HINSHAW

Alerts

New HIPAA/HITECH Breach Notification Rules for Covered Entities and Business Associates

February 5, 2013
Health Law Alert

This Health Law Alert *is the third in a six-part series Hinshaw & Culbertson is publishing detailing the significant changes to Health Insurance Portability and Accountability Act (HIPAA) privacy, security, enforcement and breach notification rules as part of the Omnibus Final Rule (Final Rule) issued by the U.S. Department of Health and Human Services (HHS).*

This alert summarizes important modifications and clarifications to the HIPAA/Health Information Technology for Economic and Clinical Health Act (HITECH) breach notification rules contained in the Final Rule.

The New Four-Factor Risk Assessment Criteria

The Final Rule addresses the manner in which covered entities (CEs) and business associates (BAs) must determine whether a breach of unsecured protected health information (PHI) that requires notification to affected individuals, HHS, and/or the media has occurred. Under HITECH, unauthorized acquisition, use or disclosure of PHI triggers these notification requirements when the security or privacy of the PHI has been "compromised."

The interim Final Rule (Interim Rule) provided that an incident compromises the security or privacy of PHI when it "poses a significant risk of financial, reputational, or other harm to the individual." The Final Rule eliminates this "significant risk of harm" standard and replaces it with a four-factor risk assessment designed to create a more uniform and objective method of determining when notification is required. The Final Rule also amends the definition of "breach" to emphasize that an impermissible use or disclosure of PHI is presumed to be a breach unless and until a CE or BA demonstrates through its risk-assessment that there is a low probability that the PHI has been compromised (or that another exception applies). The four factors that must be considered as part of the risk assessment are:

1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification.

For example, it should be considered whether the PHI included particularly sensitive financial information such as social security or credit card numbers. The nature and degree of any clinical information used or disclosed should also be considered.

2. The identity of the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made.

For example, it should be considered whether the person using or receiving the PHI has independent obligations to protect the privacy and security of the information. Although all CEs are obligated to protect PHI, an impermissible disclosure from one CE to another (unless it meets a statutory exception) does not automatically eliminate notification requirements. However, this may be considered as one factor in the risk assessment concerning such a disclosure.

3. Whether the PHI was actually acquired or viewed, or whether only the opportunity to do so existed.

For example, if a CE mails PHI concerning a patient to the wrong address, but the envelope is returned unopened, this may pose a different risk than if the CE receives a phone call from a recipient who has reviewed the PHI and realized it was sent in error.

4. The extent to which the risk to the PHI has been mitigated.

For example, the recipient of an impermissible disclosure may be asked to provide assurances that the PHI will not be further used or disclosed or will be destroyed. The extent and efficacy of any such mitigation must be considered when determining the probability that the PHI has been compromised. Assurances of an employee, affiliated entity, BA or another CE, for example, may be stronger evidence of mitigation, while assurances from certain third parties may or may not be sufficient.

Each of these factors must now be considered and documented in a risk analysis. The Final Rule requires this risk assessment even when the impermissible use or disclosure involves a limited data set, eliminating a previous exception specific to limited data sets. This is now the case even when a limited data set does not contain dates of birth and zip codes.

Once a CE or BA has considered the four factors identified above and any other factors relevant and necessary under the circumstances, it must evaluate the overall probability that the PHI has been compromised. Unless there is a low probability that the PHI was compromised, breach notification is required. HHS has indicated that it intends to issue further guidance concerning frequently occurring breach scenarios.

Clarification Regarding Other Breach Notification Requirements

The Final Rule retains the guidance in the Interim Rule regarding when a breach is deemed discovered, and the timing and the content of the required notifications. It does, however, provide a few clarifications. For example, for breaches affecting fewer than 500 individuals, the obligation to notify HHS within 60 days after the end of the calendar year will be triggered off the year in which the breaches were discovered, not the year in which they occurred.

In issuing the Final Rule, HHS has also explained that when a notification of the media is required, the reporting entity is under no obligation to incur any costs to publish a notice. Nor is the media under any obligation to publish the information it receives. Rather, notification requirements are met when a CE provides the breach notification information to prominent media outlets serving the state or jurisdiction where the affected individuals reside. Notably, publication on an entity's website does not satisfy the obligation to notify the media.

In the case of individual notifications, HHS has noted that while breach notification is required to be made in writing, it will exercise some enforcement discretion regarding this requirement in very limited circumstances where an individual has affirmatively opted for privacy reasons to receive communications from a CE only orally or by telephone. However, even in those circumstances the CE should request by phone that the individual pick up written notice of the breach. Telephone communications cannot replace written breach notification solely for the sake of convenience.

Hinshaw attorneys have extensive experience assisting clients with the development and implementation of breach notification policies and procedures and with risk assessments after security incidents. If you have questions or need assistance in determining how to make the requisite changes to your policies, procedures, and practices in order to come into compliance with the Final Rule, please contact your regular Hinshaw attorney.

Download PDF

This alert has been prepared by Hinshaw & Culbertson LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship.