Report on Patient Privacy Volume 19, Number 8. August 07, 2019 Checklist for Using the SRA Tool

By Jane Anderson

The HIPAA security rule's risk analysis requires an accurate and thorough assessment of the potential risks and vulnerabilities to all of the electronic protected health information (ePHI) the organization creates, receives, maintains or transmits. Use these tips to navigate through the Security Risk Assessment Tool (SRA Tool) from the Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR) to conduct a thorough risk assessment:

- The SRA Tool is designed for small- to medium-sized organizations, so most larger organizations will find it isn't appropriate for their needs.
- When responding to questions to identify and assess potential risks, organizations should consider how the questions apply throughout the entire enterprise. Responding to questions without considering how the questions apply throughout the organization may result in a risk analysis that is not accurate and thorough, as required by the HIPAA security rule. For example, Lisa Steffey, project manager at Altarum, said, "When responding to questions about authentication, consider authentication throughout the organization, such as remote access authentication."
- Organizations should take care that responses reflect an accurate and thorough assessment of the questions presented, and are not merely a clerical exercise to produce a report.
- When navigating through the SRA Tool, users can revisit prior questions using the "Back" button. However, changing prior answers may change the branching logic, taking that user through a different path of questions.
- If potential risks to the confidentiality, integrity and availability of an organization's ePHI are known to the organization but are not accounted for by the SRA Tool, the organization should identify and assess these potential risks by either: documenting the potential risks in the most appropriate place within the tool, or supplementing the tool with additional documentation, which can be attached to the tool using the "add document" functionality.
- If the organization undergoes a significant change to its environment, users should start a new assessment instead of updating the old one. However, the organization can leverage the information contained in the old assessment to jump-start the process.
- Organizations don't submit their assessment to either ONC or OCR. Instead, they should keep the detailed report produced by the tool in their files to demonstrate HIPAA security rule compliance.
- Right now, all of the content in the SRA Tool is contained within the downloaded tool, and so the process can't be completed on paper. However, Altarum is working on a paper version of the tool.