Risk Analysis – a Critical Step One in Safeguarding e-PHI

06.25.2010

Pamela A. Scott

For hospitals and other health care providers working to secure electronic protected health information (e-PHI), a comprehensive risk analysis is a critical first step. The draft guidance on risk analysis issued on May 7, 2010, by the Department of Health and Human Services' Office for Civil Rights (OCR) offers a starting point to help hospitals and other providers identify and implement the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI. The guidance, which is available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html, provides helpful insight into the expectations of OCR, the agency responsible for enforcing the HIPAA Privacy and Security Rules.

The HIPAA Security Rule has always required health care providers, health plans, and other covered entities to conduct an accurate and thorough analysis of potential risks to the confidentiality, integrity, and availability of e-PHI, but it does not specify how to go about conducting an effective assessment. The risk analysis requirement has received heightened attention recently in the wake of stronger enforcement provisions included in the HITECH Act for violations of the HIPAA Privacy and Security Rules, as well as the inclusion of this security measure in the "meaningful use" rules under which eligible health care providers can qualify for the electronic health record incentives program adopted last year.

OCR's draft guidance recommends that organizations include the following key steps in their risk analysis.
Define the scope of the risk analysis.

- Identify where e-PHI is stored, received, maintained, or transmitted.
- Identify and document reasonably anticipated threats and vulnerabilities that could lead to improper disclosure and access.
- Evaluate current security measures to safeguard e-PHI.
- Determine the likelihood and impact of potential risks to the confidentiality, integrity, and availability of e-PHI.
- Determine the level of risk for reasonably anticipated threats and vulnerabilities identified during the analysis.
- Document the risk analysis.
- Periodically review and update the risk analysis.

OCR's guidance indicates that the risk analysis process should be an ongoing process in order to identify new threats to the confidentiality, integrity, and availability of e-PHI and to identify and implement necessary updates, as required

by the Security Rule. The guidance recognizes that the frequency of the risk analysis will vary according to the specific needs and circumstances of each organization. It also wisely notes the value of incorporating risk analysis in planning on the front end for an organization's new technologies and operations. OCR's reported plan to conduct compliance reviews for all HIPAA data breaches involving data for more than 500 individuals highlights the importance of implementing a continuing, comprehensive risk analysis.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075