COSMOS
Navigate the Compliance Universe

Compliance Today - February 2023
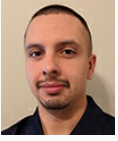
Frank Ruelas Jr. (frank@compliacademy.com) is Compliance Manager, PCP of AZ.

The latest version of the Security Risk Assessment Tool — version 3.3

by Frank Ruelas Jr.

In June 2022, version 3.3 of the Security Risk Assessment Tool (SRA Tool) was released and posted on the HealthIT.gov website.[1] This version of the SRA Tool is the latest version of an application that can be downloaded and used to help organizations comply with the HIPAA Security Rule's risk analysis implementation specification, which is listed within the security management process standard at 45 C.F.R. § 164.308(a)(1)(i). The SRA Tool is made available through a collaborative effort between the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) and the Office of the National Coordinator for Health Information Technology.

Several improvements have been made since its original release in March 2014, which makes for a more effective and efficient user experience as the tool walks users through the steps of completing a security risk assessment described in the tool's user guide.

Ongoing challenge

Complying with the risk-analysis requirement is a long-standing challenge for compliance professionals working to comply with the HIPAA Rules. In December 2020, the OCR released the results of its 2016-2017 HIPAA Audits Industry Report. The report indicated that 14% of the audited covered entities and 17% of the business associates were shown to have achieved a rating of 1 or 2 on a scale from 1 to 5 to how effectively the OCR assessed their level of compliance with the Security Rule's risk analysis requirement. The following is a description of the ratings used in the audits:

> "A rating of 1 reflects a high understanding and strong implementation of the audited elements. A 2 rating reflects activities that are largely in compliance, but reveal some weaknesses. A 3 or 4 rating reflects serious shortcomings in compliance efforts, and a 5 means no serious effort was taken by the entity."[2]

HHS has also contributed guidance containing information and suggestions related to complying with the risk analysis requirement in its HIPAA Security Series.[3] In addition, the document reviews important definitions, useful information on the types of methods that can be used to complete a risk analysis, and a step-by-step description of suggestions on how to complete a risk analysis.

SRA Tool and HIPAA compliance

On the website where the SRA Tool is posted, it clearly indicates that the use of the SRA Tool does not guarantee

compliance with the HIPAA Security Rule. The webpage also includes a recording of a webinar where the presenters repeatedly state that the SRA Tool is just that: a tool that can be used to help a covered entity or business associate comply with the risk analysis requirement. It is essential to note that in the recorded webinar, the presenters use the terms "risk assessment" and "risk analysis" interchangeably. This is understandable given that in the HIPAA Security Rule, the phrase "risk analysis" is used; in contrast, in the National Institute of Standards and Technology 800-30 publication—which is used as a cross-reference within the tool—the phrase "risk assessment" is used.[4]

The user guide for the SRA Tool also describes that the purpose of the SRA Tool is to help organizations work towards compliance with the HIPAA Security Rule's risk analysis requirement. As stated in the recorded webinar, there is repeated mention that a security risk analysis must be accurate and thorough to comply with the HIPAA Security Rule. As such, users are reminded they need to supplement the SRA Tool with additional information to show that the risk analysis is accurate and thorough concerning the operating environment of the covered entity or business associate. Because the tool could not be designed to capture all the possible threats and vulnerabilities that a practice may include in its risk analysis, version 3.3 of the tool contains numerous text boxes where a user of the tool can add additional information as needed to make sure the risk analysis is accurate and thorough.

This document is only available to members. Please log in or become a member.

Become a Member Login