Revenue Cycle Advisor

powered by HCPro

ComplyAssistant

OCR report shows risk analysis remains an issue for organizations

February 8, 2021 | Briefings on HIPAA

In addition to struggling to properly fulfill patient records requests, organizations largely failed to implement sufficient risk analyses and risk management strategies, the recently released 2016-2017 HIPAA Audits Industry Report revealed.

The report found that 94% of covered entities (CE) and 88% of business associates (BA) failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

From a risk analysis perspective, 86% of CEs failed to substantially fulfill their regulatory responsibilities to safeguard electronic protected health information (ePHI), the report stated. Overall, 63 healthcare organizations were audited for risk analysis and risk management. The sizes of the organizations were not included in the report.

The findings, while troubling, were not surprising to experts.

"Being in the industry, I can see that," says **Jay Hodes**, president and founder of Colington Consulting in Burke, Virginia. "I do a lot of initial consultations with organizations. It's not like they don't want to follow the regulations. I don't think most understand what an accurate and thorough risk assessment is."

Let's review the report findings, as well as industry recommendations on how to correct some common errors.

Key takeaways

As part of the audit, the Office of Civil Rights (OCR) asked CEs to provide evidence that they had conducted a risk analysis and to provide policies and procedures for conducting an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI the organization creates, receives, maintains, or transmits. CEs were also asked to provide evidence to demonstrate that they had policies and procedures in place for a sufficient risk management process.

Overwhelmingly, organizations failed on both these fronts.

According to the audit report, the vast majority of organizations fell short on the following responsibilities:

- Identifying and assessing the risks to all of the ePHI in their possession
- Developing and implementing policies and procedures for conducting a risk analysis
- Identifying threats and vulnerabilities, considering their potential likelihoods and impacts, and rating the risk to ePHI
- Reviewing and periodically updating a risk analysis in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event
- Conducting risk analyses consistent with policies and procedures

In addition, OCR determined that CEs lacked the necessary focus on technical safeguards needed to properly protect ePHI. OCR also found that organizations' policies and procedures displayed a misunderstanding of the importance of determining acceptable levels of risk and how to mitigate the risks or vulnerabilities to ePHI.

Across the board, healthcare organizations have fallen into a rut regarding risk analyses and risk management tactics, says **Abner Weintraub**, principal consultant at Expert HIPAA in Spokane, Washington.

"Ruts are not sustainable in this fast-paced world," says Weintraub. "We've got to get out of the rut, find better resources and better information, and up our game on learning for senior management. I think that's been a big push for the OCR. They don't really provide the missing ingredients. They provide the push, they provide the overall direction, but they're not a resource for what's needed. It's up to organizations to find or create the knowledge base."

Experts agree that risk analysis and risk management simply have not been prioritized, and that needs to change.

"I just think organizations look at the minimum, punching the regulatory ticket, nothing is going to happen to us," says Hodes. "The problem is, if you do have a breach, that's when the Pandora's box gets opened up."

The cost of outsourcing a risk analysis—the best path for smaller to mid-sized organizations that lack the in-house resources—pales in comparison to the potential costs of suffering a breach, says Hodes.

With a breach comes an OCR investigation, providing information as a part of the data request, the patient notification process, and the possibility of class-action lawsuits. In the end, a comprehensive risk analysis is not only a regulatory requirement, but it's a worthwhile investment for all healthcare organizations.

Addressing the problem

Resources are available to help guide organizations through the process. **Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB**, vice president of privacy, compliance, and HIM policy at MRO Corp. in Norristown, Pennsylvania, says her organization uses a tool called Compliance Pro to assist in the risk assessment process. Similar services are also available.

Weintraub believes organizations should lean more on IT staff for guidance.

“The IT folks that are employed by healthcare orgs aren't expected to raise these issues with senior management,” Weintraub says. “They're expected to keep the data safe, shut up, stay at your desk, don't let the network be compromised, and don't let the data be stolen. The IT folks have the input that is missing from the risk analysis equation, and senior management, business leadership in the healthcare field needs to lean on those people to get a clearer sense of what the risks are.”

Of course, a more comprehensive education plan can make a significant difference. This is often an issue for smaller to mid-sized organizations that lack the resources to devote time, energy, and money to risk analysis education. **Helen Oscislawski, Esq.**, founder and managing partner of Oscislawski LLC in Princeton, New Jersey, believes medical society organizations or other collaborative resource-sharing organizations could do more to revisit these issues and provide the necessary education and support.

From an education standpoint, OCR provides some important resources. The website has been beefed up in recent years, says Hodes, with many more FAQs and other tools available. OCR and the Office of the National Coordinator for Health Information Technology also provide a HIPAA Security Risk Assessment tool specifically designed to assist small and medium healthcare organizations and BAs. Training sessions for using the tool are available, as well.

“I do want to give OCR some credit over the last four years. I think they've done a better job on the education aspect,” Hodes says. “It's a matter of organizations understanding where they can go to find that information. It's great that they are providing it, but they just need to continue to run this education campaign.”

The increase in technical application programming interfaces (API) and the move toward interoperability introduce new risks and vulnerabilities, says **Gerry Blass**, president and CEO of ComplyAssistant in Colts Neck, New Jersey. Compliance with the information access and the information blocking rule creates additional locations of ePHI, and thus more areas to assess in a risk analysis. Blass recommends periodic risk assessments in order to manage this ever-evolving environment.

“Interoperability is going to happen one way or the other,” says Bowen. “Whether people want it or not, they might be dragged into it, screaming gnashing of their teeth, they're going to have to do it because it just makes sense. So I think that a level of risk goes with that, and there's an opportunity for health information management professionals to embrace information governance to make all of this work.”