

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

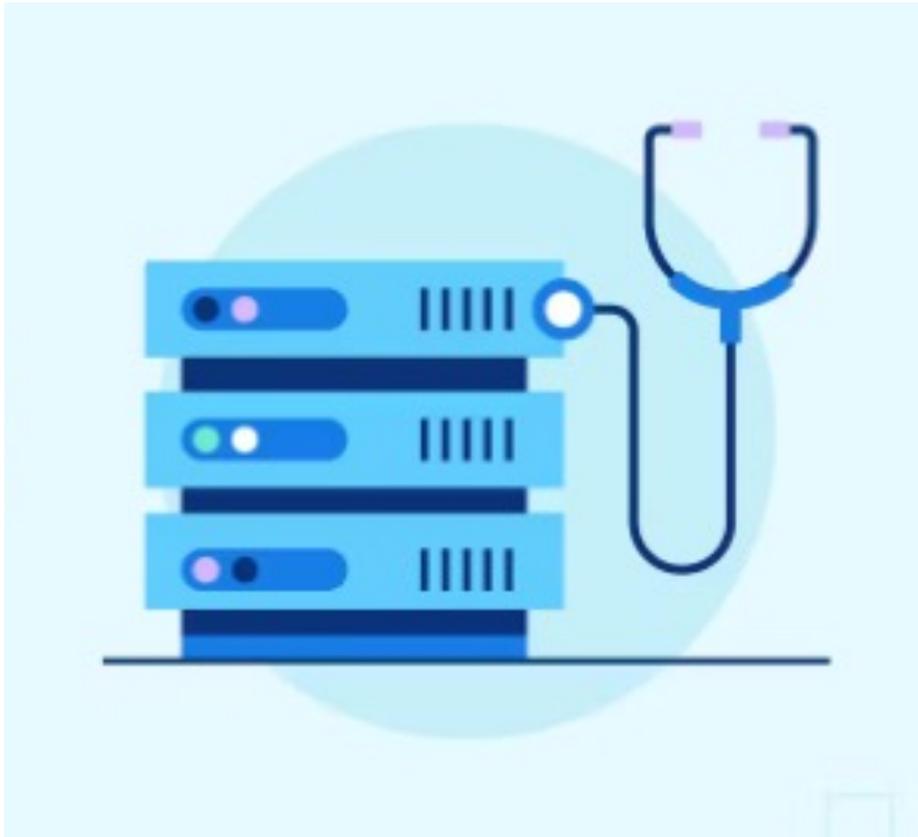
Using the SRA tool for assessment

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 products



Downloading and Installing the SRA Tool

The tool can be downloaded from [HealthIT.gov](https://www.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.

The screenshot shows the HealthIT.gov website. The header includes the HealthIT.gov logo and navigation links for TOPICS, BLOG, NEWS, and DATA. The breadcrumb trail reads: HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool. The main content area is titled "Security Risk Assessment Tool" and includes a sidebar with a list of related topics such as Educational Videos, Security Risk Assessment Videos, Top 10 Myths of Security Risk Analysis, HIPAA Basics, Privacy & Security Resources & Tools, Model Privacy Notice (MPN), How APIs in Health Care can Support Access to Health Information: Learning Module, Patient Consent and Interoperability, and Your Mobile Device and Health Information Privacy and Security. The main text explains that 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. It also provides a section titled "What is the Security Risk Assessment Tool (SRA Tool)?" which states that the tool was developed by the Office of the National Coordinator for Health Information Technology (ONC) in collaboration with the HHS Office for Civil Rights (OCR). A "SRA Tool for Windows" section describes the tool as a desktop application that guides users through a security risk assessment process. At the bottom, there is a yellow button labeled "Download Version 3.3 of the SRA Tool for Windows [msi - 70.3 MB]".

Security Risk Assessment (SRA) Tool

Security Risk Assessment

Welcome!

practice assessment summary

Home
Practice Info
Assessment
Reports
Save
Save As
Logout

What is a Security Risk Assessment?

A security risk analysis is the foundation upon which to build security activities to protect electronic protected health information (ePHI). The SRA Tool will help you identify and assess risks to ePHI in your organization so that you can implement appropriate safeguards. When using this tool, please also review the SRA Tool User Guide and OCR's [Guidance on Risk Analysis](#) requirements under the HIPAA Security Rule

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.

Next >

Clinic and Practice Information

Security Risk Assessment

Practice Information

practice assessment summary

Home
Practice Info
Assets
Vendors
Documents
Assessment
Reports
Save
Save As
Logout

Add your [practice information](#) to your security risk assessment.
Consider all contexts of your organization's operations, such as various location(s), department(s), people, and more. Select '+ another location' if you have more than one location.

Practice Name	Indian Health Organization		
Address	7222 Main Avenue		
City, State, Zip	Riverside	CA	92760
Phone, Fax	989-232-3666	(xxx)-xxx-xxxx	
Point of Contact	Reese Weber		
Title/Role	Information Security Officer		
Phone	989-725-8999		
Email	Reese.Weber@IHO.com		

Delete Save this location

Add another location

< Back Next >

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

Security Risk Assessment

Practice Assets

Home

Practice Info

Assets

Vendors

Documents

Assessment

Reports

Save

Save As

Logout

Enter your organization's [assets](#).

Consider all contexts of assets, such as your organization's location(s), department(s), equipment, people, materials, and more.

Want to [add more than one asset](#) at a time?

Add Asset

Download Asset Template

Export Asset List

Upload Asset Template

Total Assets [0] Manage Multiple

Risk	Manage Assets	ID #	Type	Status	ePHI	Encryption	Assignment	Location
No content in table								

< Back | Next >

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

The screenshot displays the 'Practice Assets' section of the Security Risk Assessment (SRA) application. A modal window titled 'Add Asset' is open, allowing for the creation of a new asset. The form includes the following fields:

- Asset Type:** Servers
- Asset Status:** Active [In-use and...]
- ePHI Access:** Receives and tran...
- Disposal Status:** Not Disposed
- Disposal Date:** (empty field)
- Asset Encryption:** Full disk encryption
- Asset Assignment:** EHR Server
- Asset Location:** Server Room
- Asset ID:** 42-83839
- Comments:** under warranty until 8 October 2024

The background interface shows a navigation menu on the left with options like Home, Practice Info, Assets, Vendors, Documents, Assessment, Reports, Save, Save As, and Logout. The main content area contains instructions to enter organization assets and a table with columns for Risk, Location, and Name. At the bottom of the modal, there are 'Back' and 'Next' buttons.

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.

The screenshot displays the SRA Assessment interface. The top navigation bar includes the SRA logo, the title "Section 5: Security and the Practice", and icons for "practice", "assessment", and "summary". A left-hand navigation menu lists "Home", "Practice Info", "Assessment", and seven sections (Section 1 to Section 7), with progress indicators (checkmarks) for Sections 1 through 4. Below the menu are "Reports", "Save", "Save As", and "Logout" options. The main content area shows question Q3: "Do you restrict physical access to and use of your equipment [i.e. equipment that house ePHI]?". Four radio button options are provided: "Yes. We have written policies and implemented procedures restricting access to equipment that house ePHI to authorized users only." (selected), "Yes. We verbally authorize individuals to access equipment that house ePHI, but no written policies or procedures.", "No. We do not have a process to restrict access to equipment that house ePHI to authorized users.", and "Flag this question for later." To the right of the question are two panels: "Education" and "Reference". The Education panel contains text: "This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Restrict access to assets with potentially high impact in the event of compromise. This". The Reference panel lists citations: "HIPAA: §164.310(a)(1)", "NIST CSF: ID.RA, PR.AC, DE.CM, PR.IP", and "HICP: TV1, Practice # 6". Below the question is a "Details" section with a text box containing the instruction: "The details field can be expanded to collect relevant and supporting information about the question/response." At the bottom right are "Back" and "Next" navigation buttons.

Vulnerabilities and Threat Ratings

The screenshot displays the SRA assessment interface, divided into two main sections. The top section, titled "Section 5: Security and the Practice", prompts the user to "Select the vulnerabilities that apply to your practice from the list below." It features a list of seven vulnerabilities, each with a checkbox. The first, "Inadequate facility access management procedures where information systems reside", and the fifth, "Inadequate access controls for business associate and vendor access", are checked. The bottom section, also titled "Section 5: Security and the Practice", prompts the user to "Please rate the likelihood and impact on your practice of each potential threat." It displays a list of threats, each with a "Likelihood" and "Impact" rating scale. The first threat, "Unauthorized access to facility occurs undetected", has a Likelihood of L (Low) and an Impact of M (Medium). The second threat, "Workforce and visitors access critical or sensitive business areas without authorization", has a Likelihood of M (Medium) and an Impact of H (High). The third threat, "Increased response time to respond to facility security incidents", has a Likelihood of M (Medium) and an Impact of M (Medium). The fourth threat, "Inconsistency in granting access to facilities", has a Likelihood of L (Low) and an Impact of M (Medium). The fifth threat, "Inadequate access controls for business associate and vendor access", has a Likelihood of L (Low) and an Impact of M (Medium). The sixth threat, "Adversary leverages third party access to gain access to facility and devices", has a Likelihood of L (Low) and an Impact of M (Medium). The seventh threat, "Adversary leverages third party access to exfiltrate data or assets", has a Likelihood of M (Medium) and an Impact of H (High). The interface includes a navigation menu on the left with options for Home, Practice Info, Assessment, Reports, Save, Save As, and Logout. The top navigation bar includes icons for practice, assessment, and summary.

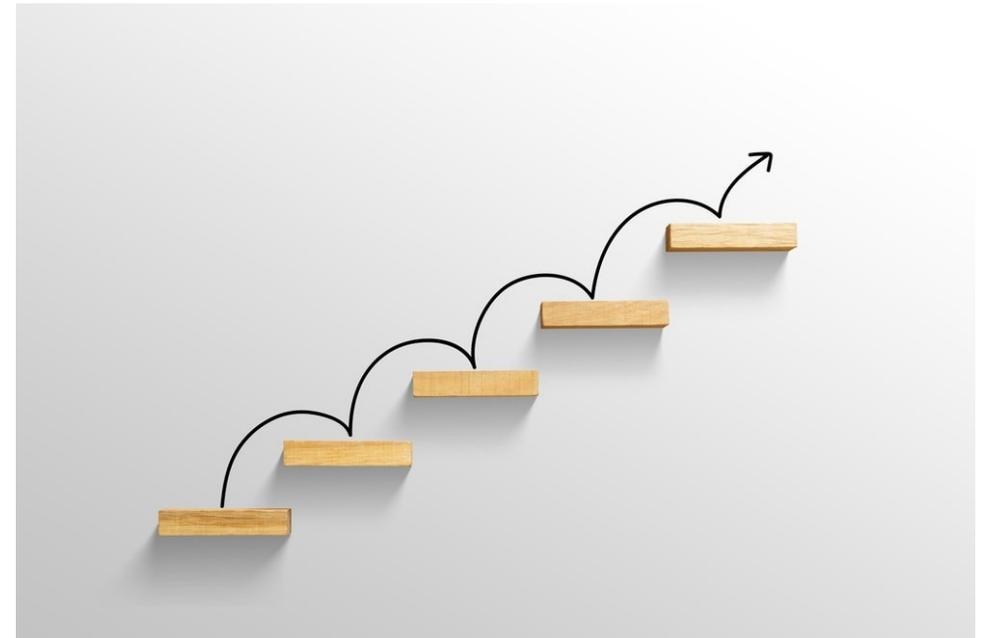
The Vulnerability Selection and Threat Rating section is presented after each section of multiple-choice questions.

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

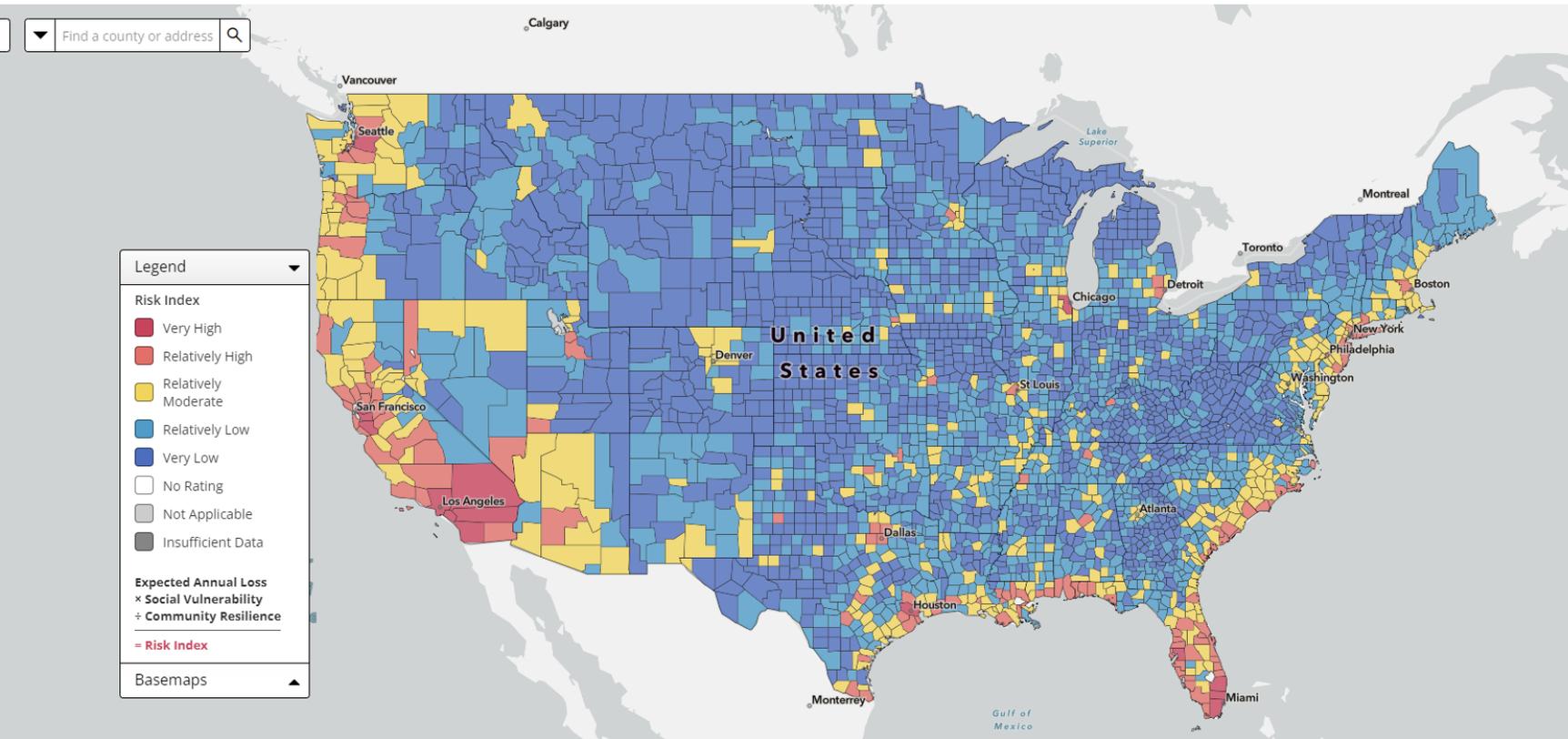
Each vulnerability comes with a list of related threats that must be rated for the **likelihood** they may occur and the **impact** they would have should they occur.

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



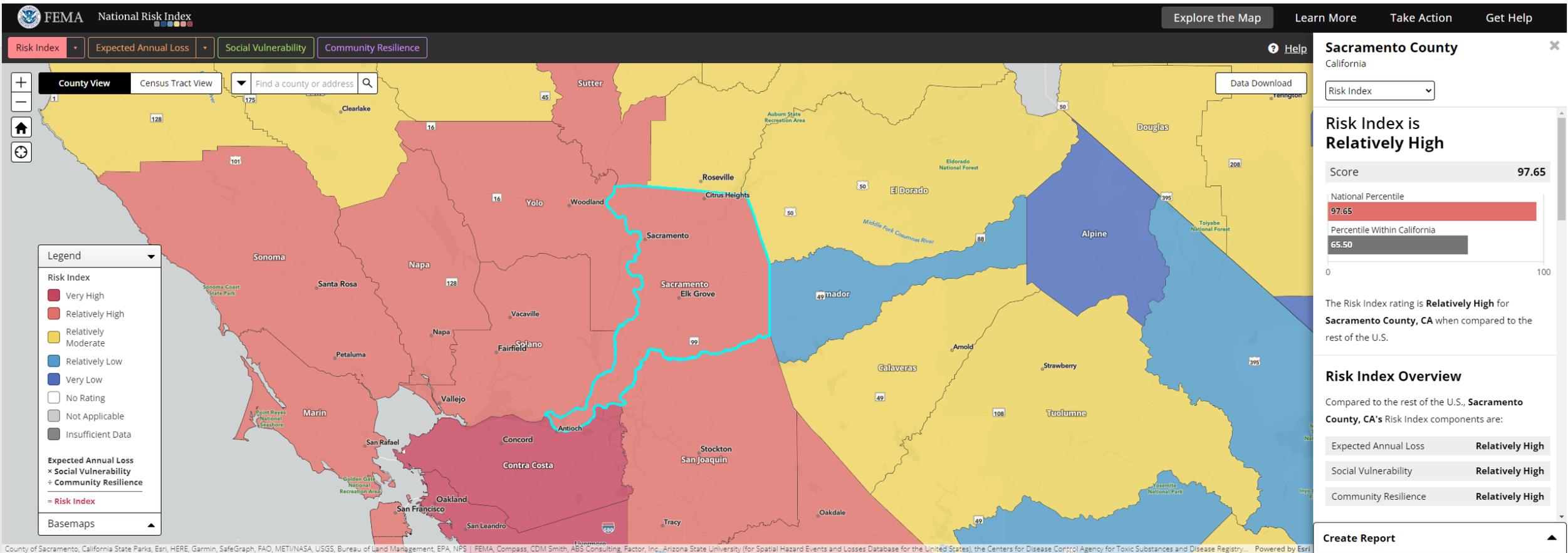
Determining Natural Risks to your Clinic



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**

National Percentile

97.65

Percentile Within California

65.50

0 100

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.

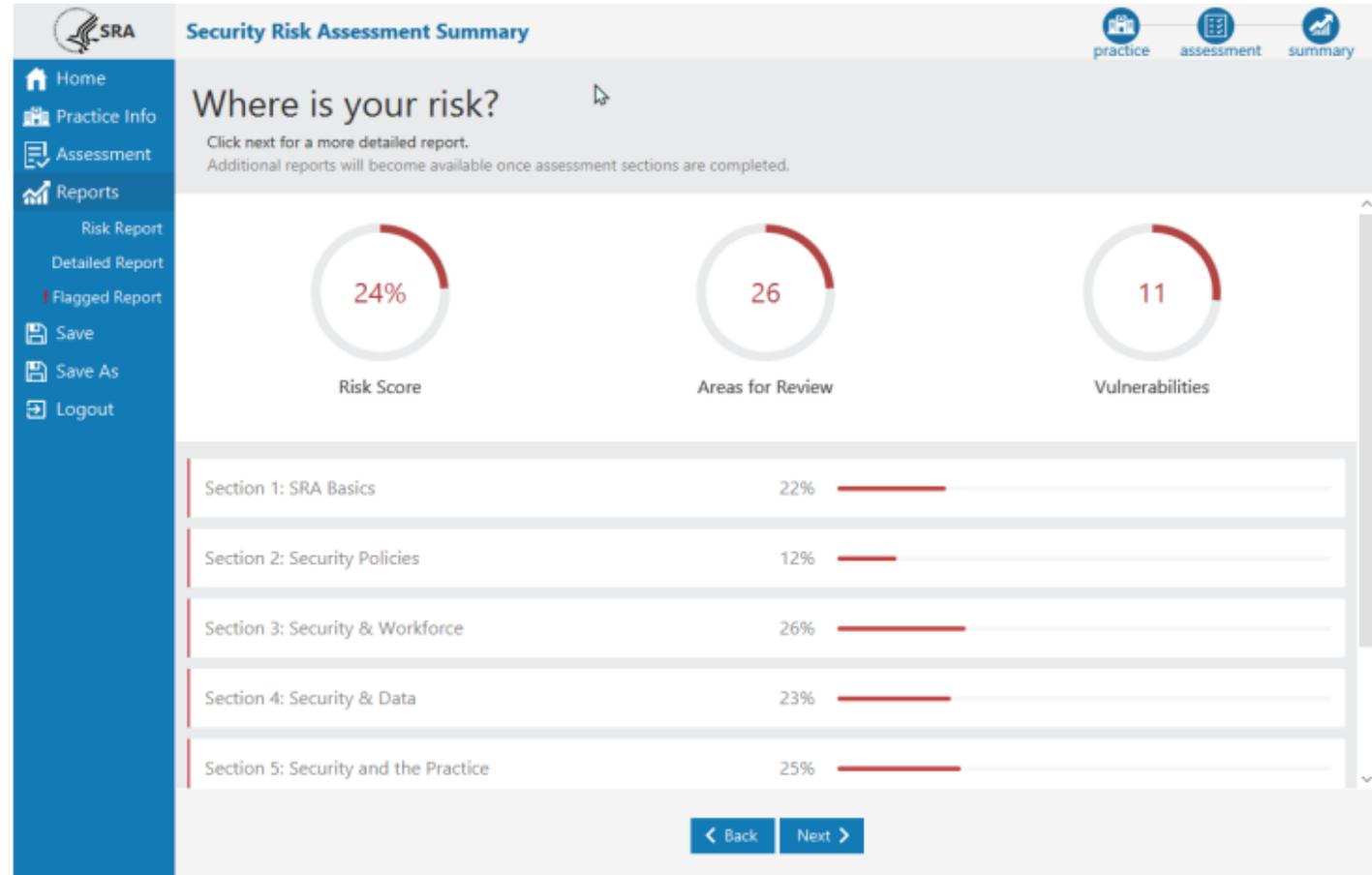
The Summary Report is high level summary of your risk assessment.

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 screenshot displays the Risk Report interface. On the left is a navigation menu with options: Home, Practice Info, Assessment, Reports (Risk Report, Detailed Report, Flagged Report), Save, Save As, and Logout. The main content area includes a header with the SRA logo and 'Risk Report' title, and navigation icons for practice, assessment, and summary. Below the header is a link to 'Understand your security risk assessment' and an 'Export' button. The 'Risk Breakdown' section features a pie chart with a legend showing 29 (green), 18 (yellow), 2 (red), and 4 (dark red). The 'Risk Assessment Rating Key' table is as follows:

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

The 'Vulnerabilities' section is expanded to show 'Section 1: SRA Basics Vulnerabilities & Threats'. It lists two vulnerabilities, both with a 'Low' risk level:

- Inadequate risk awareness or failure to identify new weaknesses
Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches. Risk level: Low.
- Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.). Risk level: Low.

At the bottom of the main content area are 'Back' and 'Next' navigation buttons.

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.

SRA Detailed Report

Click each section to expand and review more details.

- Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof, sprinkler activation), unstable building conditions **Low**
- Failure to meet minimum regulatory requirements and security standards
- Corrective enforcement from regulatory agencies (e.g. HHS, OCR, FTC, CMS, State or Local jurisdictions) **Low**
- Damage to public reputation due to breach **Medium**
- Failure to attain incentives or optimize value-based reimbursement **Low**
- Litigation from breach victims due to lack of reasonable and appropriate safeguards **Low**

Question	Answer	Education	References	Compliance Guidance/Rule	Username	Date/Time
Q1. Has your practice completed a security risk assessment (SRA) before?	Yes.	Continuing to complete security risk assessments will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR.IP, RS.MI HICP: TV1, Practice # 7, 10	Required	Ryan	Fri Mar 04 12:57:50 EST 2022

< Back Next >

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



