BURR FORMAN LLP

# HHS OCR/ONC Announce an Updated Version of Its HIPAA Security Risk Assessment Tool

Articles / Publications
*Reprinted with permission from Birmingham Medical News*
10.23.2023

The Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) have recently launched a joint HIPAA Security Risk Assessment (SRA) Tool. The tool is designed to assist small and medium-sized health care practices and business associates in complying with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Particularly, the SRA Tool helps entities identify and assess risks and vulnerabilities to their electronic protected health information (ePHI), which can be downloaded at no cost. It is designed to help smaller organizations identify risk and make a plan for remediation and compliance.

All ePHI created, received, maintained, or transmitted by an organization is subject to the HIPAA Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security and integrity of ePHI.

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way, and reports are available to save and print after the assessment is completed.

RELATED PROFESSIONALS

James A. Hoover

RELATED CAPABILITIES

Health Care

Health Care Compliance

# HHS OCR/ONC Announce an Updated Version of Its HIPAA Security Risk Assessment Tool

Version 3.4 contains several key updates based on user feedback, including a remediation report, which allows users to track responses to vulnerabilities inside the tool and log remediation efforts. In addition, the tool now contains a glossary and tooltips section, where users can learn more information and easily navigate the tool's features. Other improvements include bug fixes, usability improvements, and references to the 2023 edition of the Health Industry Cybersecurity Practices (HICP) publication.

The Security Rule requires that covered entities and its business associates conduct a risk assessment of their organization. A risk assessment helps an organization ensure that it is compliant with HIPAA's administrative, physical, and technical safeguards. Although the use of the tool does not mean an organization is compliant with the HIPAA Security Rule or other federal, state, or local laws and regulations, it does, however, assist organizations with the HIPAA Security Rule requirement to conduct periodic security risk assessments.

In addition to an express requirement to conduct a risk analysis, the Security Rule indicates that a risk analysis is a necessary tool for reaching substantial compliance with many other standards and implementation specifications. For example, the Security Rule contains several implementation specifications that are labeled "addressable" rather than "required." An addressable implementation does not mean the specification is optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate.

The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate. Accordingly, organizations should use the information gleaned from their risk analysis to design appropriate personnel screening processes, identify what data to backup and how to back it up, decide whether and how to use encryption, address what data must be authenticated in particular situations to protect data integrity and determine the appropriate manner of protecting health information transmissions.

There are numerous methods of performing a risk analysis, and there is no single method or "best practice" that guarantees compliance with the Security Rule. The scope of a risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI the organization creates, receives, maintains, or transmits. This includes ePHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus, an organization's risk analysis should take into account all of its ePHI, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted or the source or location of its ePHI.

A risk analysis is the first step in an organization's Security Rule compliance efforts. Risk analysis is an ongoing process that should provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of ePHI. The latest SRA Tool can help an organization with this first step.