MINTZ

Have You Updated Your HIPAA Security Risk Assessment Lately?

September 29, 2021 | Blog | By **Kate Stewart**

VIEWPOINT TOPICS

- Health Care

RELATED PRACTICES

- Health Care Compliance, Fraud & Abuse, and Regulatory Counseling
- Health Information Privacy and Security

RELATED INDUSTRIES

- Health Care

Last week, the **HHS Office for Civil Rights** (OCR) and the **Office of the National Coordinator for Health Information Technology** (ONC) hosted a webinar on the HIPAA Security Risk Assessment **Tool** (SRA Tool or the Tool). The webinar provided a guided tour of the SRA Tool, answered frequently asked questions, and gave updates on upcoming enhancements to the Tool. Most importantly, the webinar serves as yet another reminder for entities subject to HIPAA of their obligation to perform a security risk assessment and to update that assessment on a periodic basis and in response to new business processes, operations, and threats. Below are my top five takeaways from the webinar:

1. Just Do It!

A major theme of the webinar was the importance of conducting a thorough, periodic assessment of the security risks facing an organization. This analysis is a required administrative safeguard under the HIPAA Security Rule and is a critical tool in evaluating and improving the security of any organization subject to HIPAA. In countless settlements between OCR and covered entities, the failure of the covered entity to perform a comprehensive security risk analysis has been flagged as a major deficiency that contributed to a breach or other significant noncompliance. OCR and ONC have developed the SRA Tool as one option to help organizations comply with the requirement to conduct a risk assessment and to thoroughly document their assessment and mitigation strategies.

As was indicated multiple times in the webinar, an organization should anticipate spending a significant amount of time on conducting a risk assessment, whether or not using the SRA Tool, and that the quality of the assessment is dependent on the time and effort that the organization puts into it.

2. Cover the Entire Landscape

Critical to performing a comprehensive risk assessment is considering the entire security landscape of the organization. As the webinar reiterated, simply assessing the risks to a provider's EHR is insufficient. Organizations should instead consider all of the potential risks and vulnerabilities to electronic PHI throughout their enterprise when performing the assessment, including email, mobile devices, and cloud-based applications. The fact that a risk faced by an organization is not included in the SRA Tool isn't a "get out of jail free" card; the organization must still document that it evaluated the risk and may need to document that evaluation outside of the Tool.

3. Enhancements Are Coming

The webinar introduced SRA Tool users, or future users, to upcoming enhancements for the Tool. These enhancements include:

- The launch of an interactive spreadsheet version of the SRA Tool. The spreadsheet can be used by those who cannot run the software tool or prefer to work in a spreadsheet format.
- The incorporation of content from **Health Industry Cybersecurity Practices** (HICP) Technical Volume 1 into the Tool to give users additional context on cybersecurity best practices.
- The creation of a file association functionality to permit users to more easily open files created with the SRA Tool.
- The addition of new short instructional videos to help users navigate using the Tool.

4. MacOS Users are Still Out of Luck

Unfortunately for users of Apple computers and devices, the SRA Tool is still not compatible with macOS and the upcoming enhancements do not include compatibility. The webinar pointed out that macOS users will be able to use the downloadable, interactive spreadsheet version of the SRA Tool once it is released.

5. Give Feedback

Users of the SRA Tool can provide feedback on the Tool through the **SRA Tool User Experience Survey** . Those who have used the Tool in the past may want to provide their thoughts on the user interface and how the Tool could be improved in the future.

Authors

Kate Stewart, Of Counsel

Kate F. Stewart is Of Counsel at Mintz and a former in-house counsel who focuses on legal issues affecting health care clients, including digital health and privacy regulations, clinical trial compliance, and transactions for for-profit and nonprofit clients. She represents traditional health care providers, payors, and digital health start-ups.

More Viewpoints

Compliance is No Joke: OCR Releases Security Risk Assessment Tool

April 1, 2014 | Blog
Read more

OCR Releases Guidance on Reporting and Monitoring Cyber Threats

March 7, 2017 | Blog
Read more

OCR Provides Additional Clarification on Phishing Scam

December 2, 2016 | Blog
Read more