the entity is doing to investigate the incident, mitigate harm, and protect against further breaches; and 5) contact procedures by which affected individuals may learn additional information. In certain situations, such as when the covered entity or business associate determines that misuse of the PHI is imminent or when the entity has insufficient contact information for the affected individuals, additional or substitute notice by alternative means may be made.

Media Notice

Covered entities and business associates must also notify a prominent media outlet within the same timeframe as required for individual notice in situations in which a breach involves the PHI of more than 500 individuals within a state or jurisdiction.

When Must an Entity Report Breaches to HHS?

Finally, covered entities and business associates must track and report all breaches to HHS. Breaches involving the PHI of more than 500 individuals (in *any* state or jurisdiction) must be reported "immediately." All other breaches must be recorded and annually reported no later than sixty days after the end of each calendar year.

Summary

The Rule establishes significant new breach notification obligations for covered entities and business associates covered by HIPAA. In sum, the Rule requires such entities to provide individual and/or media notice when there has been a breach of unsecured PHI and to track and report such breaches to HHS.

Affected entities should review HIPAA compliance efforts with these new obligations in mind. For example, entities should ensure that policies are in place requiring workforce members to immediately report any potential privacy violations or security incidents so that they can effectively and promptly evaluate the incident to determine whether notification obligations are triggered. Entities should also establish policies and conduct training to communicate what notification will be required and should maintain accurate records to prepare required reports to HHS. Affected entities must remain aware of potential changes to these requirements in the future, and be prepared to revise policies and procedures accordingly.

Amy K. Fehn is an attorney at Wachler & Associates, P.C. Ms. Fehn graduated Summa Cum Laude from Kent State University and Summa Cum Laude from the University of Akron School of Law.

Ms. Fehn is a former registered nurse who has been counseling healthcare providers for the past eleven years on regulatory and compliance matters. Ms. Fehn is a member of the American Health Lawyers Association, as well as the State Bar of Michigan, Health Care Law Section, where she served as a member of the HIPAA Task Force. She also co-authored workbooks on both HIPAA Privacy and Security and has presented on HIPAA issues to local and national organizations.

She can be reached at 248-544-0888 or afehn@wachler.com.

Laura C. Range is an associate at Wachler & Associates, P.C., where she practices in all areas of health care law, with specific concentration in transactional and corporate matters, licensure and staff privileging cases, Medicare and other third-party payor audit defense and appeals, and regulatory

compliance, including HIPAA privacy and security compliance. While pursuing her LL.M. in Health Law, Range served as an intern in the Business Practices Office of The Methodist Hospital in Houston, TX, where she assisted in a variety of HIPAA compliance efforts.

She can be reached at 248-544-0888 or lrange@wachler.com.