CLIENT ALERT

HIPAA Final Rule Expands Liability for Violations, Clarifies Penalty Assessment Methodology

Feb.22.2013

The Health Insurance Portability and Accountability Act (HIPAA) final rule expands liability for HIPAA violations and clarifies how the U.S. Department of Health and Human Services (HHS) will calculate the penalties for such violations. The final rule subjects an expanded population of entities (*e.g.*, covered entities, business associates, and subcontractors) to larger monetary fines for violating an increased number of regulations. Fortunately, this increased liability is accompanied by more detailed guidance on the methodology HHS will use to assess monetary penalties. Together, these changes have significant implications for covered entities and business associates and highlight the importance of implementing sufficient security and privacy protocols.

One of the most anticipated changes to the final rule is the scope of HHS's enforcement authority. In the final rule, HHS significantly expanded liability by: (1) subjecting the HITECH Act and implementing regulation violations to a Civil Monetary Penalty (CMP); (2) subjecting business associates and all downstream subcontractors to direct liability for certain HIPAA violations;[1] and (3) increasing the monetary penalties for such violations.

Along with increasing liability, HHS explained how it will determine the precise penalty for HIPAA violations. As before, the Secretary may impose a CMP for any violation of a HIPAA "administrative simplification provision" ("provision"), which, as earlier indicated, now includes any requirement or prohibition established by the HITECH Act as well as HIPAA. As set forth in the chart below, and previously established in HHS's Interim Final Rule, the degree of culpability determines the range of the potential penalty for each violation of a given provision. The precise fine will depend on factors set forth in 45 C.F.R. § 160.408 such as the nature and extent of the violation (including the number of persons affected and time period during which the violation occurred), the nature and extent of the resulting harm, the history of prior compliance with the provision, the financial condition of the covered entity or business associate, and "such other matters as justice may require."

Civil Monetary Penalties For HIPAA/HITECH Violations		
Violation Category of Culpability – Section 1176(a)(1)	**Each Violation**	**Annual Maximum For Identical Violations**
(A) Did not know (and would not have known with reasonable diligence) of violation	$100 - $50,000	$1,500,000

(B) Violation due to reasonable cause – but not willful neglect	$1,000 - $50,000	$1,500,000
(C)(i) Willful neglect – but violation corrected	$10,000 - $50,000	$1,500,000
(C)(ii) Willful neglect – and violation not corrected	$50,000	$1,500,000

HIPAA permits the Secretary to impose a separate fine for each provision that is violated. The Final Rule also permits the Secretary to treat the violation of a provision affecting multiple people or that is ongoing as multiple violations. Prior to the Final Rule, HHS provided little guidance about how it would "count" a violation of a single provision that affected multiple individuals or continued over time without being rectified. HHS previously suggested that it would use one of several "counting" metrics: (1) the number of impermissible *actions* or failures to take required actions; (2) the number of *persons* involved; or (3) the amount of *time* during which the violation occurred.

In the Final Rule, HHS clarifies how these metrics will be used, particularly in cases involving a breach of unsecured PHI. HHS indicated that it would "count" the number of violations of a single Privacy Rule provision (*e.g.*, an impermissible disclosure of PHI under § 164.502) resulting from a breach based on the number of people whose information was disclosed. Depending on the level of culpability, HHS could therefore impose a fine up to $50,000 for each impermissible disclosure, multiplied by the number of persons affected, subject to a cap of $1.5 million. HHS further explained that the same breach could be the result of a separate, albeit related, violation of the Security Rule (*e.g.*, the failure to implement adequate physical security under § 164.310) that "continued" over a period of time. In such cases, § 160.406 permits HHS to "count" the number of times the single Security Rule provision was violated based on the number of days the violation continued. Depending on the level of culpability, HHS could therefore impose a separate $50,000 fine for each violation of the Security Rule provision, multiplied by the number of days the violation occurred, subject to a separate cap of $1.5 million for the calendar year.

Thus, the final rule makes clear that the relevant metric for Privacy Rule violations stemming from a breach is the number of persons affected and that the relevant metric for violations capable of "continuing" over time will be the number of days the violation occurred. In the example above, the entity would face potential liability of $3 million – and potentially more if the circumstances indicated violations of additional provisions.

The Security and Privacy Rules both contain a number of general "standards" that overlap to a certain degree with more specific "implementation requirements" in the same Rule, which creates the potential for duplicative fines. However, the Secretary has reiterated in the Final Rule the position taken in the Interim Final Rule, that an entity will not be fined for violations of both the general standard and the more specific implementation provision set forth in the same Rule. *See* 45 CFR § 160.404(b)(2).

[1] A more detailed explanation of the provisions applicable to business associates and subcontractors is set forth in a prior Crowell & Moring client alert, available here.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Barbara H. Ryland
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2970
Email: bryland@crowell.com