NELSON HARDIMAN
HEALTHCARE LAWYERS

# The New HIPAA Breach Rule


As of September 23, 2013, the rules are changing for evaluating whether a "breach" has occurred for purposes of the Health Insurance Portability and Accountability Act ("HIPAA"). For healthcare providers and their business associates, it is critical to understand what these changes are and how they affect your business.

In January 2013, the U.S. Department of Health and Human Services ("DHHS") published the HIPAA "Omnibus Rule." The Omnibus Rule amended various provisions of HIPAA and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which require covered entities and business associates to enact safeguards to ensure the privacy and security of protected health information ("PHI") they create, receive, maintain and transmit. If there is a "breach" which results in the unauthorized use or disclosure of PHI, a covered entity may be required to notify individuals, the Office of Civil Rights, and the media.(1)

The Omnibus Rule modifies the definition of a HIPAA "breach" which would trigger a covered entity's notification requirements. Currently, when a covered entity experiences an incident that may have compromised the privacy or security of PHI, the covered entity conducts an analysis to figure out if this security incident is considered a HIPAA breach. All security incidents are not necessarily considered to be HIPAA breaches. A "breach" is defined as the acquisition, access, use or disclosure of PHI in a manner that is not permitted by HIPAA, and that compromises the security or privacy of the PHI.(2) Under the existing version of the rule, "compromises the security or privacy of the PHI" means that the disclosure poses a significant risk of financial, reputational, or other harm to the individual.(3) Security incidents that do not pose this kind of a risk are not considered HIPAA breaches, and do not need to be reported to the government.

When the Omnibus Rule takes effect in September 2013, a security incident will be presumed to be a breach unless the covered entity or business associate, as applicable, can demonstrate that there is a "low probability" that PHI has been compromised. This determination is made by conducting a risk assessment which examines the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI, or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.4 According to DHHS, breach notification will be necessary in nearly all situations, unless the covered entity or business associate can prove that there is a low risk to the PHI.5

For those covered entities and business associates that are already complying with the obligation to respond to security incidents with some form of "risk analysis," the change may not be radical. The inquiry – whether a particular disclosure has "compromised the privacy or security of PHI – is the same; the Omnibus Rule has simply changed the presumption. A security incident must be presumed to be a HIPAA breach unless proven otherwise. This change elevates the risk level for inadequate documentation of the analysis.

For business associates and covered entities that are not yet in the process of performing risk analyses following data security incidents (or are not yet operating in a sufficiently compliant environment to detect possible breaches), the Omnibus Rule raises the stakes of continued noncompliance. The presumption of a HIPAA breach is likely to translate into more aggressive government enforcement against businesses that are disregarding their compliance obligations.

Irrespective of their current state of HIPAA compliance, covered entities and business associates alike should ensure that they have sufficient documentation to support their breach analysis following a security incident. In particular, if a covered entity does not notify individuals after a security incident, it needs to have documentation to support their assessment of a “low probability” that PHI has been compromised.

Covered entities may want to reexamine the breach provisions of their business associate agreements in light of this modified rule. If a covered entity’s business associate experiences a security incident, the covered entity may want to participate in the risk assessment process, and make sure that the business associate is communicating with the covered entity about the incident.

Finally, covered entities and business associates should ensure that they have the appropriate policies in place to effectively respond to a HIPAA breach. The federal government wants to see that covered entities and their business associates have effective compliance programs in place to detect, respond to, and report breaches.

---

(1) Many state laws require covered entities to provide notice to the state Attorney General as well.

(2) 45 C.F.R. § 164.404.

(3) Id.

(4) Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; 78 Fed. Reg. 17, 5695 (Jan. 25, 2013)(to be codified at 45 C.F.R. § 164.402).

(5) Id at 17, 5641.