Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Department of Health & Human Services Upgrades Security Risk Assessment Tool

Publication — 10/31/2018

Under the Health Information Privacy and Portability Act (HIPAA), “covered entities” (generally speaking health care providers and their business associates) must all complete a risk assessment to identify and mitigate potential security risks (45 C.F.R. 164.308(a)(1)(ii)(A)). As many companies and providers have discovered, completing a risk assessment is time and resource-intensive and can be an overwhelming and expensive undertaking.

The Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) launched a security risk assessment tool in 2014 to help covered entities complete the required risk analysis. The ONC and OCR recently updated this tool to make it more user-friendly and to cover a broader range of risks to health information. The tool is designed for use primarily by small- to medium-sized health care practices (1 to 10 providers), covered entities, and their business associates, to help them identify and address potential risks to electronic protected health information (ePHI). And although the tool does not guarantee compliance with any laws, it may be a helpful tool for small- to medium-sized “covered entities” that either have never completed a risk assessment or that have not recently updated their risk assessment. The updated tool is currently only available for computers (laptop or desktop), although the iPad app for the old version of the tool is still available.

The new tool boasts many new features, including:

- Enhanced User Interface
- Modular workflow with question branching logic
- Custom Assessment Logic
- Progress Tracker
- Improved Threats & Vulnerabilities Rating
- Detailed Reports
- Business Associate and Asset Tracking

More information about the updates to the tool and the upgraded tool can be found at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

Completing a risk assessment, or updating an old assessment, is critical for any covered entity. All covered entities are required to complete an initial risk assessment and update that assessment “regularly” (45 C.F.R. 164.308(a)(1)(ii)(D)). Although the OCR has not defined what “regularly” means, with fast-advancing technology and ever-evolving security threats,

if your current risk assessment is more than a couple years old, or if you have recently made any meaningful changes to your IT systems, you should seriously consider performing a new risk assessment. With fines of $110 to $55,100 per HIPAA violation (45 CFR 160.404) (with each ePHI record considered a separate violation if there is a breach), the costs of non-compliance will quickly outpace the costs of the risk assessment if your systems are breached and any ePHI is compromised.

Holland & Hart has extensive experience helping its clients with all aspects of HIPAA compliance. Don't hesitate to contact Kim Stanger, Steve Lau, or Romaine Marshall for questions about or help with completing a risk assessment, responding to a data breach (or potential breach) of ePHI, or for general questions about HIPAA compliance.