HEALTH CARE WEEKLY~REVIEW®

April 8, 2013
Volume 29, Issue 13

MICHIGAN EDITION

HIPAA: Breach Notification Rule Under HITECH—The 'Final Rule'

By Aaron Beresh and Lori-Ann Rickard

Technology is rapidly progressing and integrating into every aspect of our lives, including the health care industry. There is no avoiding technology especially as health care providers are becoming increasingly aware of the frequency in which they are accessing protected health information to accomplish more in a limited amount of time. For instance, health care providers may receive updates regarding patients via email or may even correspond with a patient via text messaging. As health information is more easily stored and transmitted electronically, health care providers—and those working with protected health information—need to understand whether a disclosure of unsecured protected health information requires notification under the Health Information Technology for Economic and Clinical Health Act ("HITECH").

Pursuant to the interim final rule, which became effective on September 23, 2009, covered entities and business associates must perform a risk assessment to determine whether a breach of unsecured protected health information posed a significant risk of financial, reputational, or other harm to the individual. In response to the interim final rule, HHS received several comments arguing that the harm standard resulted in an overly subjective analysis—based on a combination of factors—that set too high a bar for triggering breach notification. Based on the interim final rule standard, if an organization determines that the incident does not pose a significant risk of harm, it may forgo breach notification.

As a result, on January 25, 2013, the U.S. Department of Health and Human Services ("HHS") published the final rule outlining significant changes to the Health Insurance Portability and Accountability Act ("HIPAA") Privacy, Security and Enforcement Rules mandated by HITECH. The final rule, known as the Omnibus Rule, became effective on March 26, 2013, and supplanted the interim final rule's breach notification standard. Covered entities and business associates must comply with the final rule by September 23, 2013. The final rule's modification to the breach notification standard establishes that an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the protected health information was compromised, or another exception applies. Thus, in the final rule, HHS ultimately struck a balance by establishing a presumption standard, and detailed that organizations must assess the probability that protected health information was compromised based on a risk assessment that considers at least the following factors:

1. The nature and extent of the health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the health information or to whom the disclosure was made;
3. Whether that health information was actually acquired or viewed; and
4. The extent to which the risk of the health information has been mitigated.

According to the final rule, if the analysis of the factors described above fails to demonstrate that there is a low probability that the health information was compromised, breach notification may be required. Organizations should always consult with competent legal counsel regarding the specific facts at issue.

Ultimately, the removal of the harm standard in the final rule will likely result in more frequent breach notifications, and organizations should be in the process of updating their policies and procedures accordingly. Healthcare providers and individuals who work in or around the health care industry should be cognizant of the importance of properly safeguarding protected health information, and make certain that all protected health information, whether at rest, in transit, or in use, is properly encrypted to avoid breach notification obligations and associated penalties.