Report on Patient Privacy Volume 18, Number 7. July 31, 2018
OCR Newsletter on Gap Analysis Offers Reminders on Risk Plans

By HCCA Staff

HIPAA covered entities and business associates know they must perform a risk analysis of the electronic protected health information they maintain, to comply with the security rule.

Specifically, the requirement is for "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the [organization]."

Even though a basic requirement, conducting the analysis—and the necessary risk management plan to address the identified risks—is still something organizations struggle with. That was confirmed by the audit findings the Office for Civil Rights (OCR) recently released (*RPP 5/18, p. 1*).

But say for the sake of argument that the risk analysis and management plans are done. One way to determine whether they've actually resulted in compliance with the safeguards required by the security rule, according to OCR, is to conduct a gap analysis.

"A gap analysis, while not required by the HIPAA Rules, is a useful tool to identify whether certain standards and implementation specifications of the Security Rule have been met," OCR says in a recent edition of its monthly "cyber awareness" newsletter.

Here's the difference between the two, says OCR:

◆ "A risk analysis is a comprehensive evaluation of a covered entity or business associate's enterprise to identify the ePHI and the risks and vulnerabilities to the ePHI. The risk analysis is then used to make appropriate modifications to the ePHI system to reduce these risks to a reasonable and appropriate level.