American Hospital Association

SPECIAL BULLETIN

Friday, January 18, 2013

This bulletin is two pages.

HHS Office for Civil Rights Releases Final HIPAA Rule

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) on Jan. 17 released a final "omnibus" rule (http://www.ofr.gov/OFRUpload/OFRData/2013-01073_PI.pdf) that updates several provisions in *Health Insurance Portability and Accountability Act* (HIPAA) regulations, as mandated by the *Health Information Technology for Economic and Clinical Health Act* (HITECH). The omnibus rule:

- Replaces the "harm" threshold from the interim rule on breach notification with a more objective standard;
- Requires business associates to comply with specific HIPAA privacy and security requirements and imposes direct liability for their noncompliance with these regulatory standards;
- Incorporates the increased and tiered civil money penalty structure provided by HITECH;
- Limits the use and disclosure of protected health information (PHI) for marketing and fundraising; restricts the sale of PHI; permits greater flexibility in using and disclosing the PHI of decedents and the immunization records of students; and obligates covered entities to honor an individual's request to restrict disclosure of PHI in certain circumstances; and
- Prohibits most health plans from using or disclosing genetic information for underwriting purposes, as required by the *Genetic Information Nondiscrimination Act*.

Highlights of the Revised Breach Notification Requirements

The final rule clarifies that, unless covered entities or business associates specifically demonstrate that there is a "low probability that the PHI has been compromised" or that one of the exceptions to the definition of breach included in the rule applies, breach notification is required to be provided. The use of this presumption in the risk approach of the final rule is intended to ensure that the breach notification obligations are interpreted and applied in a uniform way by all covered entities and business associates and to address some commenters' concerns that the requirement, as stated in the interim final rule, was unclear and could be understood and implemented in unintended ways.

Rather than providing, as the interim final rule does, that no notice is required because "there is no significant risk of harm" to the individual from the breach of PHI, the final rule requires a demonstration that there is a low probability that the PHI has been compromised through a risk assessment that, at a minimum, examines ***all*** of the following factors:

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

Given the particular circumstances of the breach, however, it may be necessary to consider additional factors to assess appropriately the risk that the information has been compromised. OCR notes that the risk assessment factors above are "derived from [those] listed in the interim final rule as well as many of the factors suggested by commenters." OCR also concludes that the risk assessment approach in the final rule "should not be a new or different exercise" for covered entities and business associates because they already must "be performed routinely following security breaches and to comply with certain State breach notification laws."

In addition, the final rule provides that notice is not required in certain situations where the unauthorized use, disclosure, acquisition or access of PHI is "so inconsequential that is does not warrant notification." These situations are specific to statutory exemptions in the definition of breach included in HITECH. The final rule discussion also recognizes that "there may be other similar situations [in addition to the statutory exceptions] that do not warrant breach notification." Disagreeing with commenters who urged a bright line rule for notification, OCR says: "We agree . . . that providing notification [in these inconsequential circumstances] may cause the individual unnecessary anxiety or even eventual apathy if notifications . . . are sent routinely." In addition, OCR says that a bright line standard "would be extremely burdensome and costly for entities to implement."

NEXT STEPS

The final HIPAA rule will be published in the Jan. 25 *Federal Register,* and takes effect March 26. However, covered entities and their business associates generally will have until Sept. 23 to comply with most of the rule's provisions, including the changes to the breach notification requirements. The final rule also provides for establishing a 180-day compliance window for future modifications to the HIPAA rules ***unless*** a future published final rule provides otherwise. Where a future modification of the HIPAA rules requires a longer compliance period, that longer period will be expressly provided for in the particular rulemaking. Watch for an *AHA Regulatory Advisory* examining the many provisions in the final rule in the coming weeks.