Indian Health Service

HIPAA Security Risk Assessments

REESE WEBER, MBA, CISSP

2023 IHS PARTNERSHIP CONFERENCE

AUGUST 21-24, 2023

Objectives

Why Perform an Assessment?

Take stock!

Downloading and Installing the Security Risk Assessment (SRA) Tool

Using the SRA tool for assessment

Determining local hazards using the FEMA National Risk Index

SRA Reports

Follow-Up

Why Perform a Security Risk Assessment?

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule **requires** that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk.

Outsourcing HIPAA SRA is Unnecessary

YOU know more about your clinic operations than anyone else

Private assessments cost between $5K and $25K+

There is no REQUIREMENT for an external party to conduct assessment

Who should be involved?

The Security Risk Assessment is NOT an exclusively IT task. In fact, most of the assessment covers policies, procedures and planning.

The assessment should include, but is not limited to:

- ❑ A formally appointed Security Officer
- ❑ Informatics and/or Clinical Applications Coordinator
- ❑ IT Site Manager
- ❑ EHR Site Manager
- ❑ Clinic Manager and/or Medical Director
- ❑ CEO or Clinic Director
- ❑ Network administrator(s)

Expectations

- This will be a significant time investment in this process – 4 hour minimum if ALL information and clinic knowledge is handy and accessible
- You get out of it what you put into it
- Try to think outside the box – focus on actual clinic operations/workflows versus ideals
- Be prepared to troubleshoot and/or solve on the spot
- Consider ALL systems that MAY house PHI, regardless of whether or not it SHOULD
  - Network Drives
  - Emails
  - Cloud based file systems, local file systems
  - Local workstations, handheld devices
- Ensure the assessment team has access to:
  - Network and security configurations
  - Policies and Procedures for the clinic
  - Vendor and Contractor information
  - Business Associate Agreements and/or contracts

Take Stock – Inventory your Assets

You can't protect it if you don't know you have it

- Use Crowdstrike, Forescout or some network discovery tool to locate and identify clinic equipment
- Physically walk through facilities to locate and identify equipment
- Query Active Directory or other LDAP software to see domain joined systems
- Interview individual departments to uncover "Shadow IT" products
- Involve facility or maintenance manager to discover facility automation systems (HVAC, solar, security, etc.)
- Use Wi-Fi APs and network equipment to discover IoT pro

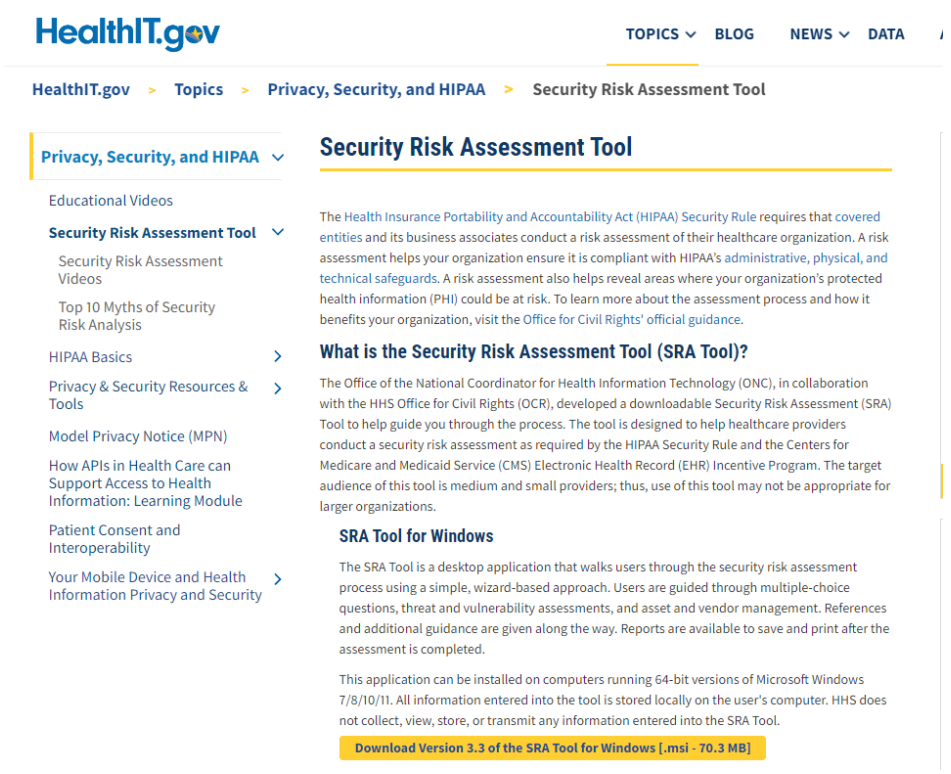
Downloading and Installing the SRA Tool

The tool can be downloaded from HealthIT.gov

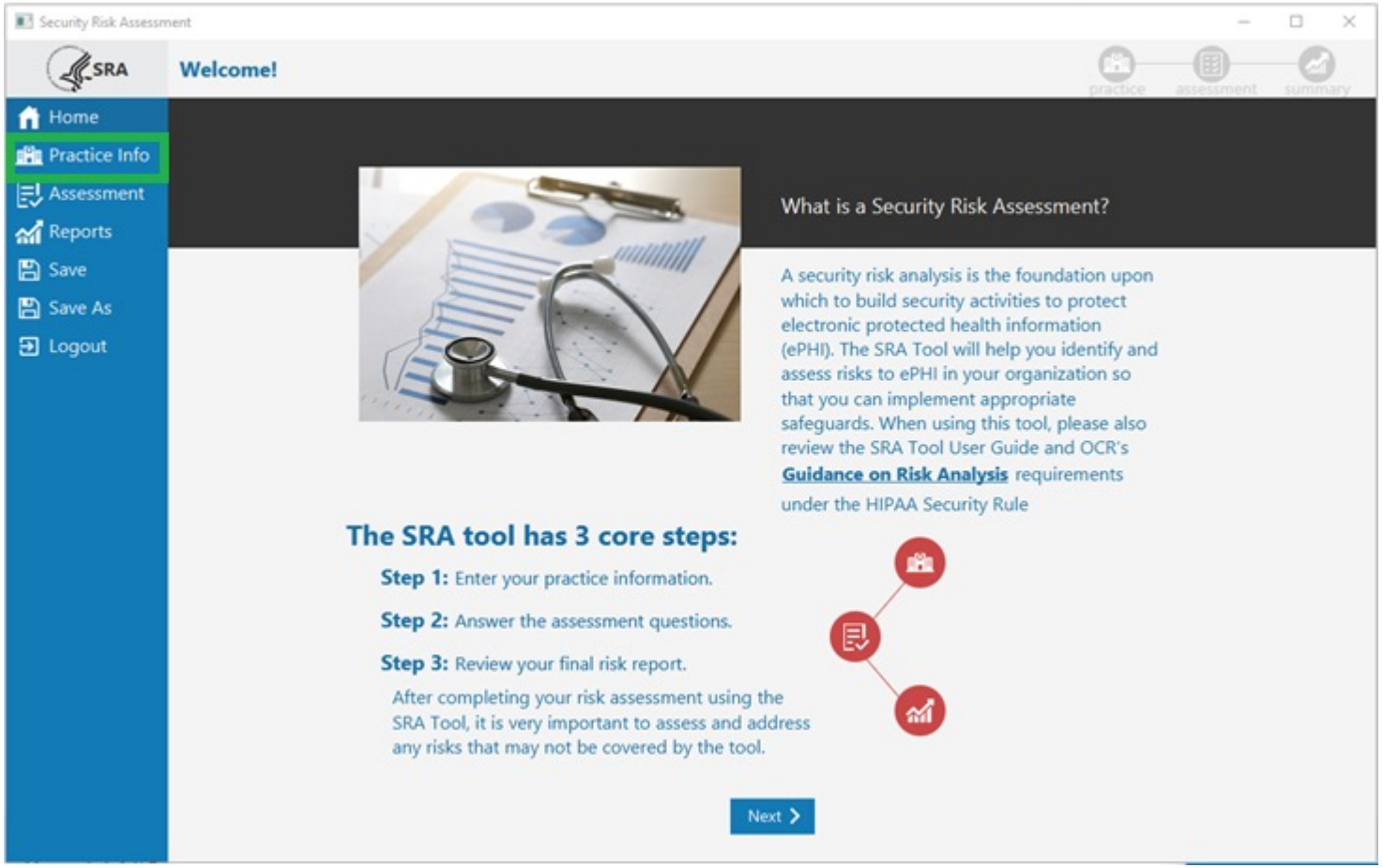
The downloaded file is the installer for the tool. Double click to run the installer and walk through install process. Once downloaded, a blue “SRA-Tool” icon will appear on your desktop.

Note: Users must have administrative privileges in order to install the SRA Tool. For this reason, you may need help from your IT department or system administrator to install the tool. Admin privileges are not needed to run the tool once it has been installed.

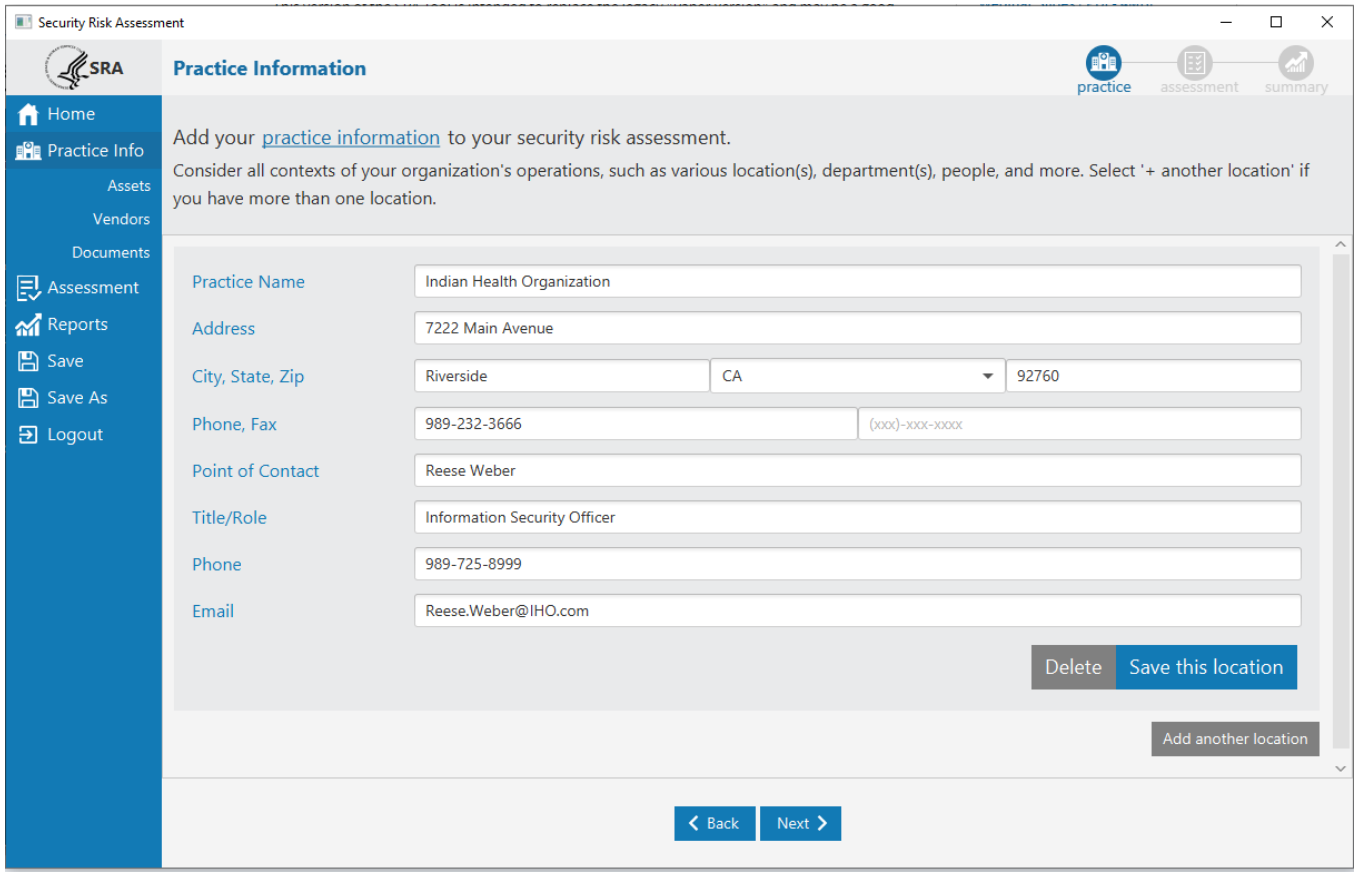
The tool runs on Windows, 7, 8, 10, and 11. All information entered into the tool is contained locally. No information is transmitted to DHHS, ONC or OCR.



Security Risk Assessment (SRA) Tool



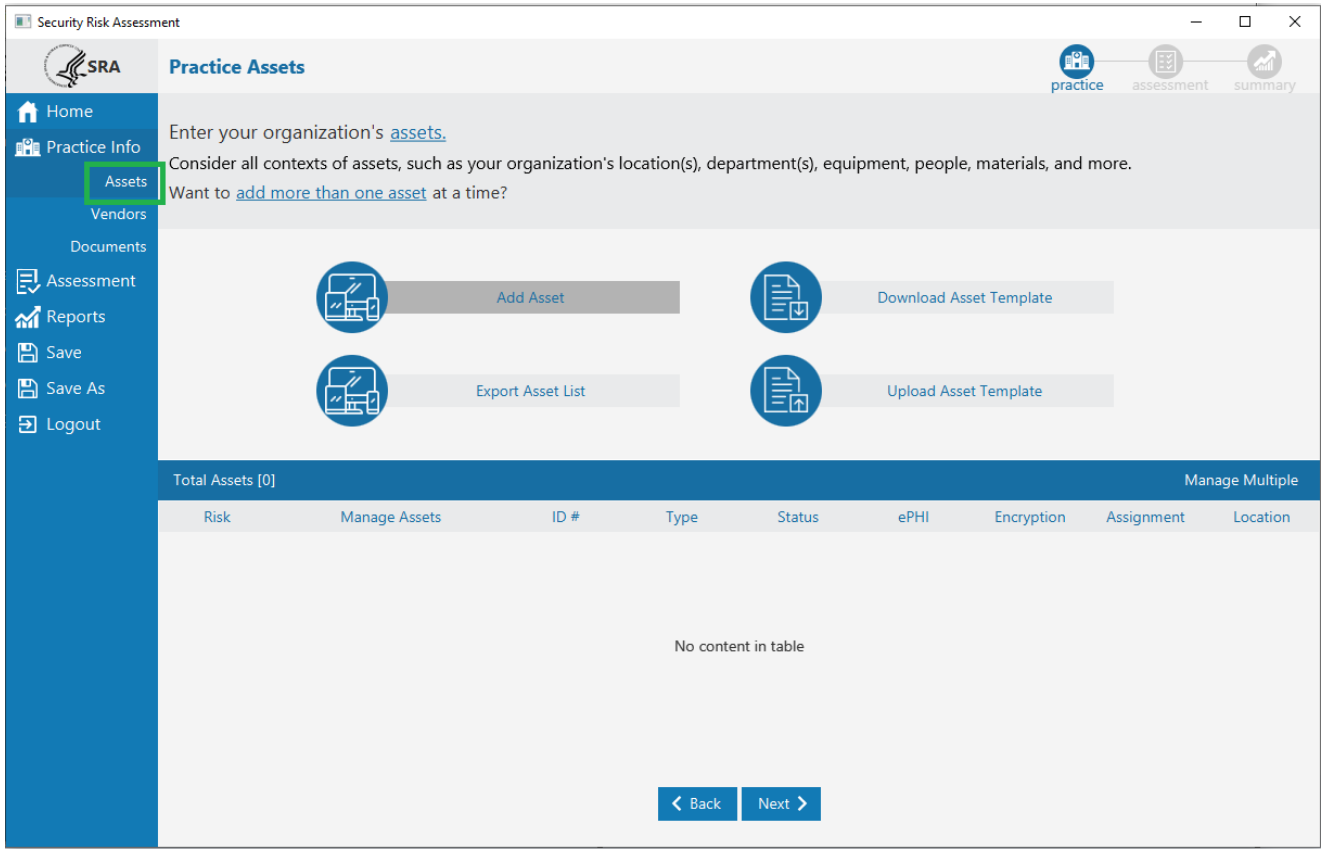
Clinic and Practice Information



The Practice Information screen captures some basic information from the practice(s) involved with the assessment.

This information will be included in the printable PDF report available once the assessment is completed.

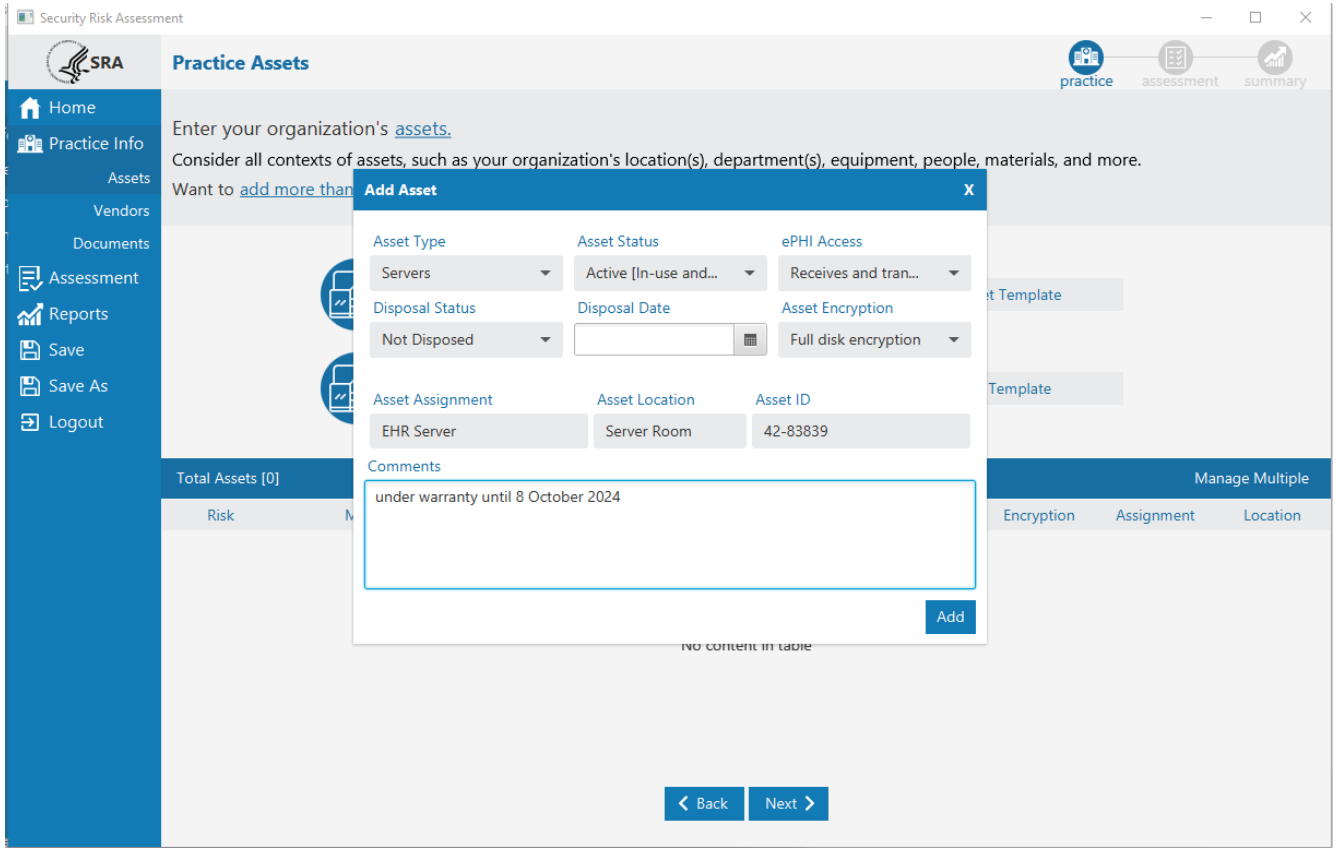
Assets – IT Equipment



The Assets screen captures a list of IT assets within a practice – computers, diagnostic/imaging equipment, network infrastructure, etc…

Assets can be entered one at a time, or imported in a list from a CSV file by using the Asset Template.

Assets – IT Equipment



Available Fields

- Asset Type
- Asset Status – active, inactive
- ePHI Access – does it access PHI?
- Disposal Status – if inactive, has it been properly wiped/disposed?
- Disposal Date – date asset was disposed
- Asset Encryption – type of encryption protection of data
- Asset Assignment – who is responsible for this asset?
- Asset Location – physical location of the asset.
- Asset ID – asset tag or internal identifier
- Comments

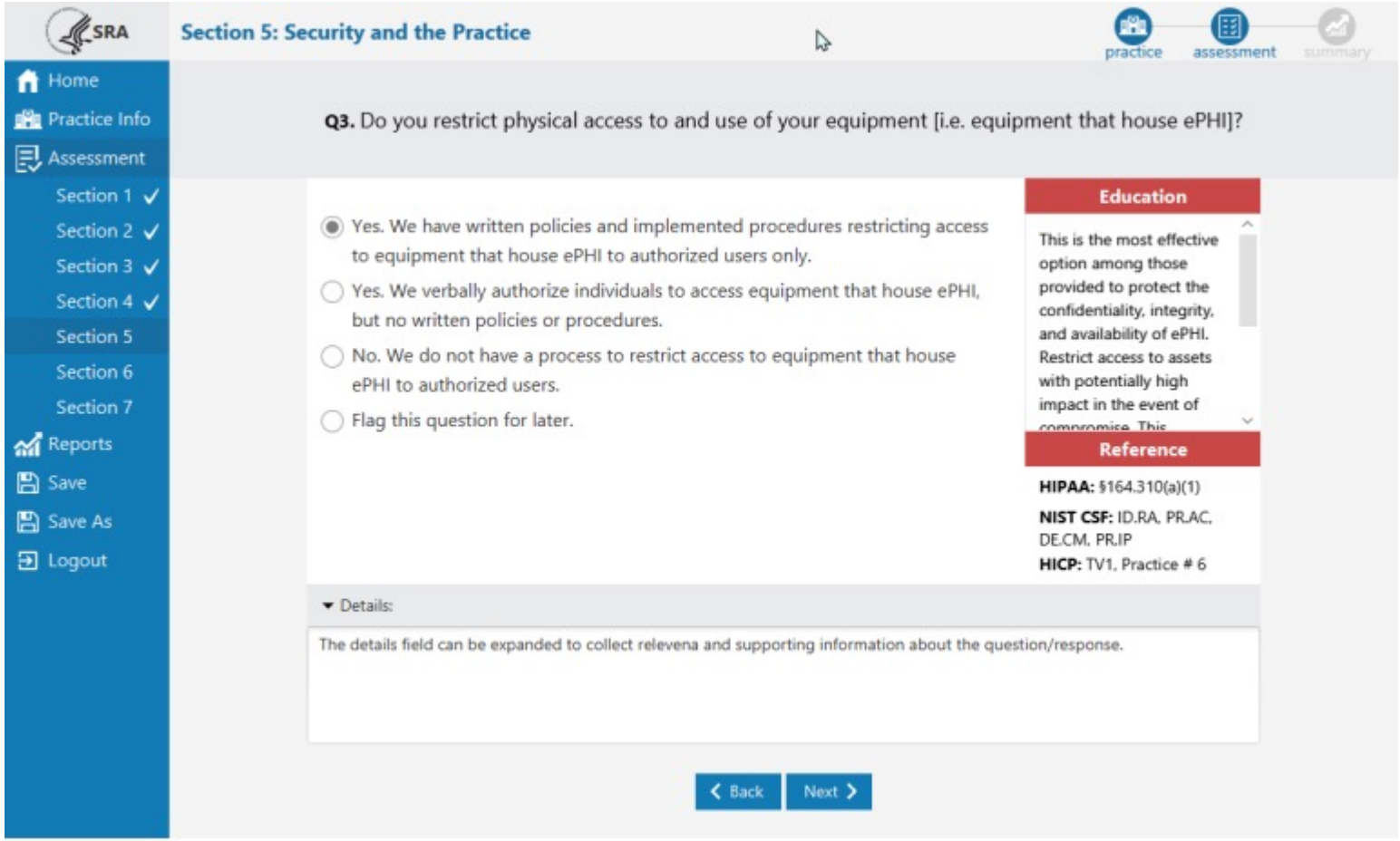
Assessment

The Assessment section contains 7 sections with multiple -choice questions and branching logic.

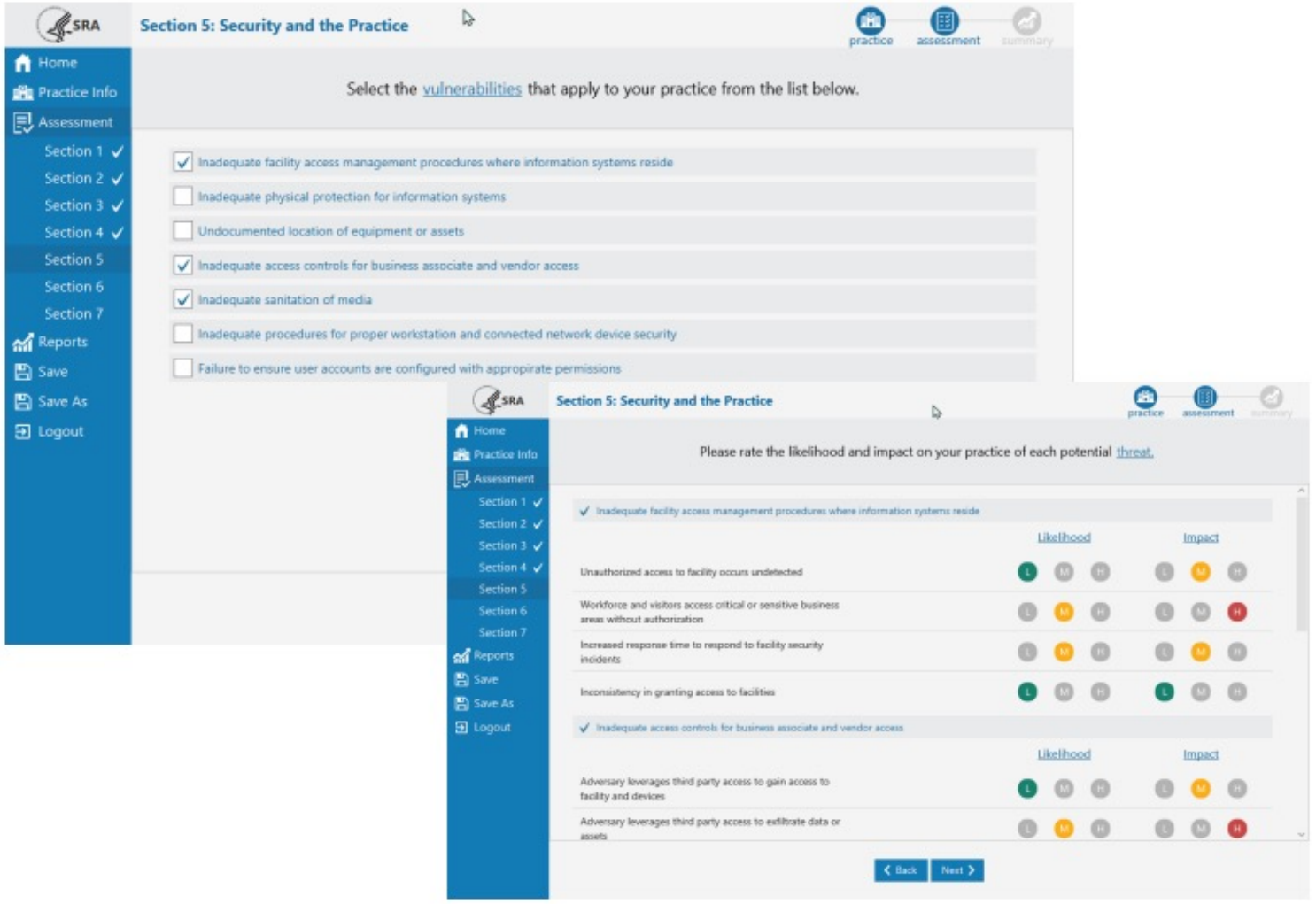
The Education panel provides guidance related to each response given.

The Reference panel links each question to a HIPAA Security Rule citation.

Progress indicators are provided in the navigation panel as sections are completed.



Vulnerabilities and Threat Ratings



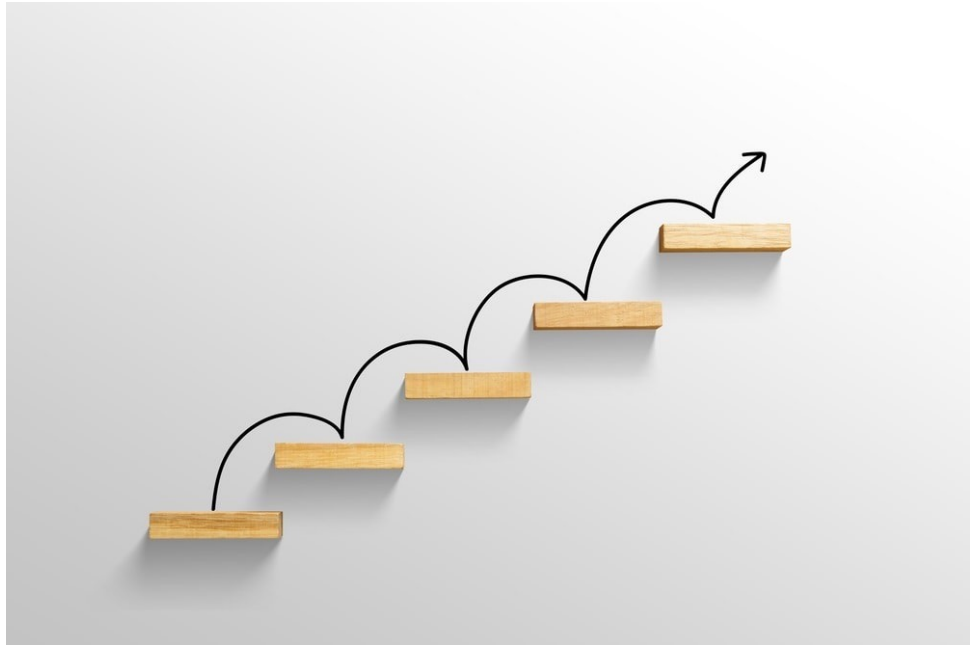
The Vulnerability Selection and Threat Rating section is presented after each section of multiple-choice questions.

Users are asked to select from a list of vulnerabilities that may be applicable to their practice.

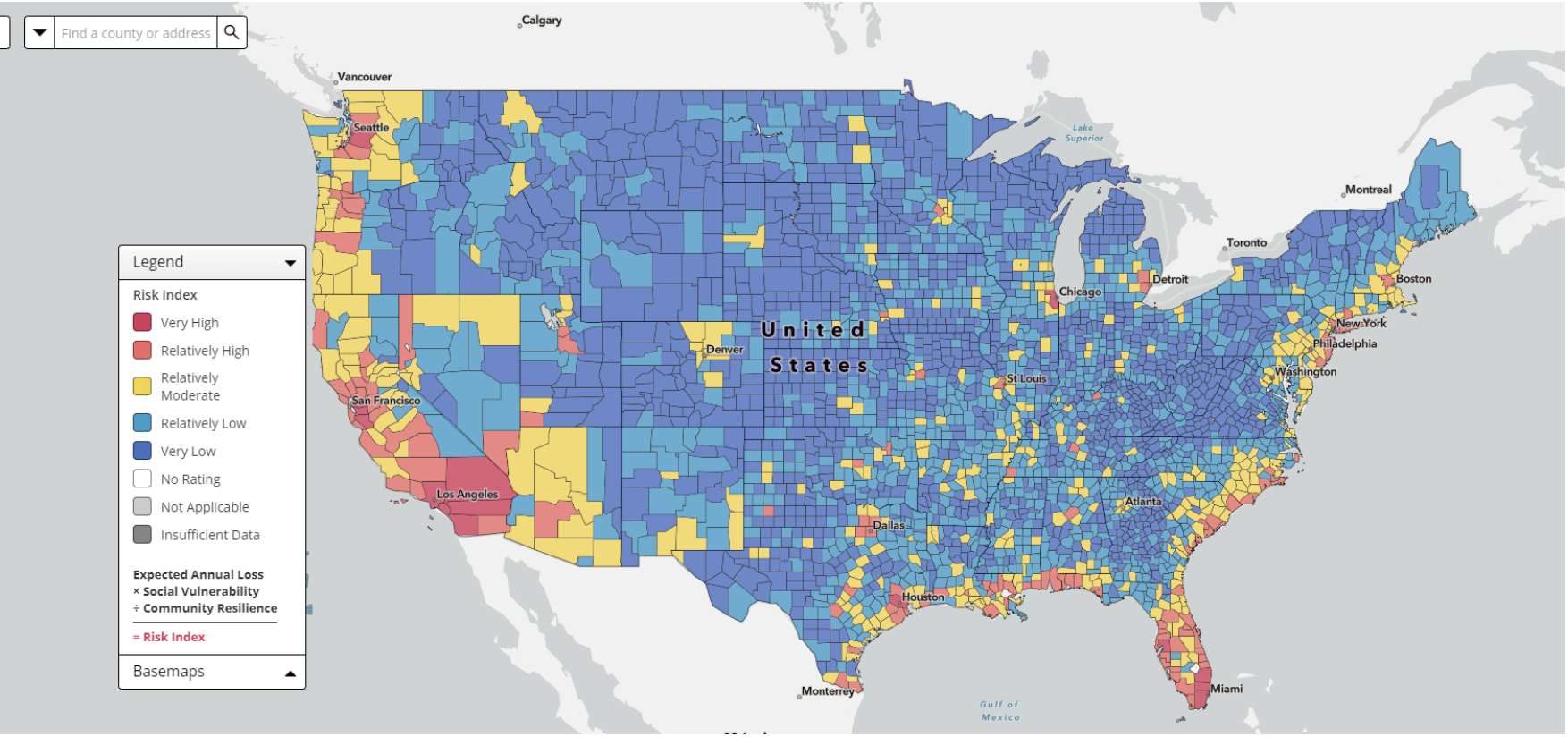
Each vulnerability comes with a list of related threats that must be rated for the **likelihood** they may occur and the **impact** they would have should they occur.

Don’t Overstate your Security Posture!

- Keep in mind – the CFR *requires* initial and periodic ASSESSMENT – not a perfect score!
  - By honestly assessing your organization’s posture, you create an ACTUAL opportunity for improvement
  - During an OCR Audit- they are looking for *improvement* between assessments
  - Overstating the cyber abilities *reduces* your organization’s ability to show improvement
  - There is NO SUCH THING as a perfectly secure environment



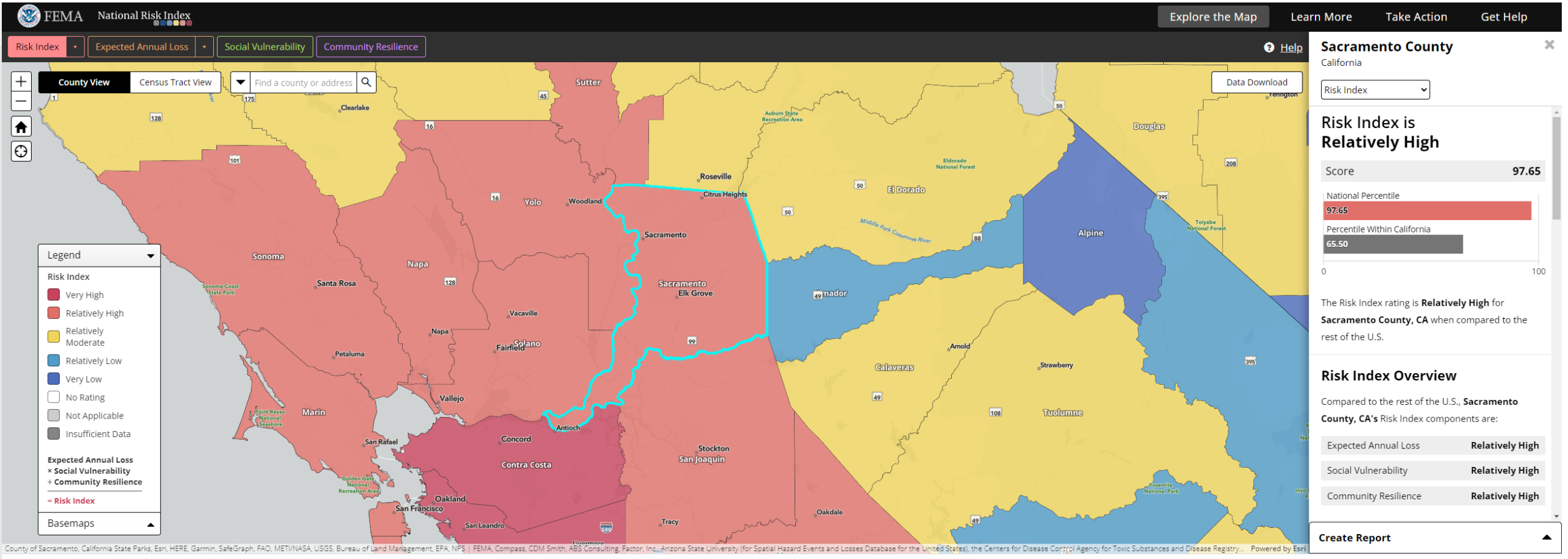
Determining Natural Risks to your Clinic



FEMA's National Risk Index (NRI) is an easy-to-use, interactive tool that shows which communities are most at risk to natural hazards. It includes data about the expected annual losses to individual natural hazards, social vulnerability and community resilience, available at county and Census tract levels.

https://hazards.fema.gov/nri/map

What's the Risk Index for YOUR county?



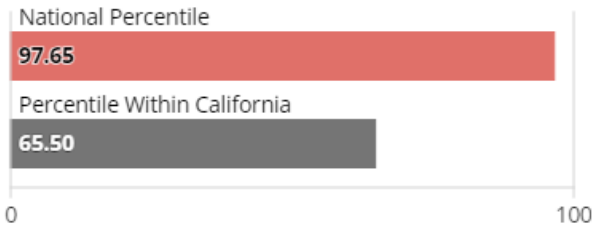
Sacramento County

California

Risk Index

Risk Index is **Relatively High**

Score	**97.65**



The Risk Index rating is **Relatively High** for **Sacramento County, CA** when compared to the rest of the U.S.

Risk Index Overview

Compared to the rest of the U.S., **Sacramento County, CA's** Risk Index components are:

Expected Annual Loss	**Relatively High**
Social Vulnerability	**Relatively High**
Community Resilience	**Relatively High**

Hazard Type Risk Ratings

Compared to the rest of the U.S., **Sacramento County, CA's** risk to each hazard type is:

Avalanche	Not Applicable
Coastal Flooding	No Rating Score **0.0**
Cold Wave	No Rating Score **0.0**
Drought*	**Very High** Score **99.7** *Note: Risk Index is based on Agricultural (crop only) impacts
Earthquake	**Relatively High** Score **99.0**
Hail	**Very Low** Score **17.8**
Heat Wave	**Relatively High** Score **99.2**
Hurricane	Not Applicable
Ice Storm	Not Applicable
Landslide	**Relatively Moderate** Score **91.3**
Lightning	**Very Low** Score **27.0**
Riverine Flooding	**Relatively Moderate** Score **75.4**
Strong Wind	**Very Low** Score **1.7**
Tornado	**Relatively Low** Score **69.6**
Tsunami	No Rating Score **0.0**
Volcanic Activity	Not Applicable
Wildfire	**Relatively Moderate** Score **93.0**
Winter Weather	**Very Low** Score **11.5**

Assessment Summary Report

After all sections are complete, the Summary section becomes available.

The Summary Report is high level summary of your risk assessment.

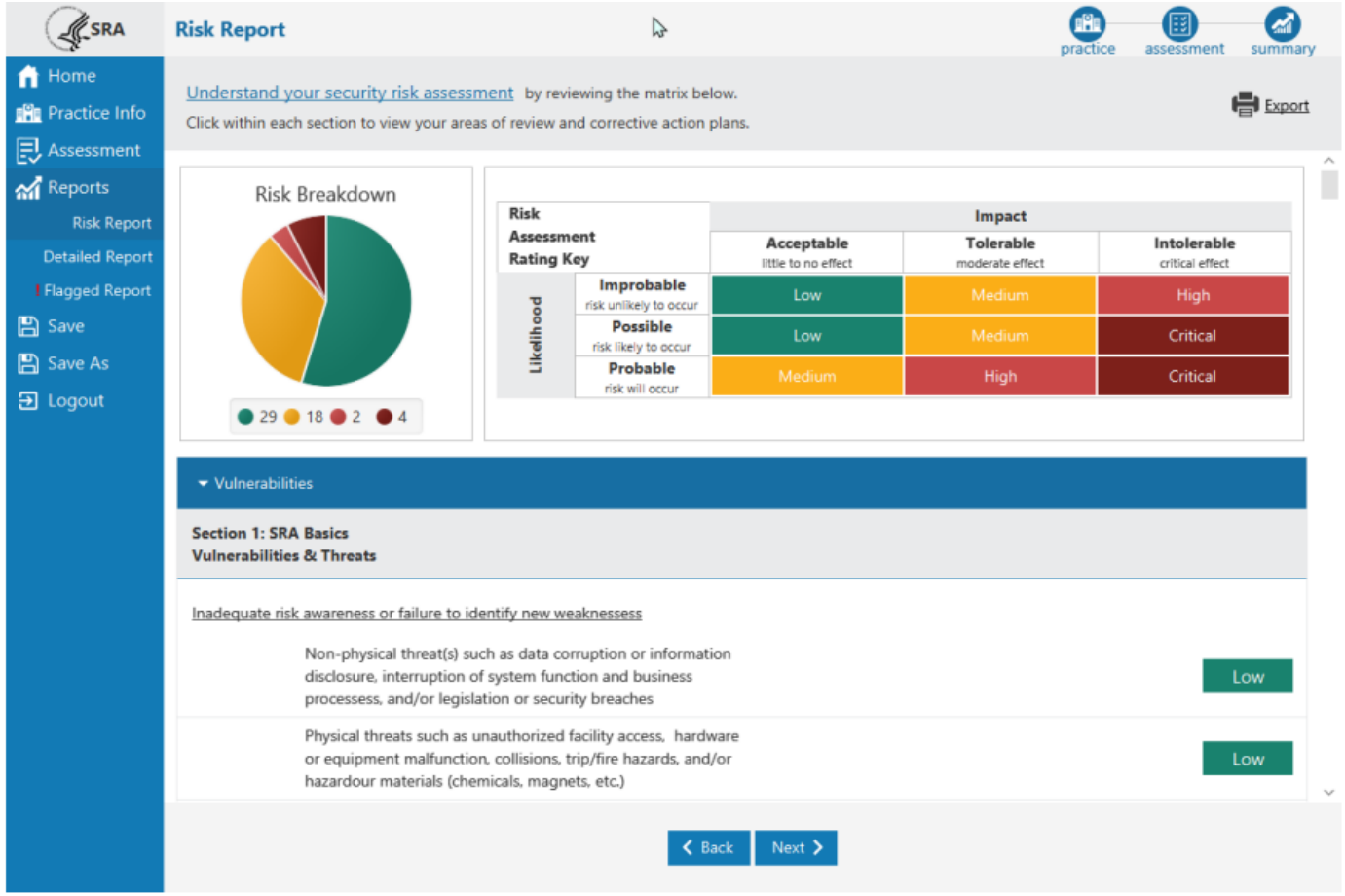
Risk Score –shows the number of questions sorted into Areas for Review divided by the total questions the user answered.

Areas for Review –shows the total number of questions answered sorted into Areas for Review.

Vulnerabilities –shows the total number of vulnerabilities selected as applicable to the practice or organization.

Each assessment section's Risk Score is shown as a percentage.

Risk Report



The Risk Report identifies all areas of risk collected across your entire assessment.

Each vulnerability selected is shown here along with each response that fell into the category Areas for Review.

Risk Breakdown – shows a sum of threat ratings in each risk level (Low, Medium, High, and Critical).

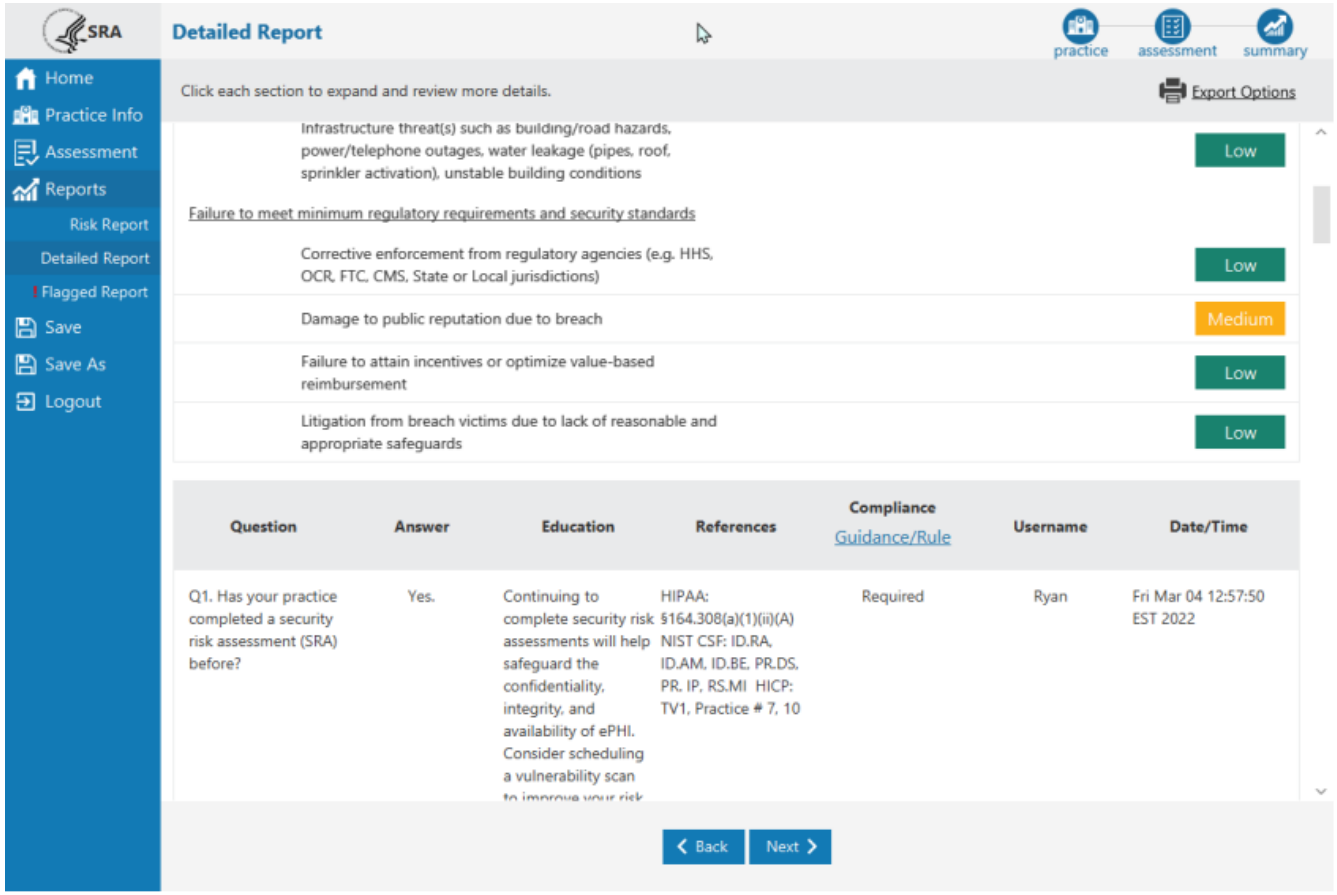
Risk Assessment Rating Key – shows how likelihood and impact ratings combined create the risk level.

Detailed Report

The Detailed Report is a collection of all data captured throughout the entire assessment.

Each question and response, each threat and vulnerability rating, all of the Practice Information, Assets, and Vendor information is shown in the Detailed Report. There is also an audit log of each contributing user with a date/time stamp.

Export a PDF or Excel copy of the report using the Export Options button.



Follow-up Actions

Using the SRA Risk Reports, begin addressing and taking action on findings.

Prioritize activities using the Low, Medium, High and Critical designations.

Create and/or update Policies and Procedures to address specific findings

Schedule follow up meetings to track progress

Consider implementing a permanent, multi-disciplinary committee responsible for reviewing and updating future assessments

Questions?

Reese Weber, MBA, CISSP

Chief Information Security Officer and Privacy Coordinator

Indian Health Service, California Area

916-930-3981 x 307

Theresa.weber@ihs.gov

https://www.linkedin.com/in/reese-weber-mba-cissp-6085203b

References:

CMS Guidance for Risk Analysis - https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/downloads/2016_securityriskanalysis.pdf

FEMA National Risk Index - https://hazards.fema.gov/nri/

HHS HIPAA Security Risk Assessment Tool - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

HHS / HealthIT.GOV SRA User Guide - https://www.healthit.gov/sites/default/files/page/2019-10/SRATv3.1User%20Guide.pdf

HHS Summer 2020 Cybersecurity Newsletter - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2020/index.html#footnote8_bdqzath


INDIAN HEALTH SERVICE
PHS · 1955 ·