Foster Garvey

Risky Business: Is Your Organization's HIPAA Security Rule Risk Assessment Up to Date?

Legal Alert
March 25, 2013

Garvey Schubert Barer Legal Update, March 2013.

Tucked away in a file cabinet or buried in a thick binder on a shelf, your organization's HIPAA Security Rule risk assessment report is gathering dust. If you cannot remember the last time you saw it, this would be a good time to dig it out, shake off the dust, and determine whether an update is in order. The Office for Civil Rights (OCR) is stepping up HIPAA enforcement. If an OCR investigator comes calling, you need to be ready with a current assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (e-PHI) held by your organization.

According to the U.S. Department of Health and Human Services' July 2010 Guidance on Risk Analysis Requirements under the HIPAA Security Rule, a complete and thorough risk assessment is the first step in an organization's Security Rule compliance effort. But risk assessment was never meant to be a one time process. Implementing regulations require updates (with documentation) "as needed." There is no mandatory timeline for updates, but a good rule of thumb is to do so at least once a year. In addition, there should be a review as new technologies or business operations are planned, if there has been a change in ownership, key staff or management, and any time there has been a security incident.

All elements of the original risk analysis should be revisited. What is the organization's e-PHI? Has there been any change in the way that e-PHI is stored, received, maintained or transmitted? How do the current "threats" align with areas of "vulnerability" and what is the likelihood that each of the "reasonably anticipated" threats will occur? What are the organization's current security measures? What are the potential impacts if each identified threat were realized? Finally, how will the organization address areas of risk identified during the current review? Every step of the review process and updated risk assessment should be documented in a new report or supplement to the original report.

Neither the Security Rule, nor any of the government's guidance dictates how, by whom, or how often a risk assessment must be performed, but this lack of specificity should not be taken to suggest that the government is not concerned about compliance. According to statistics posted on the DHHS website, a lack of administrative safeguards for e-PHI is one of the OCR's top five areas of investigation. Private practices and general hospitals rank first and second, respectively, among organizations required to take corrective action in connection with OCR

investigations.

The results of an OCR investigation in Arizona illustrate the need for diligence in this area. Following a complaint about the group's on-line scheduling calendar, OCR investigated Phoenix Cardiac Surgery, P.C., and identified what OCR characterized in a press release as a "multi-year, continuing failure" to comply with the privacy and security regulations. The resulting Corrective Action Plan, made public in April 2012, required Phoenix Cardiac to update and implement comprehensive privacy and security policies and procedures, including an update to its initial December 2009 risk assessment report. The group was also required to pay a $100,000 as part of its settlement with DHHS. OCR's press release included what can only be characterized as a warning from Leon Rodriguez, director of OCR: "We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity." As the one-year anniversary of that statement is looming, every covered entity and business associate should be asking whether, and to what extent, its organization has identified and addressed HIPAA risk within its organization. This is not the time for risky business.