Security Risk Analysis

Presented by:

Linda Castranova Feldman- Value Based Care Account Manager
Maggie Black-Value Based Care Account Manager

Host: Sharon Hart, Senior Manager, Transformation and Quality

May 2025

McKESSON

The information and documentation provided in this webinar is for educational and informational purposes only and is not intended as nor should be construed as legal advice or as a substitute for the original source documents.

Users should consult the original source documents and other guidance published by CMS. Users are solely responsible for understanding and satisfying all requisite conditions of the applicable incentive program, and McKesson makes no warranty or representation as to the accuracy of the information contained herein or that users will qualify for any incentive.

The statements contained in this document are solely those of the authors and do not necessarily reflect the views or policies of CMS. The authors assume responsibility for the accuracy and completeness of the information contained in this document

Agenda


Overview
Safeguards
Security Risk Assessment
SAFER Guides
Key Takeaways

Avoid Becoming Another Breach Headline!

[Duncan Regional Hospital Data Breach Impacts 92K]

[South Denver Cardiology Associates Confirms Data Breach Affecting 287,000 Patients]

[Sea Mar Community Health Centers Facing Class Action Lawsuit over 688,000-Record Data Breach]

[Ransomware Gangs Claim Health Plan and Healthcare Provider Attacked]

[Spokane Regional Health District Announces Second Phishing Attack in 3 Months]

[CSI Laboratories and Christie Clinic Report Data Breaches; Scripps Health Sends Additional Notification Letters]

MCKESSON

Protect Health Information

Security Rule:

- Sets standards ensuring only those who **should** have access to ePHI have access

Security Risk Assessment:

- Covers all PHI and ePHI
- Includes ePHI/PHI that is created, received, maintained and transmitted

Privacy Rule:

- Sets standards for who may have access
- Applies to all forms of PHI- oral, paper and electronic

PHI= Protected Health Information

ePHI= Electronic Protected Health Information

Overview: What is A Security Risk Analysis (SRA)?

Assists the organization in ensuring compliance with HIPAA's administrative, physical and technical safeguards

Helps reveal areas where protected heath information (PHI) could be at risk

Who does an SRA affect?

Security Official
Privacy Official
IT Coordinator
All Practice Staff

Top 10 Myths of Security Risk Analysis

- The security risk analysis is optional for small providers.
- Simply installing a certified EHR fulfills the security risk analysis requirement.
- My EHR vendor took care of everything I need to do about privacy and security.
- I must outsource the security risk analysis.
- A checklist will suffice for the risk analysis requirement.
- There is a specific risk analysis method that I must follow.
- My security risk analysis only needs to look at my EHR.
- I only need to do a risk analysis once.
- Before I attest for an EHR incentive program, I must fully mitigate all risk.
- Each year, I'll have to completely redo my security risk analysis.

Why Perform a Security Risk Analysis?

- Protect Patient Information
- Protect Practice Information and Operations
- Required for MIPS- Audit Preparation
- Required for Covered Entities under HIPAA regulations
- **COVID-19 work environment and workflow shifts**

Protect Patient Health Information

2025 Measure Specifications:

Merit-Based Incentive Payment System (MIPS)

Promoting Interoperability Performance Category Measure

2025 Performance Period

Objective:	**Protect Patient Health Information**
Measure:	**Security Risk Analysis** Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.
Measure ID:	**PI_PPHI_1**

Definition of Terms

N/A

Reporting Requirements

YES/NO

To meet this measure, MIPS eligible clinicians must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies.

Security Risk Analysis: MIPS Promoting Interoperability

- Promoting Interoperability category requirement although not scored
- For your promoting interoperability score to count clinicians **must** attest yes to:
  - Conducting/Reviewing a security risk analysis
  - Implementing Security updates as necessary
  - Correcting identified security deficiencies

- The SRA must be completed during the reporting year January 1, 2025 - December 31, 2025.
  - Suggest aim to complete no later than October 31, 2025

- **NO EXCLUSIONS**

MCKESSON

Safeguards

Administrative Safeguards

What are they?

Administrative actions and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information (ePHI) and to manage the conduct of the covered entities workforce in the relation to the protection of the information

Examples

- Staff Training
- Security Awareness
- Written Policies/Procedures
- Incident Response Plans
- Policy enforcement

Assessment Questions

Does your practices awareness and training content include information about the importance of implementing software patches and updating antivirus software when requested?

Does you practice include password management as part of its awareness and training programs?

Administrative Safeguards

Workforce Security Information Access Management

Implement policies and procedures to:

- Ensure staff have appropriate levels of access
- Prevent access from those who do not need it

Access based on job function:
What is needed, when it is needed and **only** what is needed
Minimum necessary!

Termination process:
Ensure access privileges are removed when an employee is terminated or job role changes

Physical Safeguards

What are they?

Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Standards of Physical Safeguards Include:

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Examples

- Locked Doors
- Security Cameras
- Clean Desk Policy
- ID Badges (Employees/Visitors)
- Screens Shielded from Secondary Viewers

Assessment Questions

Do you have an inventory of the physical systems, devices and media in your office space that are used to store or contain ePHI?

Do you have procedures to create, maintain and keep a log of who accesses your facilities (including visitors), when the access occurred and the reason for the access?

Technical Safeguards

What are they?

The technology and the policy and procedures for its use that protect electronic protected health information and control access to it

1. Access Control
2. Audit Controls
3. Integrity
4. Authentication
5. Transmission Security

Examples

- Tracked unique user IDs
- Automatic logoff due to inactivity
- Data Encryption for Telehealth Platforms
- Backing-up data
- Virus Checks

Assessment Questions

Does your practice have backup information systems so that it can access ePHI in the event of an emergency when your practices primary systems become unavailable?

Does your practice have the capability to activate emergency access to its information systems in the event of a disaster?

Helpful Resources

HealthIT.gov

SRA Tool for Windows

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. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's computer. HHS does not collect, view, store, or transmit any information entered into the SRA Tool.

Download Version 3.3 of the SRA Tool for Windows [.msi - 70.3 MB]

SRA Tool Excel Workbook New!

This version of the SRA Tool takes the same content from the Windows desktop application and presents it in a familiar spreadsheet format. The Excel Workbook contains conditional formatting and formulas to calculate and help identify risk in a similar fashion to the SRA Tool application. This version of the SRA Tool is intended to replace the legacy "Paper Version" and may be a good option for users who do not have access to Microsoft Windows or otherwise need more flexibility than is provided by the SRA Tool for Windows.

This workbook can be used on any computer using Microsoft Excel or another program capable of handling .xlsx files. Some features and formatting may only work in Excel.

Download Version 3.3 of the SRA Tool Excel Workbook [.xlsx - 128 KB]

Need help?

SRA Webinars

ONC held 3 webinars with a training session and overview of the Security Risk Assessment (SRA) Tool. The slides for these sessions are posted below and a recording of the webinar is also available.

SRA Tool User Guide

Download the SRA Tool User Guide for FAQs and details on how to install and use the SRA Tool application and SRA Tool Excel Workbook.

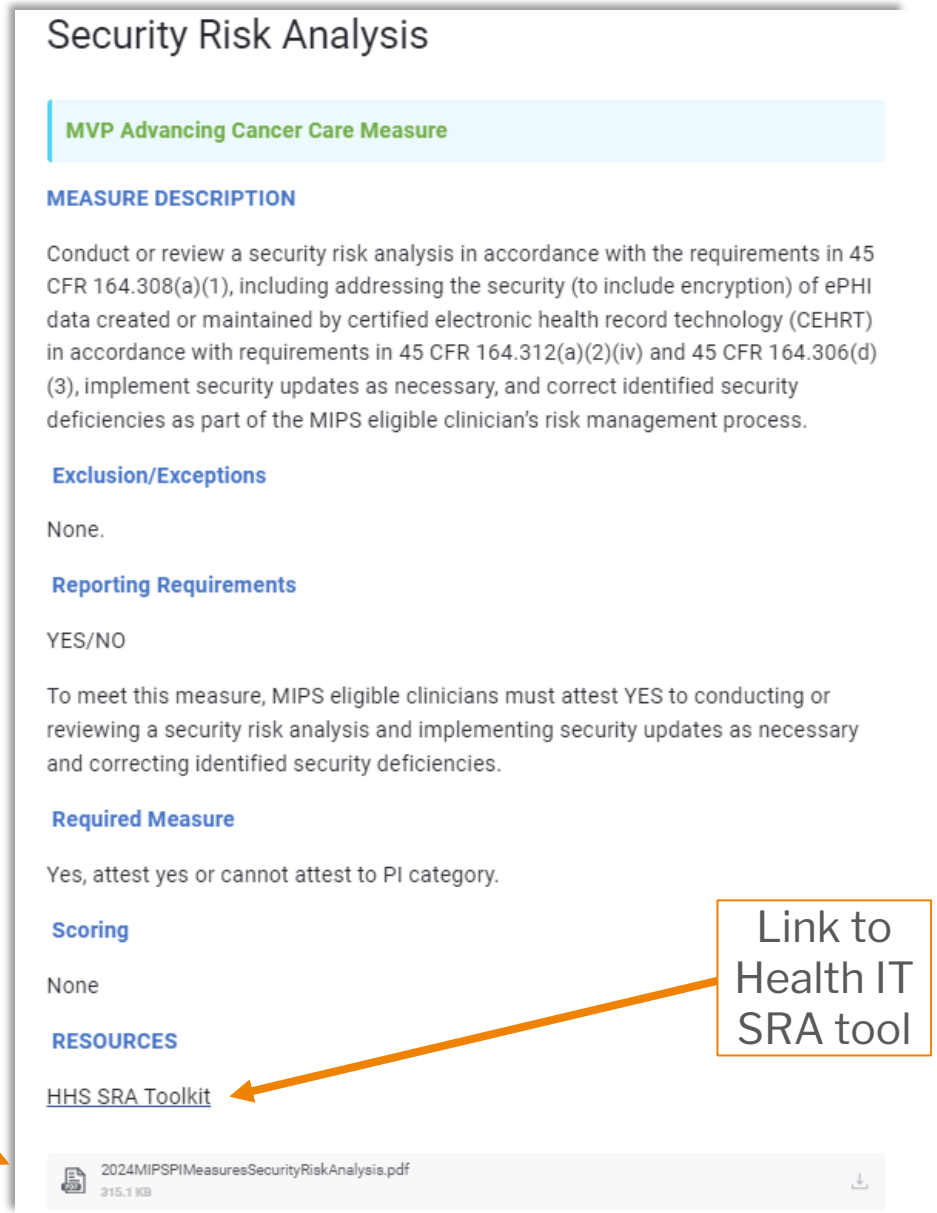
Download SRA Tool User Guide [.pdf - 6.4 MB].

MCKESSON

HHS.gov: Health Information Privacy

Health Information Privacy

QPP Resource Guide—Protect Health Information



Security Risk Analysis

MVP Advancing Cancer Care Measure

MEASURE DESCRIPTION

Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.

Exclusion/Exceptions

None.

Reporting Requirements

YES/NO

To meet this measure, MIPS eligible clinicians must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies.

Required Measure

Yes, attest yes or cannot attest to PI category.

Scoring

None

RESOURCES

HHS SRA Toolkit

2024MIPSPIMeasuresSecurityRiskAnalysis.pdf
315.1 KB

Link to CMS 2025 Measure Specification sheet

Link to Health IT SRA tool

McKESSON

Conducting a Security Risk Assessment

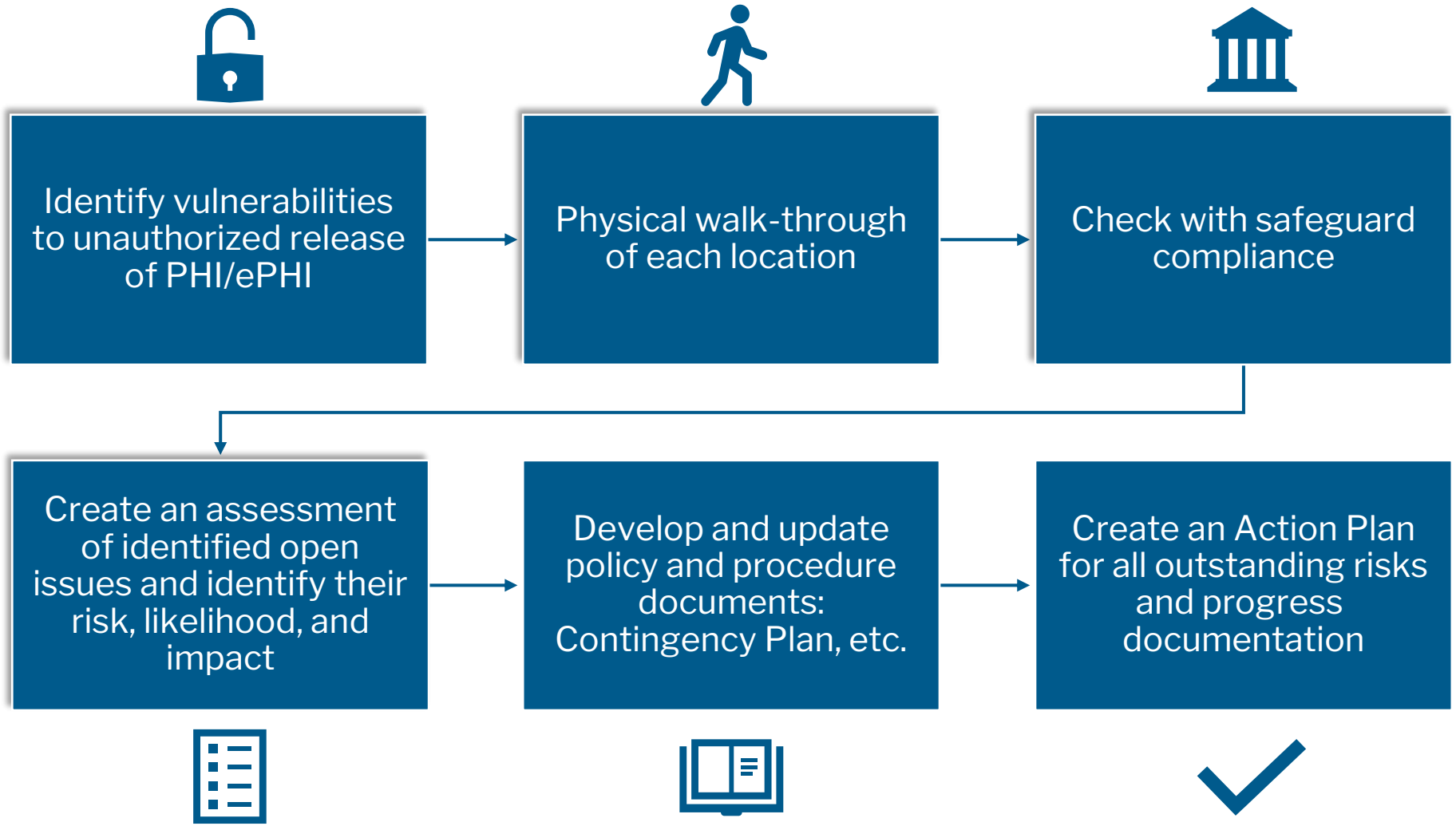
Security Risk Assessment

- Reduce risks and vulnerabilities to a reasonable and appropriate level
- Preparation for emergencies/disasters/breech
  - Contingency plan

- All PHI and ePHI that the practice creates, receives, maintains or transmits

SRA Process Flow

Ongoing Process



Security Risk Assessment—Policies & Procedures

Review policies and procedures	*Written policies for HIPAA compliance*
	Security policies
	Business Associate Agreements
	Written protocols for EHR access
	Record retention policy
	Plan for identifying and managing vendors
	Contingency plan

Sample list only

Example of Policy: Contingency Plan/Disaster Plan

WHY?

To continue to provide care/be accessible for patients and community needs

WHAT IF?

- Critical staff unavailable or cannot be contacted
- Vendors or supplies unavailable
- Facility or hospital unavailable
- Equipment is not working at the Health Center
- Software is ruined or not working due to hardware issues
- Critical data and records are unavailable or destroyed
- Utilities are down

EXAMPLES:

- How are you handling staff shortages?
- PPE shortage?
- Patient exposure?
- How have you continued to care for patients?

Use your experience to help you in developing your Disaster Recovery Plan

Who Completes the SRA?

Can complete internally, if company is small to medium size

- HHS tool—free
  - A practice-wide activity
  - Administrative and Physical components: Practice Administrator, Clinical Supervisor, EMR Manager, Front Desk Staff, Medical Records
  - Technical component: IT Technician (if available)

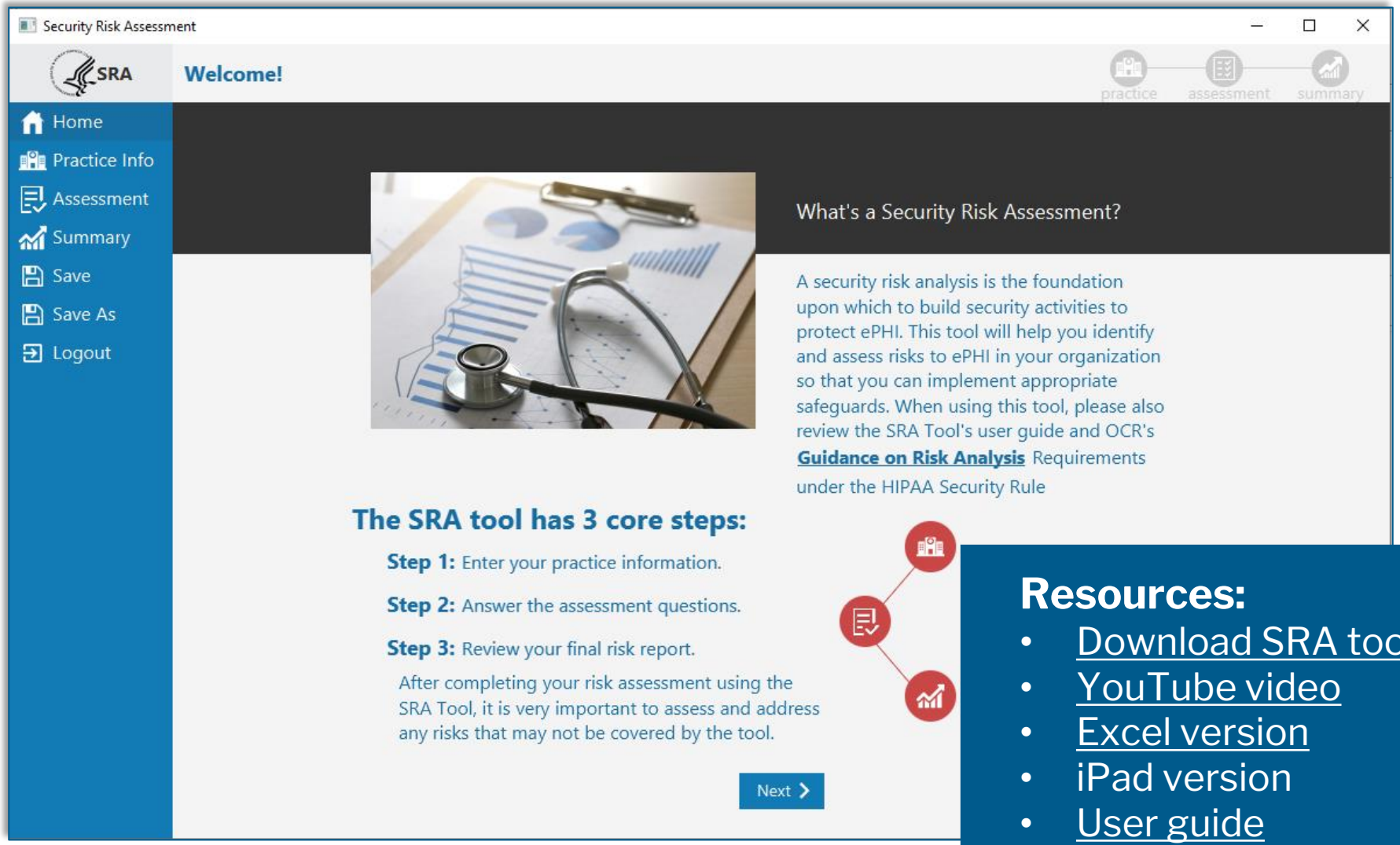
Hire outside company

- Often Technical portion only
  - Some IT companies will only offer a security scan, best practice but not required for SRA
  - Practice may be responsible for the Administrative and Physical safeguards
- Practice responsible for review, authentication, and action plan

McKESSON

HHS – Security Risk Assessment Tool

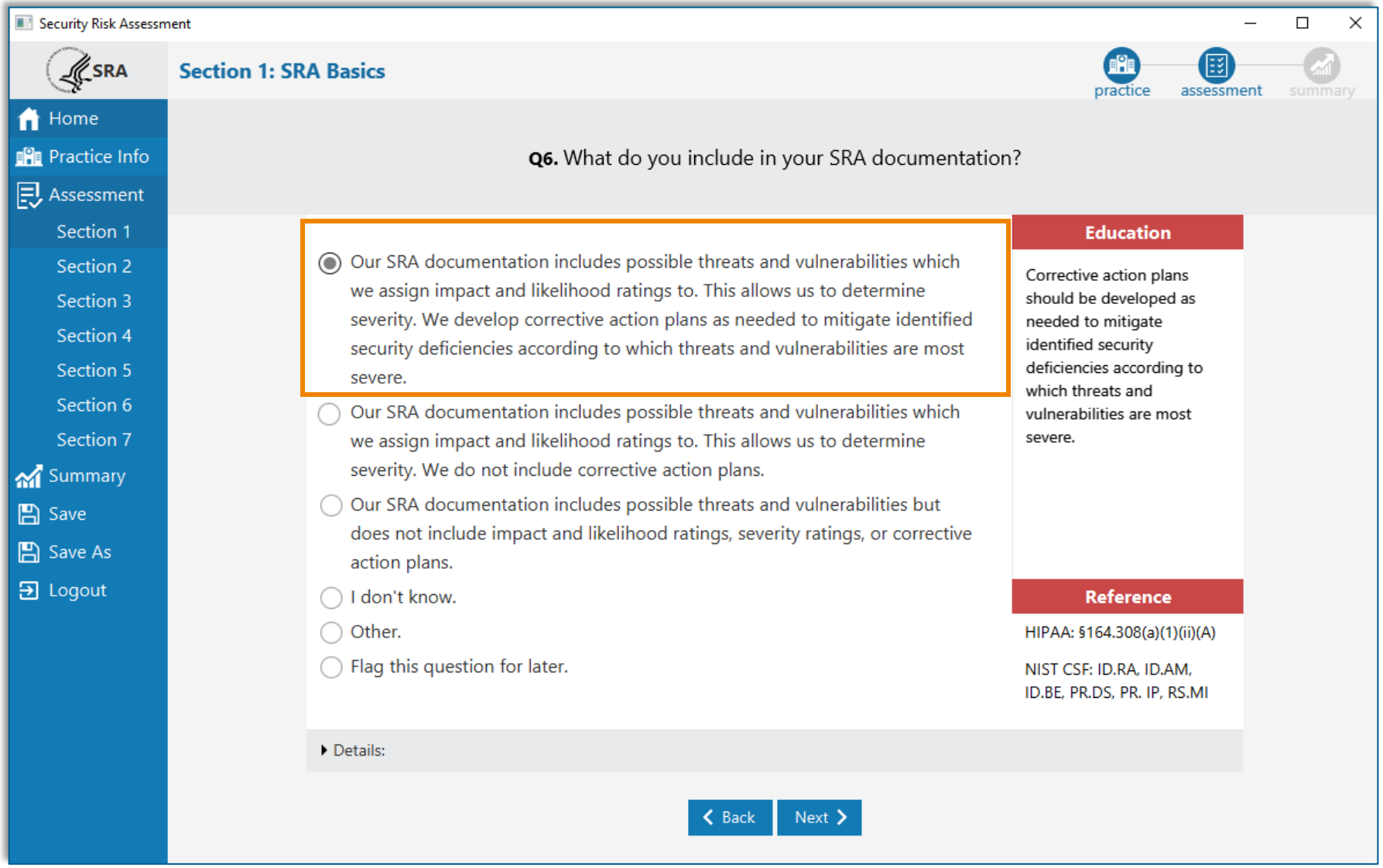
HHS – Security Risk Assessment Tool



Resources:

- Download SRA tool
- YouTube video
- Excel version
- iPad version
- User guide

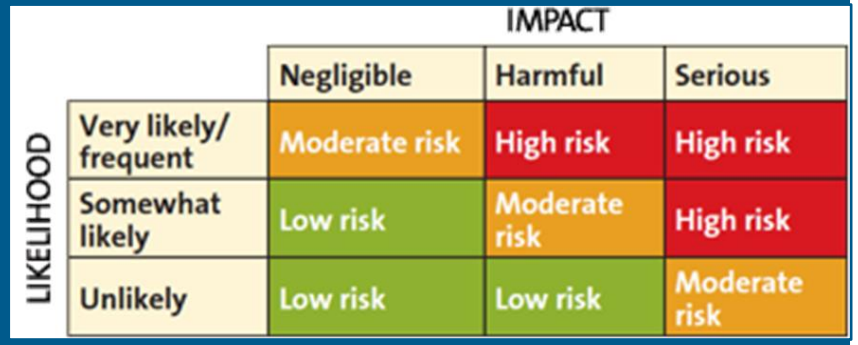
HHS – Security Risk Assessment Tool



MCKESSON

Identify Level of Risk

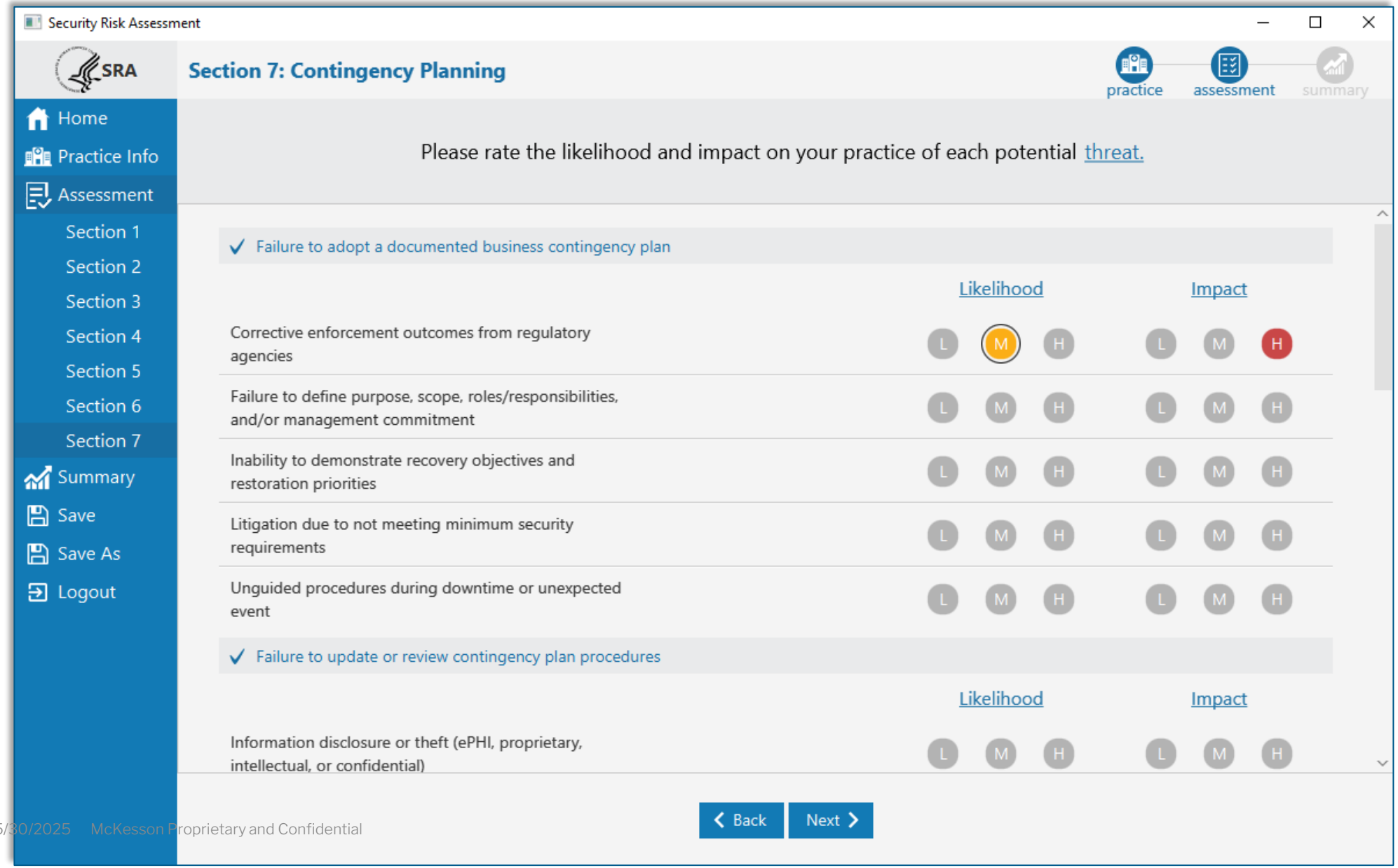
- **Likelihood of occurrence**
  - Examples: Weather, hacker, rogue or disgruntled employee
- **Impact on practice**
  - Examples: Financial cost of response; damage to reputation; impact on providing ongoing patient care



LIKELIHOOD	IMPACT: Negligible	IMPACT: Harmful	IMPACT: Serious
Very likely/ frequent	Moderate risk	High risk	High risk
Somewhat likely	Low risk	Moderate risk	High risk
Unlikely	Low risk	Low risk	Moderate risk

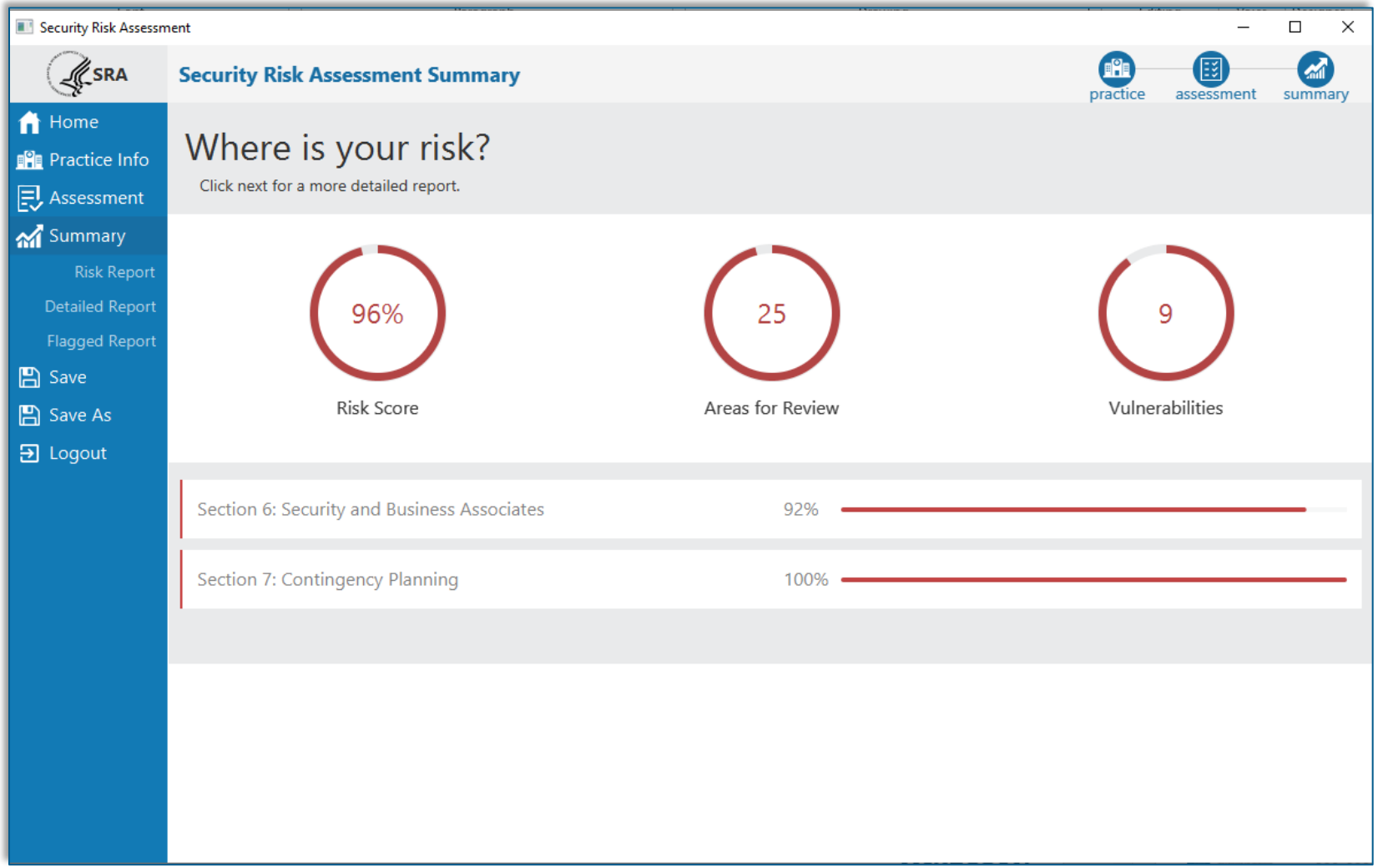
Example only

Likelihood and Impact Risk Assessment



MCKESSON

Areas of Risk



MCKESSON

Corrective Action Plan

ID	Citation	Answer	Flagged	Risk Level	Current Activities	Notes	Remediation	Reason	Last Edit
A01	§164.308(a)(1)(i)	Yes		Low	Policies and Procedures developed by Practice Manager and viewed annually			N/A	[TG]6/6/2017 10:01:07 am
A02	§164.308(a)(1)(i)	Yes		Low	Reviewed annually			N/A	[TG]6/6/2017 10:01:30 am
A04	§164.308(a)(1)(ii)(A)	No	✓	Medium				N/A	[TG]6/13/2017 6:37:08 pm
A05	§164.308(a)(1)(ii)(B)	Yes		Low	Bi-annual review o				[TG]6/13/2017 6:37:18 pm
A07	§164.308(a)(1)(ii)(B)	Yes		Low	Corrective Action Meeting				[TG]6/13/2017 6:41:18 pm
A08	§164.308(a)(1)(ii)(B)	Yes			All procedures do				[TG]6/13/2017 6:40:53 pm
A14	§164.308(a)(2)	Yes		Low	Security Officials a				[TG]6/13/2017 6:40:21 pm
A57	§164.308(a)(8)	Yes		Low	Annual risk Assessment			N/A	[TG]6/13/2017 6:39:54 pm
A58	§164.308(a)(8)	Yes		Low	Site assessments every 6 months			N/A	[TG]6/13/2017 6:39:19 pm
A59	§164.308(a)(8)	Yes		Low	Security Official			N/A	[TG]6/13/2017 6:38:57 pm

Export as Excel document to create the Corrective Action Plan for your Practice

SAFER Guides

SAFER Guides

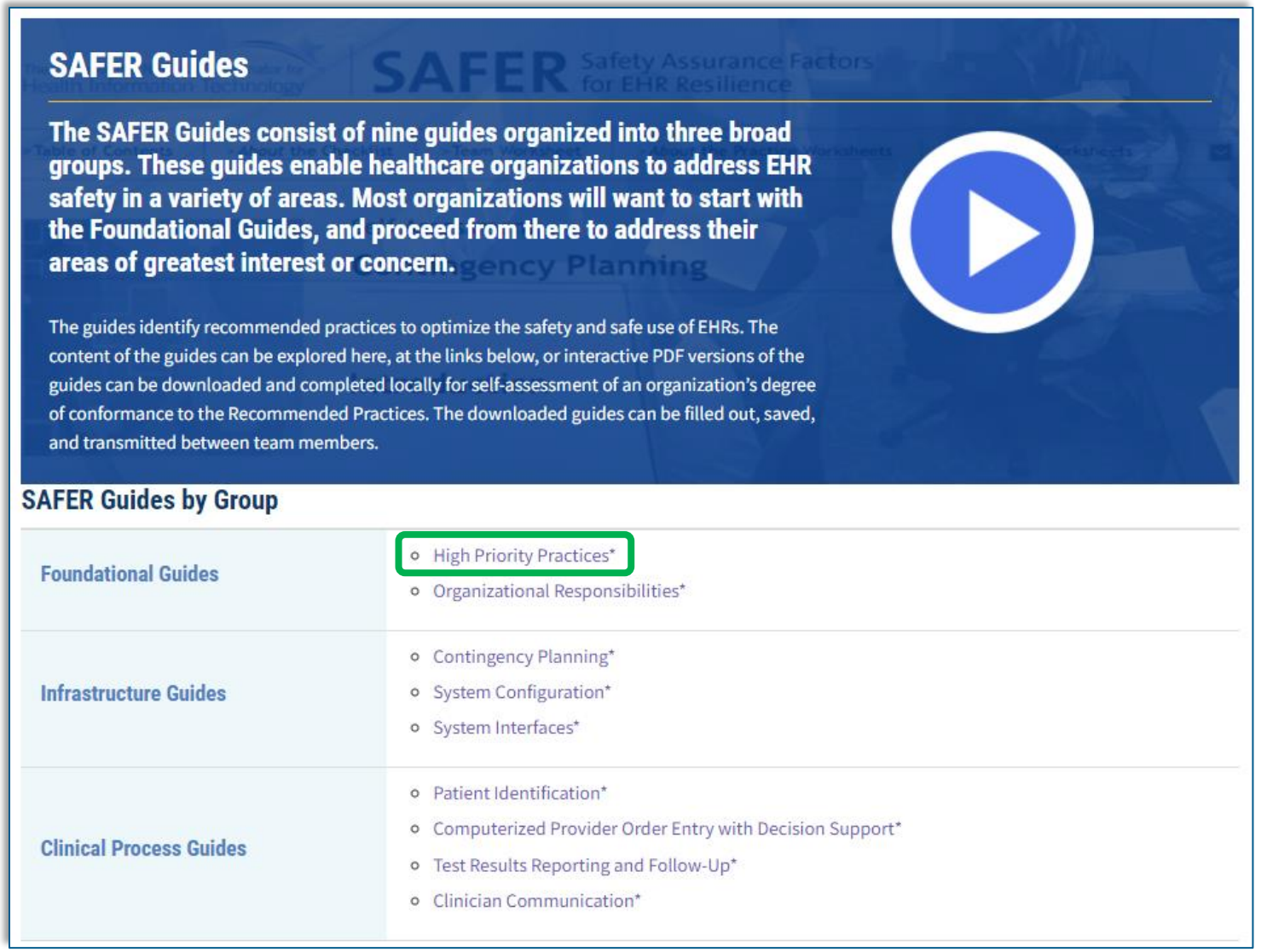
- SAFER Guides are designed to help healthcare organizations conduct self-assessments to optimize safety & safe use of EHRs

- ***Promoting Interoperability requires High Priority Guide for reporting***
  - Yes attestation, no points but required
  - Keep completed guide for 6 years in case of audit
- Complete anytime during the 2025 calendar year

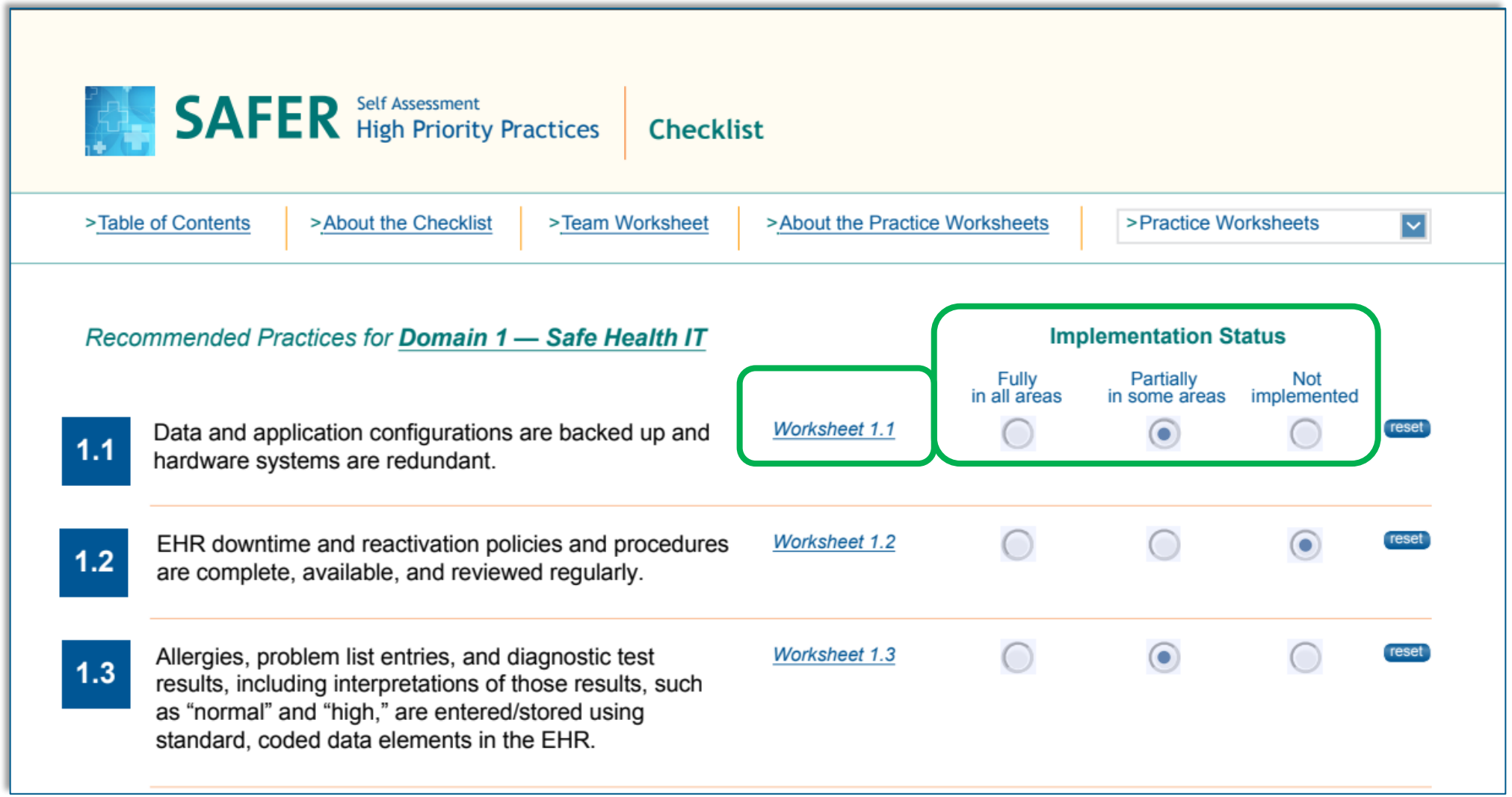
- Team approach- may need input from EHR to complete

- Workbook, checklists and guides available on healthIT.gov

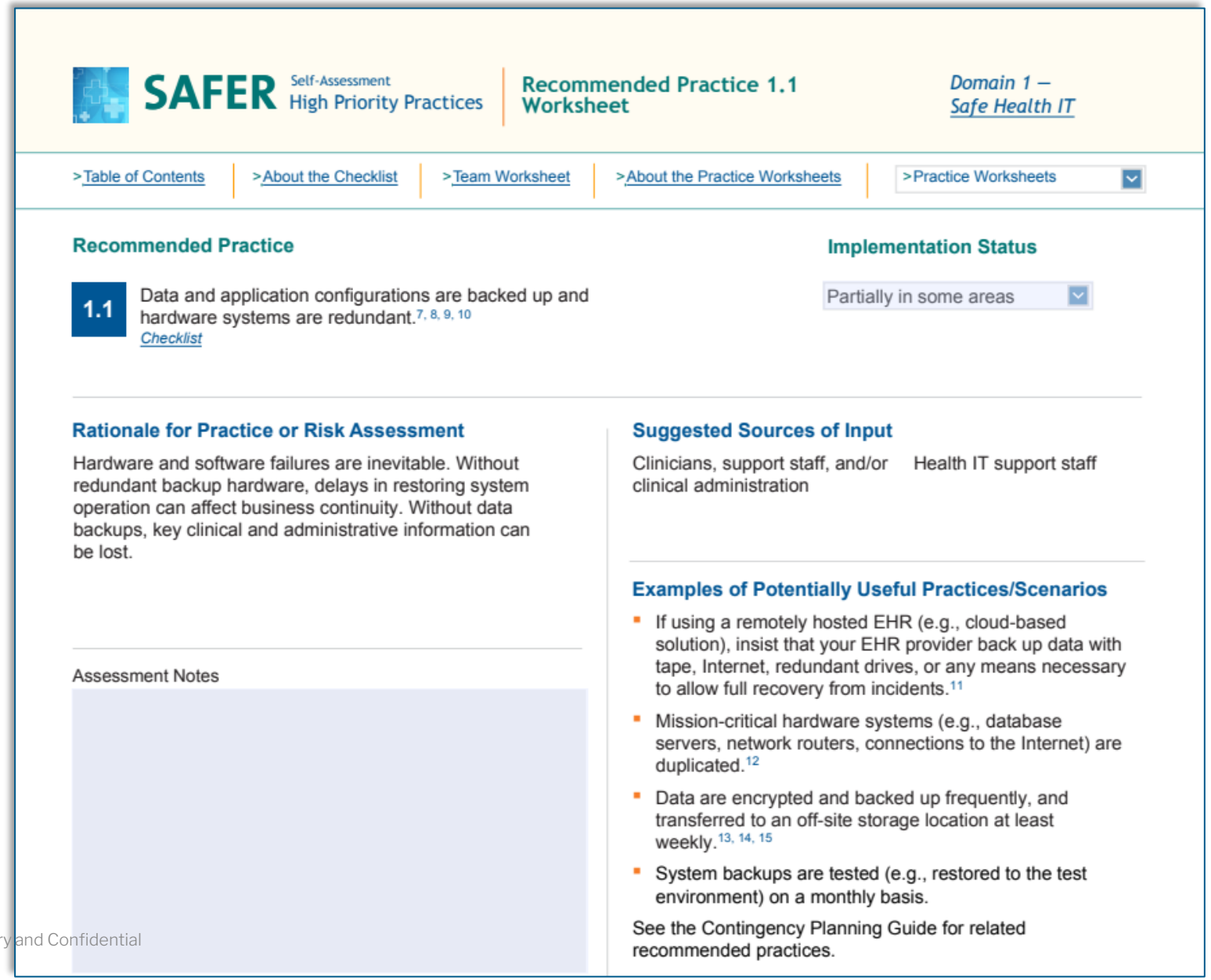
SAFER Guides—High Priority Practices



SAFER Guides--Questionnaires



SAFER Guides--Worksheet



SAFER Self-Assessment High Priority Practices | Recommended Practice 1.1 Worksheet | Domain 1 – Safe Health IT

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

Recommended Practice

1.1 Data and application configurations are backed up and hardware systems are redundant.[7, 8, 9, 10]
Checklist

Implementation Status

Partially in some areas

Rationale for Practice or Risk Assessment

Hardware and software failures are inevitable. Without redundant backup hardware, delays in restoring system operation can affect business continuity. Without data backups, key clinical and administrative information can be lost.

Assessment Notes

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- If using a remotely hosted EHR (e.g., cloud-based solution), insist that your EHR provider back up data with tape, Internet, redundant drives, or any means necessary to allow full recovery from incidents.[11]
- Mission-critical hardware systems (e.g., database servers, network routers, connections to the Internet) are duplicated.[12]
- Data are encrypted and backed up frequently, and transferred to an off-site storage location at least weekly.[13, 14, 15]
- System backups are tested (e.g., restored to the test environment) on a monthly basis.

See the Contingency Planning Guide for related recommended practices.

Key Takeaways

Who Needs a Security Risk Assessment?

Any practice that is a “Covered Entity”

- Providers who conduct HIPAA transactions, like electronic claims, are considered a Covered Entity
- Even if not submitting MIPS, APM, or EOM data, Covered Entities must complete or update an SRA annually

Full Risk Assessment

- Risks identified, documented, reviewed and risk rated
- An Action Plan created and kept up to date—living document
  - Who
  - When

Corrective Action Plan

2024 Action Plan for Northeastern XYZ

Date: _____

Based on the Risk Analysis Report by Susan Sloan

Recommendations [Suggested corrective actions or controls]	Estimated Resources [Time (duration) and Costs (investment)]	Action Plan			Comments/Progress
		Assigned to:	Start Date:	Finish Date:	
Ensure encryption is used to protect data stored on the internal hard drive of laptops and high-risk workstations.	Cost of software and installation	Barbara Smith	3/1/25		
Utilize privacy screens and/or password protected screensavers to prevent incidental disclosure of PHI in public areas.	$30-50 for each screen or 10 mins with IT vendor	Doug Jones	2/1/25	5/1/25	Bought privacy screens, installed on all patient facing monitors. 2/1/25
Conduct a self-assessment questionnaire (SAQ) of PCI DSS Compliance	1 hour	Pete Smith	1/15/25		Started 2/1/25 ., in progress.
Conduct annual mandatory staff training on HIPAA and Security Breach Policy	2 hours for prep, 1 hour for training staff	Doug Jones	2/1/25		Scheduled during in-service day 4/1/2024.

Example only

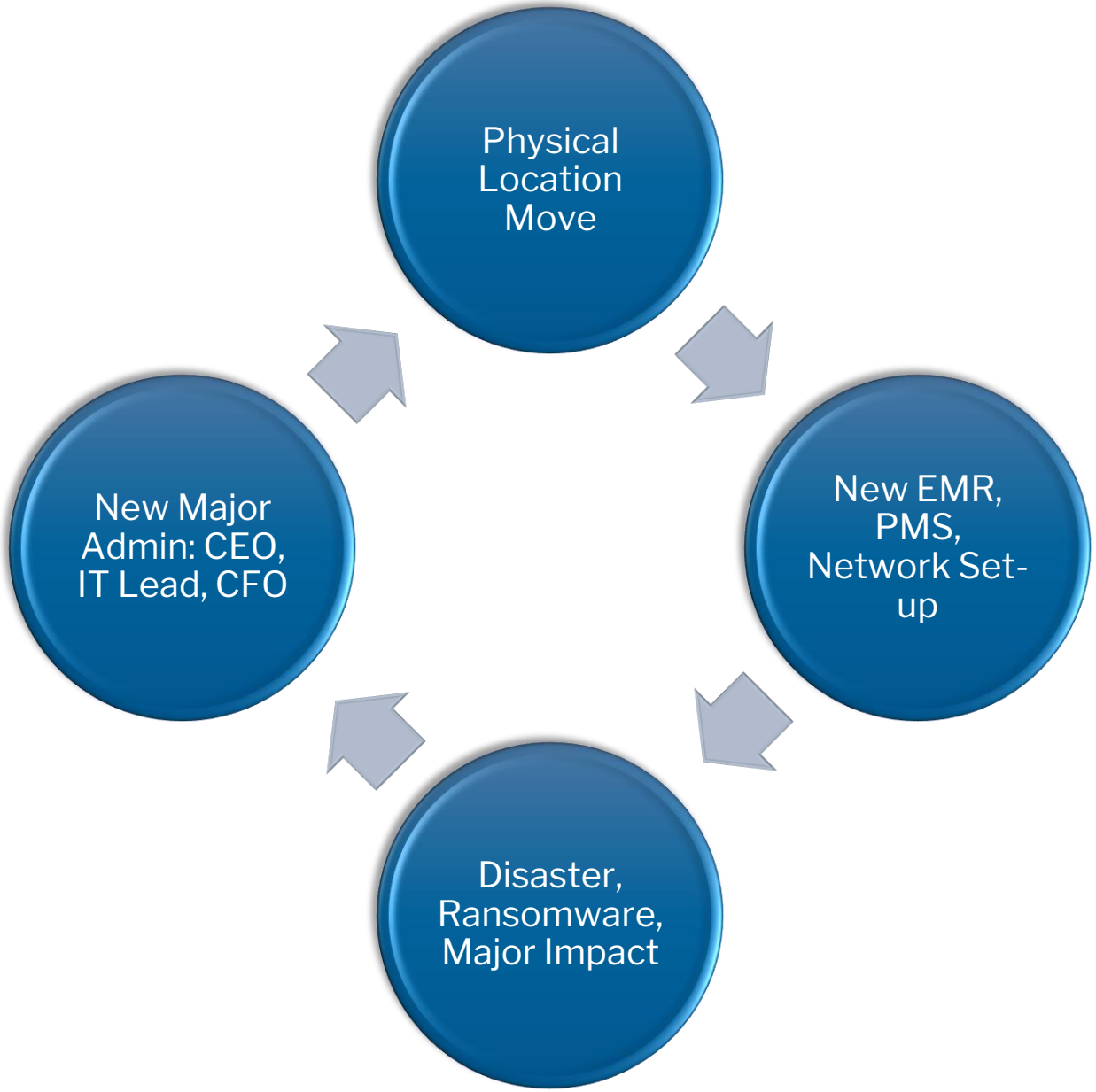
Do You Need to *Redo* a Full Risk Assessment?

If <u>all</u> of these are accurate, then:

1. Revisit & thoroughly review previous year's assessment
2. Complete a new yearly physical walk-through & document
3. Update Action Plan with new findings & updates

Have Any Changes Occurred Since Last SRA?

If one or more occurred, suggest completing a full risk assessment and action plan.



Full Risk Assessment

Revise or Create New Policies and Procedures

Review past assessments

Conduct full assessment for 3 Safeguards

Complete physical walk-throughs of all locations that contain PHI/ePHI

Create new Corrective Action Plan

- *Written policies for HIPAA compliance*
- *Security policies*
- *Business Associate Agreements*
- *Written protocols for EHR access*
- *Record retention policy*
- *Plan for identifying and managing vendors*
- *Contingency plan*

Sample list only

Future Plans

No Changes?

- Review original assessment, complete a walk- through, update Action Plan including any outstanding risks, old and new

3 years

- Plan to conduct a full, new Risk Assessment every 3 years, regardless of changes

Monitor & Update

- Update and review Action Plan during the year
- Send reminders to staff on policies and issues
- Keep for at least 6 years in case of audit

PRO TIP:

- Easier to document as things happen, rather than remember at year end.
- Remind staff of issues when noticed.

Questions?

We’re here to help
AdvisoryServices@McKesson.com
or
QPP.info@McKesson.com