PUBLICATION

Updated Version of HHS Security Risk Assessment Tool Released

November 11, 2019

October was National Cyber Security Awareness Month and, as its parting gift, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and the Office of the National Coordinator for Health Information Technology (ONC) released an updated version of the HHS Security Risk Analysis (SRA) Tool with additional features and improved functionality. In the event of an investigation or audit by OCR, a copy of the organization's most recent Security Risk Analysis (SRA) is often the first document requested. Version 3.1 of the SRA Tool may offer certain covered entities and business associates a useful tool for conducting an SRA without a third-party consultant.

The HIPAA Security Rule requires that covered entities and business associates conduct an accurate and thorough assessment – an SRA – of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (PHI) held by the covered entity or business associate. This can be a particularly difficult task for smaller providers who do not have the same resources as larger organizations. While OCR and ONC caveat that the Tool does not guarantee compliance with applicable state and federal laws, including HIPAA, the jointly-issued SRA Tool is intended to assist small and medium-sized covered entities in complying with the HIPAA Security Rule. At a high-level, the SRA Tool guides entities through a series of questions based upon the standards and implementation specifications from the Security Rule using the following seven sections:

1. **Security Risk Assessment (SRA) Basics**, which addresses the security management process;
2. **Security Policies, Procedures, & Documentation**, which helps organizations define their policies and procedures;
3. **Security & Your Workforce**, which helps organizations define and manage system access and workforce training;
4. **Security & Your Data**, which covers technical security procedures;
5. **Security & Your Practice**, which covers physical security procedures;
6. **Security & Your Vendors**, which covers business associate agreements and vendor access to PHI; and
7. **Contingency Planning**, which addresses backup processes and data recovery planning.

Once the seven assessment sections are completed, the Tool provides an SRA Summary, which includes total risk scores and risk scores per section, areas for review, and vulnerabilities applicable to the entity. The Tool also offers a risk report and detailed report with output of all information entered into the Tool.

In addition to improved functionality and the ability to export the final detailed report into an Excel spreadsheet, the new version 3.1 also includes the following new features:

- Incorporation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework for informational and cross-referencing purposes; and
- The option to "flag" questions for later where follow-up is needed and to create a report of those flagged questions.

Using the SRA Tool will take time and effort, and the results are only as useful as the data entered into the Tool. Although any entity can use it, the SRA Tool may not be practical for larger entities with a more complex information technology (IT) infrastructure and numerous vendor relationships. For these types of entities, and to ensure accuracy of the results, there is often value in bringing in a third-party expert to conduct an independent SRA. However, the HHS SRA Tool can be a good starting place for entities that do not have formal processes in place for conducting regular SRAs.

If you have any questions regarding whether the SRA Tool is appropriate for your organization, general HIPAA compliance, or any other cybersecurity or data privacy-related matters, please contact Alisa Chestler or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.