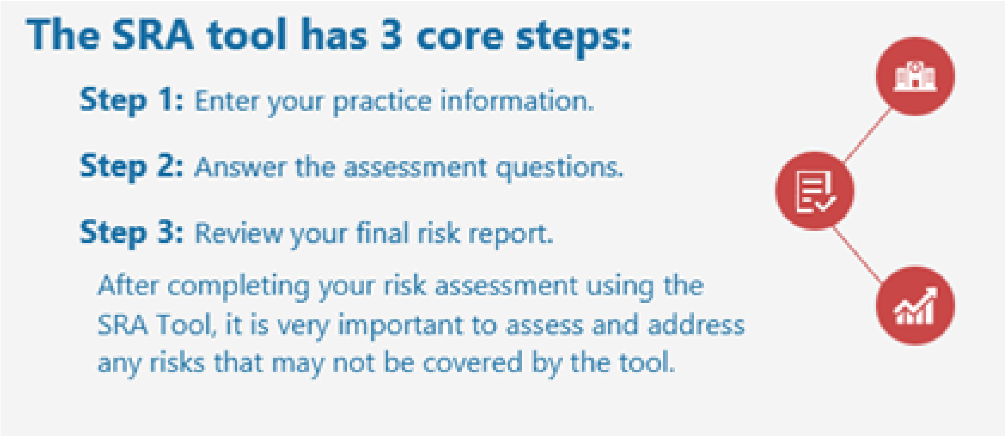
How to Use the HIPAA Security Risk Analysis to Improve Compliance

The first time you conduct a Security Risk Analysis (SRA), it may seem a little difficult to answer each question with 100% confidence — but that's alright. Getting through the process for the first time is a great starting point. The SRA provides the framework for understanding *Vulnerabilities*, *Threats*, and *Risks* applicable to your organization. The intent of the SRA is to perform an analysis on an annual basis or anytime there is an incident or new threat discovered.

The SRA begins with answering basic questions about your organization and ensuring that you have identified all of the equipment that is capable of receiving, storing, and transmitting Protected Health Information (PHI).

W*hy is this important*? Computers, servers, fax machines, copiers, and many types of medical equipment can store PHI.



The SRA tool has 3 core steps:

Step 1: Enter your practice information.

Step 2: Answer the assessment questions.

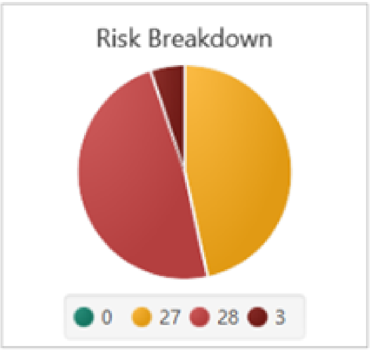
Step 3: Review your final risk report.

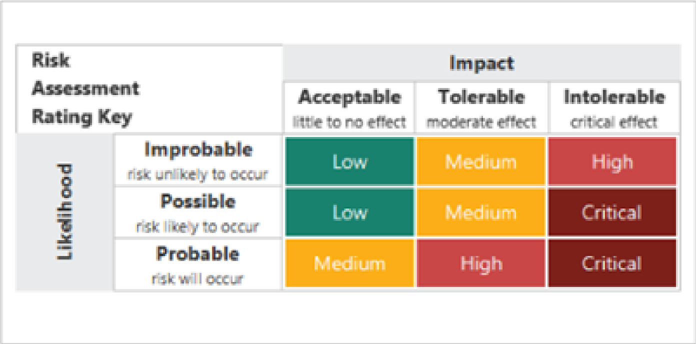
After completing your risk assessment using the SRA Tool, it is very important to assess and address any risks that may not be covered by the tool.

TIP 1: Keep an inventory of all electronic equipment and maintain a system to identify and manage all electronic equipment from the point of entry, how it is secured, assigned, and ultimately disposed.

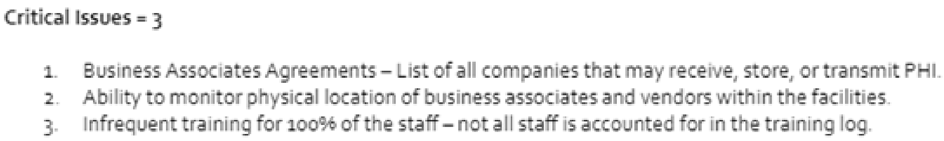
TIP 2: If personal smart phones and tablets are used by providers or staff, make sure to have clear policies on accessing, storing, and sharing PHI.

The Risk Analysis must take into consideration how PHI is received, stored, and transmitted. An SRA with a score indicating high-risks and vulnerabilities should be taken very seriously. While it's common for healthcare organizations to have *trusted* *vendors* that provide equipment or IT services, the SRA may reveal inadequate computer systems, questionable user activity, unconfirmed identities, or unsecure connections between the IT infrastructure and devices.





Risk Assessment Rating Key		Impact		
		Acceptable little to no effect	Tolerable moderate effect	Intolerable critical effect
Likelihood	Improbable risk unlikely to occur	Low	Medium	High
	Possible risk likely to occur	Low	Medium	Critical
	Probable risk will occur	Medium	High	Critical



Critical Issues = 3

1. Business Associates Agreements – List of all companies that may receive, store, or transmit PHI.
2. Ability to monitor physical location of business associates and vendors within the facilities.
3. Infrequent training for 100% of the staff – not all staff is accounted for in the training log.

TIP 3: A trusted service that has actual or potential access to PHI should always have a written Business Associate Agreement (BAA) and transparency regarding how the business associate (BA) will protect PHI. Proper staff training at both organizations will help to create awareness and accountability.

TIP 4: BAs should be ready and willing to verify that staff have been properly trained and that access to systems and equipment are monitored to ensure information is used for the intended purpose. BAs are directly liable for breaches.

Once you have completed the SRA, it is important to share it with the appropriate stakeholders and elicit feedback on closing operational gaps to decrease potential vulnerabilities. Making sure that the organization has policies in place as a result of the SRA findings, will help to facilitate a culture of compliance and awareness. This is key to being prepared and must include how to recover from natural and man-made (cybersecurity) events, should they occur.

TIP 5: MedTrainer's Policy and Document Management tool is a great mechanism to ensure that HIPAA Security policies are acknowledged and supported by the educational content in MT | Learning.

Imagine the impact of sharing the SRA with everyone in the organization to develop location-specific job aides, simple reporting instructions, and organizational engagement on a whole new level!