Report on Patient Privacy Volume 19, Number 8. August 07, 2019 SRA Tool Can Help Identify Risks, But Responsibility Still Falls to Organizations

By Jane Anderson

The Security Risk Assessment Tool (SRA Tool) from the Office of the National Coordinator for Health Information Technology (ONC) can help small- and mid-sized covered entities identify where they may not be in compliance with the HIPAA security rule. However, organizations need to use the tool thoughtfully and recognize that it may not identify all risks.

"The health care industry needs a tool that is easy to use and can help small practices evaluate their security posture against increasingly sophisticated security attacks," Lisa Steffey, project manager at Altarum, the nonprofit research and consulting firm that created the latest version of the SRA Tool, said in a July 29 webinar sponsored by the Office for Civil Rights (OCR) and ONC.

The new SRA Tool, version 3.0 of the original tool created and released in 2014, provides users with an updated layout and an enhanced user experience, and has been downloaded more than 56,645 times, Steffey said.

Still, she added, "the SRA Tool is not a do-it-all tool." It can help users assess risks and vulnerabilities to protected health information (PHI), but it may not address all risks that are known, and risks not addressed by the SRA Tool must be documented elsewhere, Steffey said.

Content within the SRA is broken down into seven main categories:

- Section 1: SRA basics (the organization's security management process as it stands at the time of the evaluation)
- Section 2: Security policies, procedures and documentation (defining policies and procedures and whether the organization keeps documentation on hand)
- Section 3: Security and the workforce (defining and managing access to systems, plus workforce training)
- Section 4: Security and data (technical security procedures to keep data secure)
- Section 5: Security and the practice (physical security procedures such as maintaining locked doors)
- Section 6: Security and vendors (business associate agreements and vendor access to PHI)
- Section 7: Contingency planning (backups and data recovery plans)