HHS's New Security Risk Tool for HIPAA Compliance

Authors: Alisa L. Chestler
March 31, 2014

On March 28, 2014, the HHS Office of the National Coordinator for Health Information Technology (ONC), in conjunction with the HHS Office for Civil Rights (OCR), released a Security Risk Assessment tool (SRA tool) to assist small- to medium-sized providers as they perform a security risk assessment, as required by the HIPAA Security Rule.

Often a daunting (and expensive) task, a security risk assessment is meant to uncover potential weakness in a provider's security policies, procedures and systems to prevent data breaches and other security incidents. A security risk assessment is the first step in HIPAA's core compliance obligations, and the lack of conducting a proper security risk assessment is the first issue cited in every enforcement action in this area. In the past, some of the largest penalties have been levied against those entities that experienced a data event, but failed to conduct a proper security risk assessment.

With the SRA tool, HHS is seeking to simplify the process for smaller providers. The SRA tool takes a provider through each HIPAA requirement by asking a series of "yes" or "no" questions (156 total) about an organization's activities. Every "yes" or "no" question will explain whether corrective action should be taken for a particular item. Notably, each question provides resources to help providers (1) understand the context of the question; (2) consider the potential impacts to the entity's PHI if the requirement is not met; and (3) see the actual safeguard language in the HIPAA Security Rule. All answers, comments and risk remediation plans can be saved directly in the tool. The results can be printed in PDF or Excel formats to produce a report for auditors.

The SRA tool is currently available for Windows and Apple's iPad operating systems. The SRA Tool application for iPad, available at no cost, can be downloaded from Apple's App Store.

If you have questions about performing a security risk assessment or other data security issues, please contact a member of the Firm's Health Information Technology group.