Health Information Compliance Alert

Reader Questions: Know the Facts on Gap Analysis Vs. Risk Analysis

Question: We keep hearing that a gap analysis of how we implement our HIPAA compliance plan is a whole lot easier and quicker than performing an annual risk analysis. Is that true and should we switch to that type of risk management process?

Michigan Subscriber

Answer: A gap analysis has some benefits, but overall, your organization is better off sticking with the more thorough and involved risk analysis for HIPAA planning.

Here's why: "A gap analysis is typically a narrowed examination of a covered entity or business associate's enterprise to assess whether certain controls or safeguards required by the Security Rule have been implemented," notes the HHS Office for Civil Rights (OCR) in its Cybersecurity Newsletter. "A gap analysis provides a high-level overview of how an entity's safeguards are implemented and show what is incomplete or missing (i.e., spotting 'gaps'), but it generally does not provide a comprehensive, enterprise-wide view of the security processes of covered entities and business associates."

A gap analysis is a partial investigation of your HIPAA compliance practices and usually focuses specific problem areas such as IT systems, workforce sanctions for noncompliance, or logging protocols.

On the other hand, a risk analysis offers a more in-depth look at an organization's practices in their entirety - and OCR also allows CEs and BAs to choose their own methodology for implementation and documentation.

"There are certain practical elements" that entities should incorporate into their Security Rule risk analysis compliance, OCR says. Here's a short runsheet of what you should be doing as part of your risk analysis, according to the Cybersecurity Newsletter:

- Collect data.
- Determine scope of the analysis.
- Identify and document potential threats and vulnerabilities.
- Evaluate current security tactics.
- Gauge likelihood and potential impact of threats.
- Create risk analysis documentation.
- Review findings, update, and manage risks.