eALERT

INCompliance

August 02, 2010

# HIPAA: Final Guidance on Security Rule Risk Analysis Released

On July 14, 2010, the Office of Civil Rights (OCR) published a final version of its Guidance on Risk Analysis Requirements Under the HIPAA Security Rule ("Guidance"). The Guidance is the first document stemming from the HI-TECH Act requirement that OCR issue annual guidance on the provisions of the HIPAA Security Rule. The final version is nearly identical to the prior draft version with a few minor changes.

The Guidance explains that it "clarifies the expectations" of OCR regarding meeting the risk analysis requirements in the Security Rule. A risk analysis is expressly required by the Security Management Standards (45 CFR 164.308) of the Security Rule. The Guidance also explains that OCR believes a risk analysis is required in order for a Covered Entity or Business Associate to assess the "addressable" implementation specifications contained in standards throughout the Security Rule.

HIPAA allows for a flexible approach in performing a risk analysis that is tailored to the size and nature of the organization. However, the Guidance does provide a list of certain required elements of a risk analysis and a description of what is expected for each requirement. The required elements include:

- Proper Scope of Analysis
- Data Collection
- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Measures
- Determine the Likelihood of Threat Occurrence
- Determine the Potential Impact of Threat Occurrence
- Determine the Level of Risk
- Finalize Documentation
- Periodic Review and Updates to the Risk Analysis

The Guidance also adds new definitions of "vulnerability," "threat," and "risk," which are terms not currently defined in the HIPAA regulations.

The Security Rule requires organizations to update and document security measures "as needed." Importantly, the Guidance explains that in order to satisfy these requirements organizations should "conduct continuous risk analysis to identify when updates are needed." Further, in addition to making "as needed" changes, the Security Rule requires organizations to conduct periodic risk analysis. Neither the Security Rule nor the Guidance proscribe a time period required for periodic risk analysis. However, the Guidance states that a "truly integrated risk analysis and management process is performed as new technologies and business operations are planned" and explains that in the following situations "the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected":

- After a security incident
- Upon a change in ownership
- Upon turnover in key staff or management
- When planning to incorporate new technology