PUBLICATION

Changes to the Security Risk Assessment (SRA) Tool Require Attention

Authors: Alisa L. Chestler
October 18, 2018

The HHS Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) released an updated Security Risk Assessment (SRA) Tool this week. All covered entities and business associates must review this updated tool to ensure they are addressing the risks identified by OCR and ONC. An enterprise-wide SRA is not only a requirement of the HIPAA Security Rule, it is a foundational process designed to identify and mitigate security concerns for information systems to prevent costly data breaches whenever possible.

What is an SRA? First, it is helpful to know what it is not: It is not an assessment of how an organization meets each of the HIPAA Security Rule requirements. An assessment is only one small step in the process of an SRA; a properly conducted SRA also includes an analysis of the risks, threats and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (PHI). This information is then analyzed across all information systems with PHI to the likelihood of the harm and the potential risk (high, medium or low).

While the OCR/ONC SRA Tool was designed for use by small to medium-sized health care practices – those with one to ten health care providers – covered entities and business associates should consider reviewing the Tool to help them ascertain the kinds of risks and vulnerabilities to ePHI that OCR has identified. The updated tool provides enhanced functionality to document how organizations can implement or plan to implement appropriate security measures to protect ePHI. New features include but are not limited to a progress tracker, detailed reporting, and business associate and asset tracking.

Larger organizations (both business associates and covered entities) can benefit from reviewing these enhancements to ensure their continued understanding of how OCR will view SRAs and should use this as an opportunity to make sure the organization has an SRA that meets current expectations. Remember, the SRA is the first document requested by OCR in the case of a breach and is almost always cited as an issue in all OCR and States Attorneys' General settlement agreements.

A link to the updated SRA can be found here.

If you have any questions regarding the content of this alert, please contact Alisa Chestler, or any member of the Baker Ober Health Law Group.