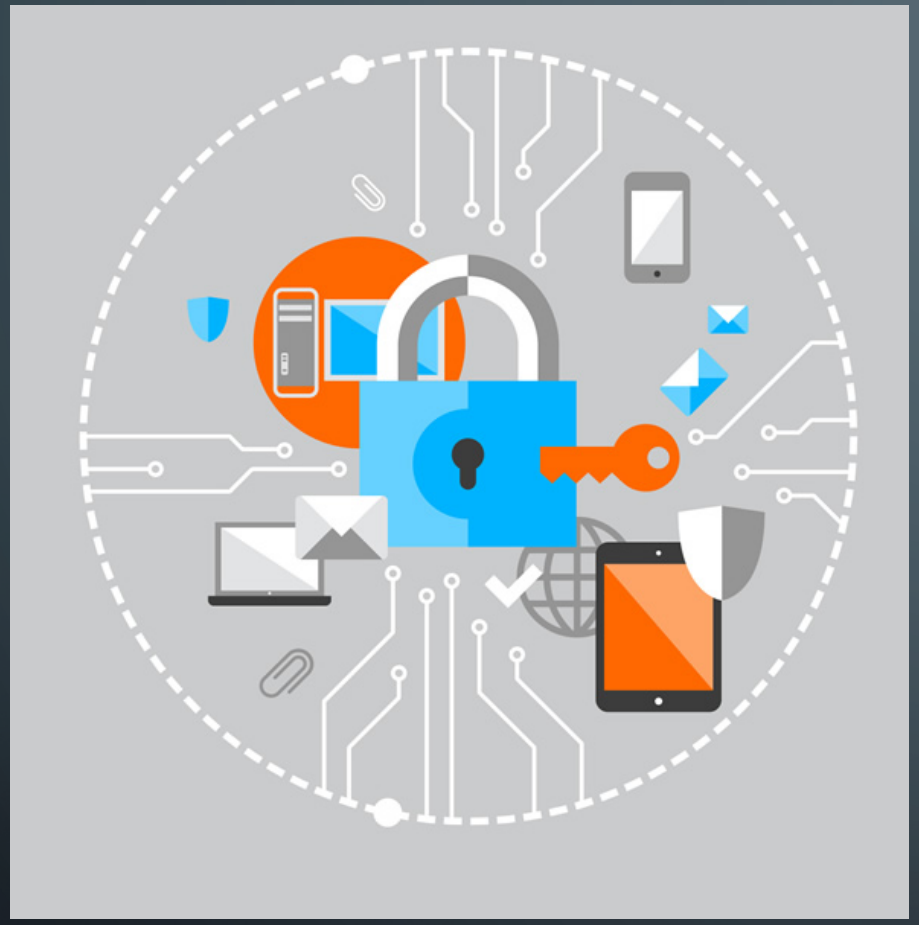


IMPROVING HEALTH CENTER CYBERSECURITY

Health Center Security Risk Assessment & Cybersecurity Defense

PRESENTED IN PARTNERSHIP WITH MPCA AND THE HITEQ CENTER OCTOBER 8TH, 2020

Maine Primary Care Association

HEALTH INFORMATION TECHNOLOGY, EVALUATION, AND QUALITY CENTER
HITEQ

Housekeeping

HITEQ CENTER

The HITEQ Center is a HRSA-funded Cooperative Agreement that collaborates with HRSA partners to support health centers in full optimization of their EHR/Health IT systems

HITEQ

HEALTH INFORMATION TECHNOLOGY, EVALUATION AND QUALITY CENTER

hiteqcenter.org

The HITEQ Center is a HRSA-funded National Cooperative Agreement that collaborates with HRSA partners including Health Center Controlled Networks, Primary Care Associations and other National Cooperative Agreements to support health centers in full optimization of their EHR/Health IT systems.

HITEQ identifies and disseminates resources for using health information technology (IT) to improve quality and health outcomes. HITEQ includes:

- A searchable **web-based health IT knowledgebase** with resources, toolkits, training, and a calendar of related events
- **Workshops and webinars** on health IT and QI topics
- **Technical assistance** and responsive teams of experts to work with health centers on specific challenges or needs

Contact HITEQ for training or technical assistance

HITEQ SERVICES SUPPORT:

- Health IT Enabled Quality Improvement
- EHR Selection & Implementation
- Health Information Exchange
- Health IT/QI Workforce Development
- Value-Based Payment
- Privacy & Security
- Electronic Patient Engagement
- Population Health Management & Social Determinants of Health
- Achieving Meaningful Use
- Telehealth & Telemedicine

Legal Disclaimer

- The information included in this presentation is for informational purposes only and is not a substitute for legal advice.

- Please consult an appropriate attorney if you have any particular questions regarding a legal issue.

Session Agenda

- Conducting a Security Risk Analysis
- Strengthening Breach Mitigation and Response Plans
- Cybersecurity Concerns Specific to Working Remotely
- Questions and Discussion

Your Presenter

Nathan Botts, PhD, MSIS

- Senior Study Director, Westat – Healthcare Delivery, Research, and Evaluation
- Privacy & Security domain lead for the HRSA HITEQ Center
- Health informatics specialist, with over 15 years of clinical software and systems R&D experience.
- Knowledge Integrator for the Privacy and Security Community of Practice, for the ONC Regional Extension Centers.
- Co-lead of the HL7 Consumer Mobile Health Application Functional Framework for Privacy and Security Considerations
- Professor of Cybersecurity – Purdue University Global

Conducting a Security Risk Analysis

Problem Statement

- *Privacy and Security management covers just about every aspect of a healthcare organization*
- *Risk measures cover a broad range of physical, analog, and digital systems and include both internally and externally housed systems*
- *Settings and technologies deployed vary to such a high degree that there are no singular tests that can be conducted to ensure compliance*
- *The Security Risk Assessment is one method for auditing the measures and mitigation strategies in place at a healthcare site.*

Healthcare Privacy & Security Policies and Regulations

- August 1996 – HIPAA Enacted by President Bill Clinton
- April 2003 – Effective Date of the HIPAA Privacy Rule
- April 2005 – Effective Date of the HIPAA Security Rule
- March 2006 – Effective Date of the HIPAA Breach Enforcement Rule
- September 2009 – Effective date of HITECH and Breach Notification Rule
- March 2013 – Effective Date of the Final Omnibus Rule

HIPAA Impact on Eligible Providers

- HIPAA compliance requires that providers be prepared to handle ePHI properly and follow the requirements in the HIPAA Privacy, Security, and Breach Notification Rules

- If a problem surfaces, an enforcement action can result—including million-dollar financial settlements, and Corrective Action Plans that can take years to complete and can cost many times the monetary settlements

- In order to comply with the HIPAA Security Rule, providers need to maintain an ongoing security program.

General OCR HIPAA Settlements

Issues:

- Lack of risk analysis/risk management
- Large breaches (e.g., 300,000 or more)
- Improper disposal
- Unencrypted mobile devices
- Widespread snooping

Triggers:

- Media attention
- Breach report
- DOJ/OIG referral
- Complaints

Reference: http://www.dwt.com/people/adamhgreene/

Impact on Eligible Providers

- Providers must conduct a security risk assessment (SRA), implement updates as needed, and correctly identify security deficiencies.

- By conducting an SRA regularly, providers can identify and document potential threats and vulnerabilities related to data security, and develop a plan of action to mitigate them.

Security Rule Requirements

Security Components	Example Variables	Example Security Measures
Physical Safeguards	• Facility structure • Data storage center • Computer hardware	• Building alarm system • Locked doors • Monitors shielded from view
Administrative Safeguards	• Designated security officer • Staff training and oversight • Information security control • Security Risk Assessment / review	• Staff training • Monthly review of user activity • Policy enforcement • New hire background checks
Technical Safeguards	• Controls on access to EHR • Audit log monitoring • Secure electronic exchanges	• Secure passwords • Data backup • Virus scans • Encryption
Policies and Procedures	• Written P&P addressing HIPAA Security requirements • Documentation of security measures	• Written protocols on safeguards • Record retention • Periodic policy and procedure review
Organizational Requirements	• Breach notification and other policies • Business Associate agreements	• Periodic Business Associate Agreement review and updates

Reference: Michigan Center for Effective IT Adoption

SRA Frequency

- Practices must conduct an SRA every year
- SRAs should be updated after major changes or upgrades to practice, technology, or environment
- Recommendation is at least annually for HIPAA compliance
- Risk management and assessment is a continuous process, so make sure you have documentation to support your ongoing risk assessment and management process
- Beyond compliance conducting SRAs is well-worth the money
- Leverage your membership in CHCNet for technical assistance if outside of your organization’s current capacity

SRA Fact Check

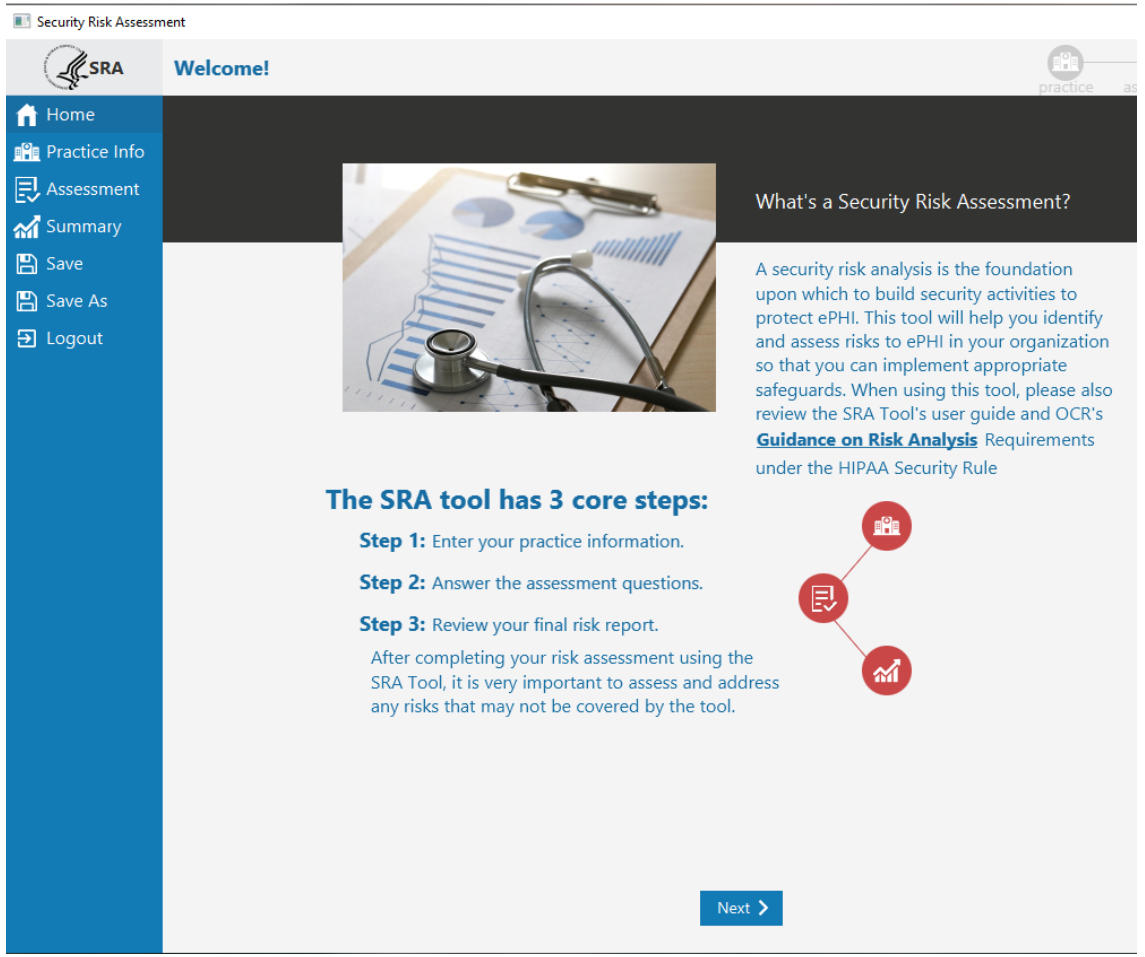
The security risk analysis is optional for small providers.	**False.** All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.
Simply installing a certified EHR fulfills the security risk analysis MU requirement.	**False.** Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.
My EHR vendor took care of everything I need to do about privacy and security.	**False.** Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.
A checklist will suffice for the risk analysis requirement.	**False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.**

Reference: ACR 2 Solutions

Enter the ONC SRA Tool

- Designed to help health care providers and business associates that handle patient information to evaluate risks, vulnerabilities and adherence to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

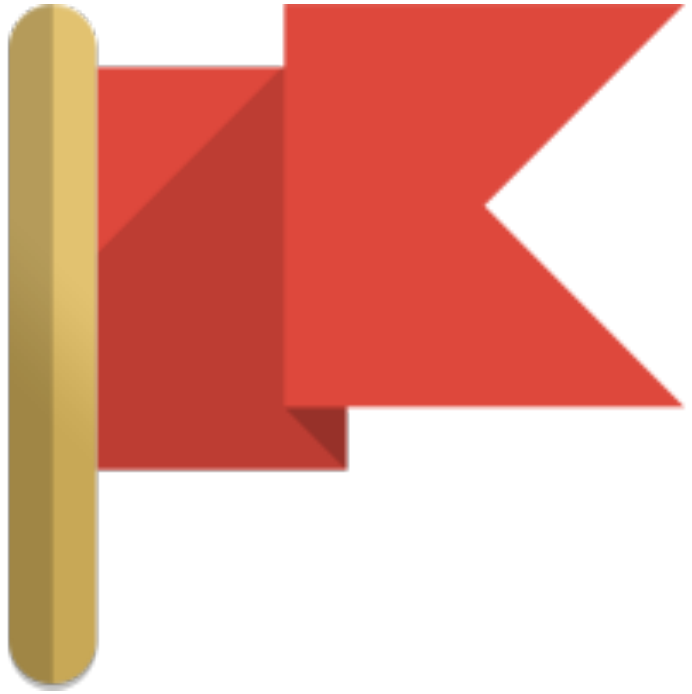
- The Office of the National Coordinator for Health Information Technology (ONC) worked together with the Office for Civil Rights (OCR), which enforces the HIPAA Security Rule, to develop this tool to enable providers and other entities to meet their HIPAA Security Rule compliance responsibilities.



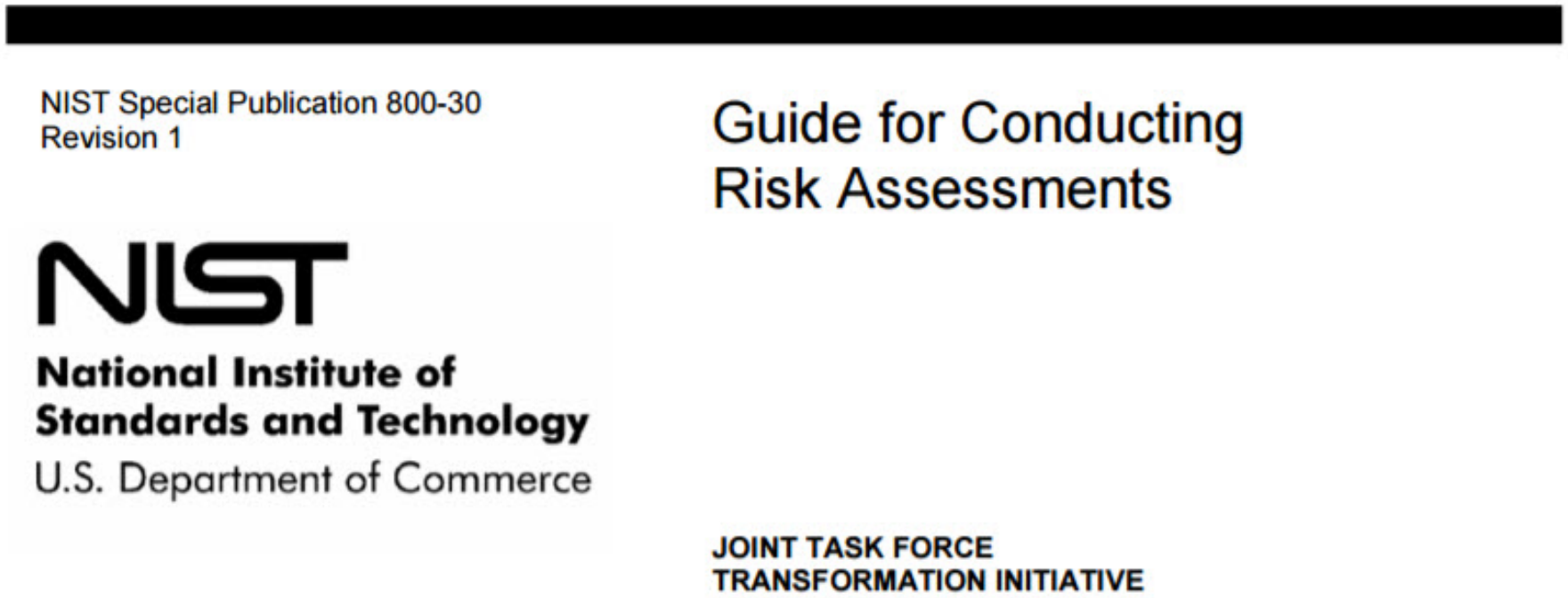
ONC SRA Limitations

- Use of this tool is neither required by nor guarantees compliance with federal, state or local laws.

- The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.



NIST 800 Series: Primary Resource for ONC SRA Toolkit



Primary SRA Sections 1-6

- Maintaining Your Security Program
- Identifying Your Assets
- Managing Access to Your Assets
- Managing the Integrity of Your ePHI
- Managing Your Media
- Managing Your Facilities

Each section broke down into subcategories:

- Administrative
- Physical
- Technical

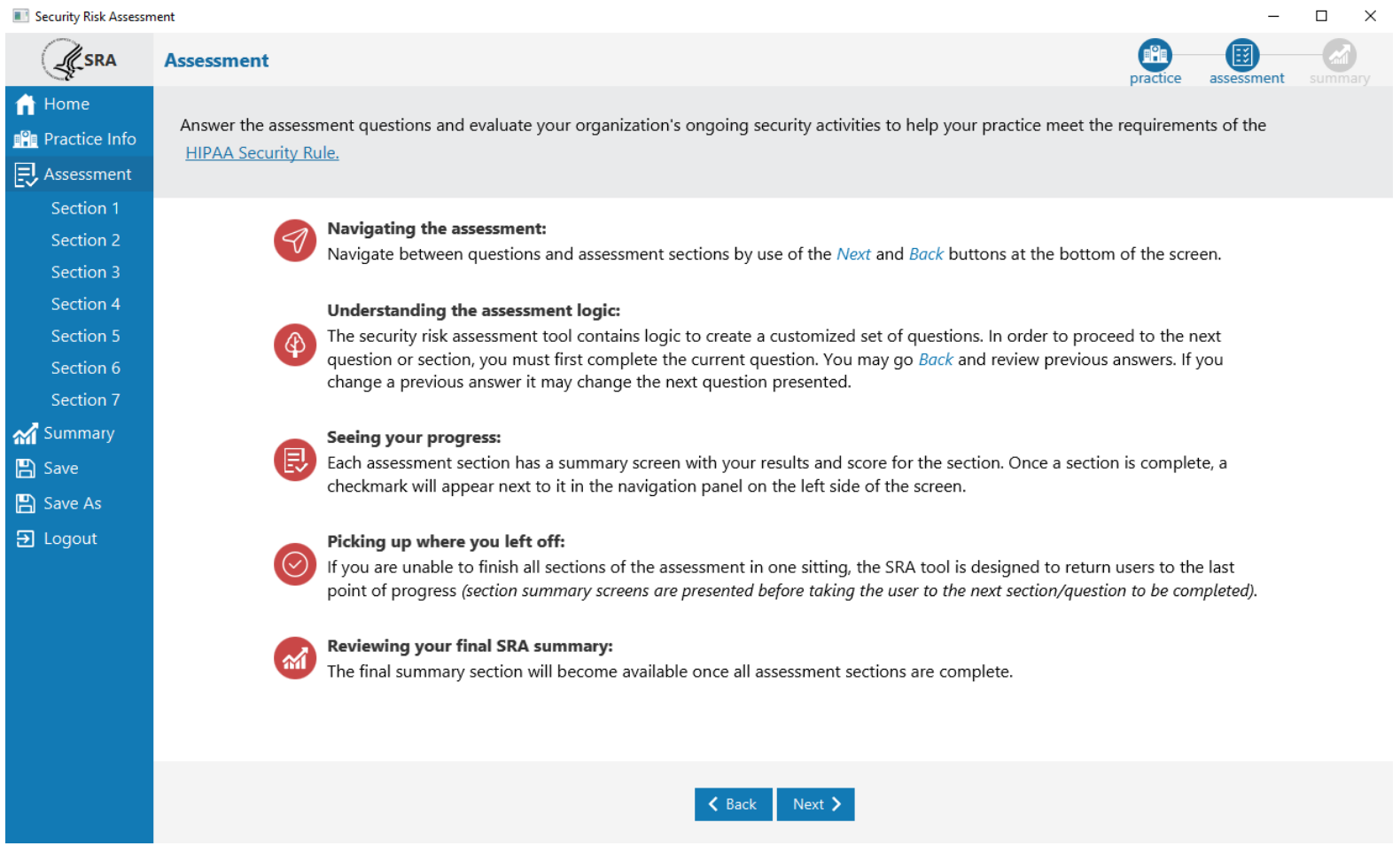
Primary SRA Sections 7-12

- Managing Your Workforce
- Educating Your Workforce
- Managing Your Vendors
- Continuing Your Operations When Emergencies Occur
- Auditing Your Operations
- Managing Incidents

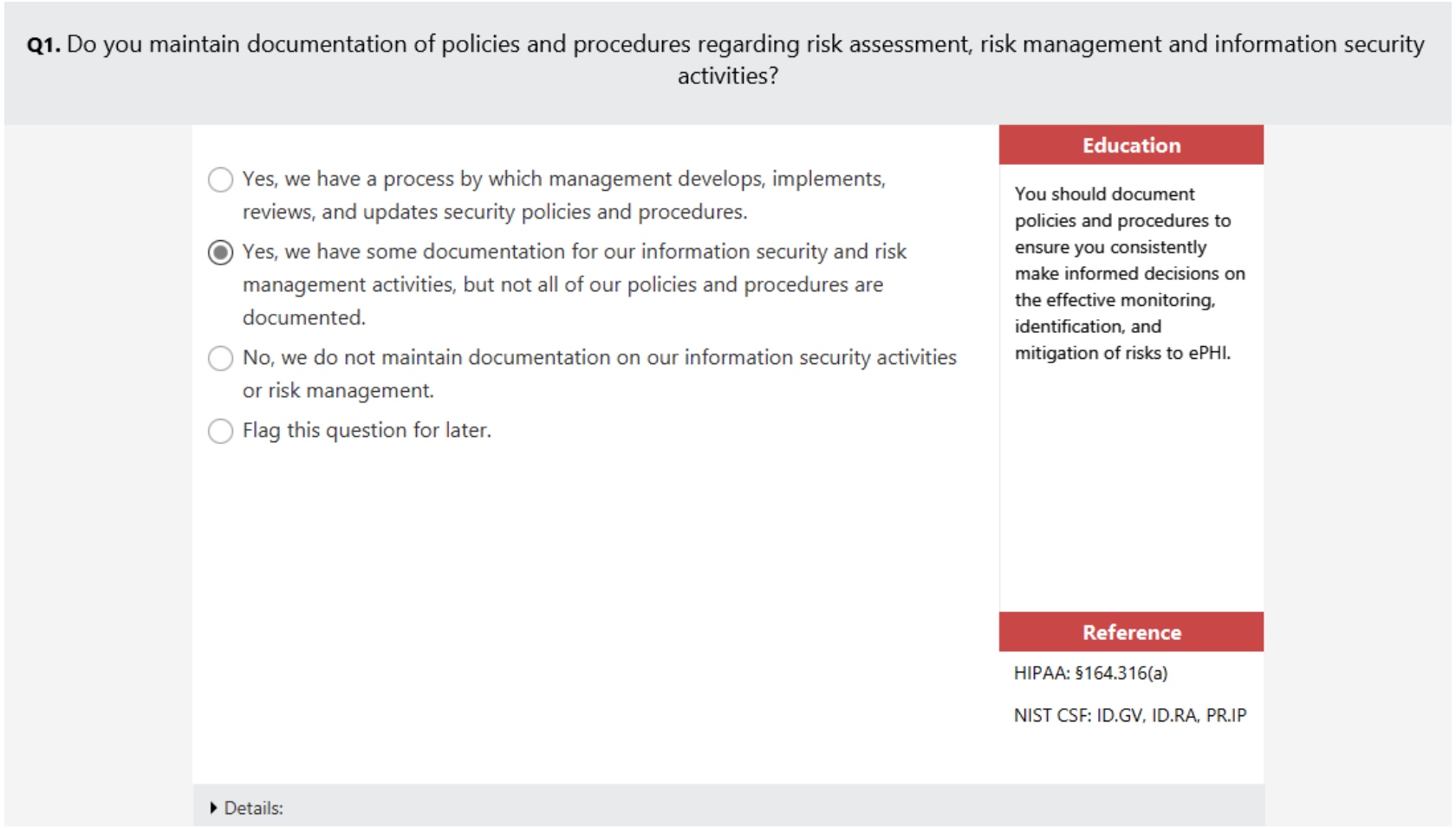
Each section broke down into subcategories:

- Administrative
- Physical
- Technical

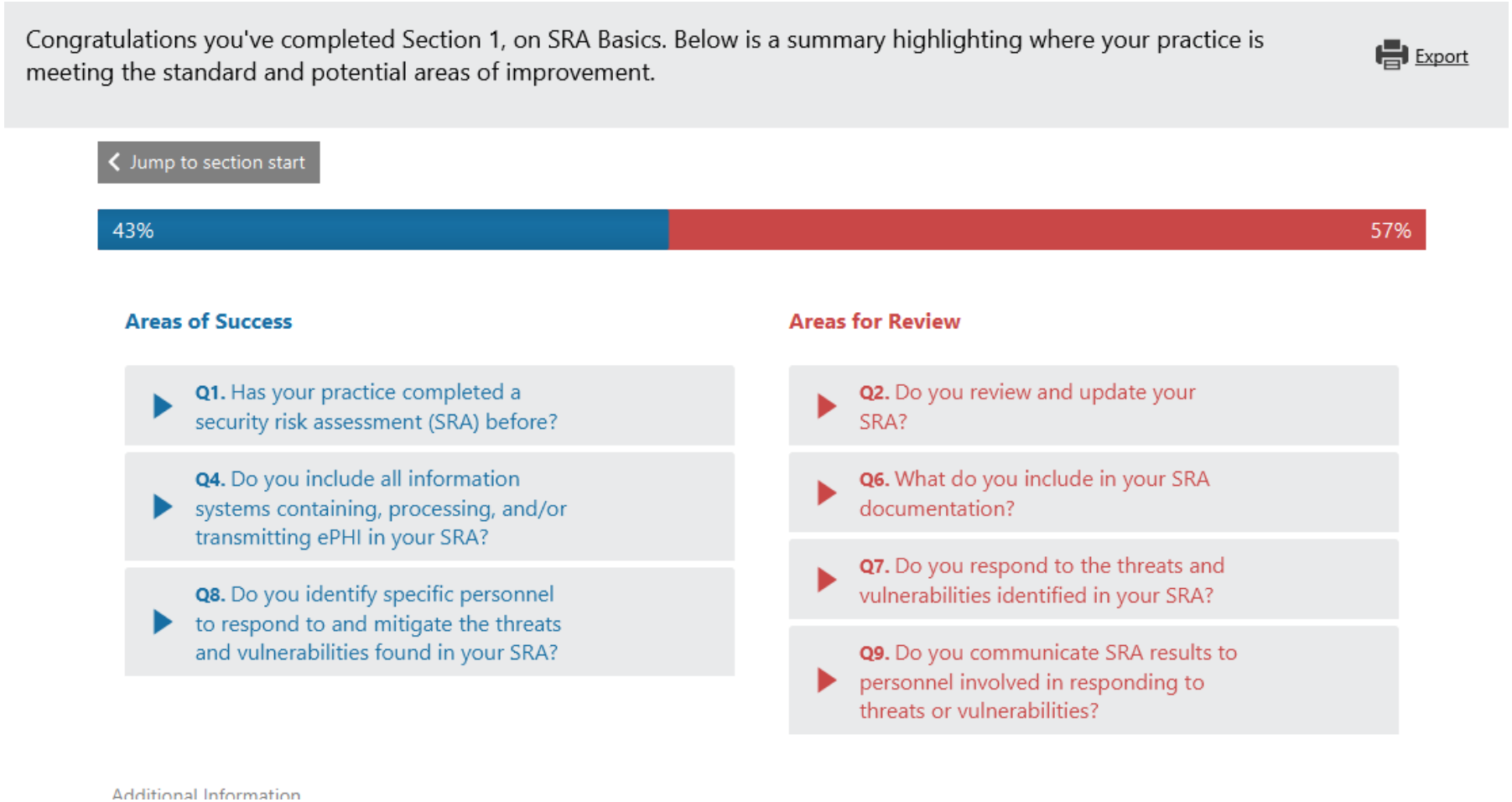
ONC SRA Assessment Menu



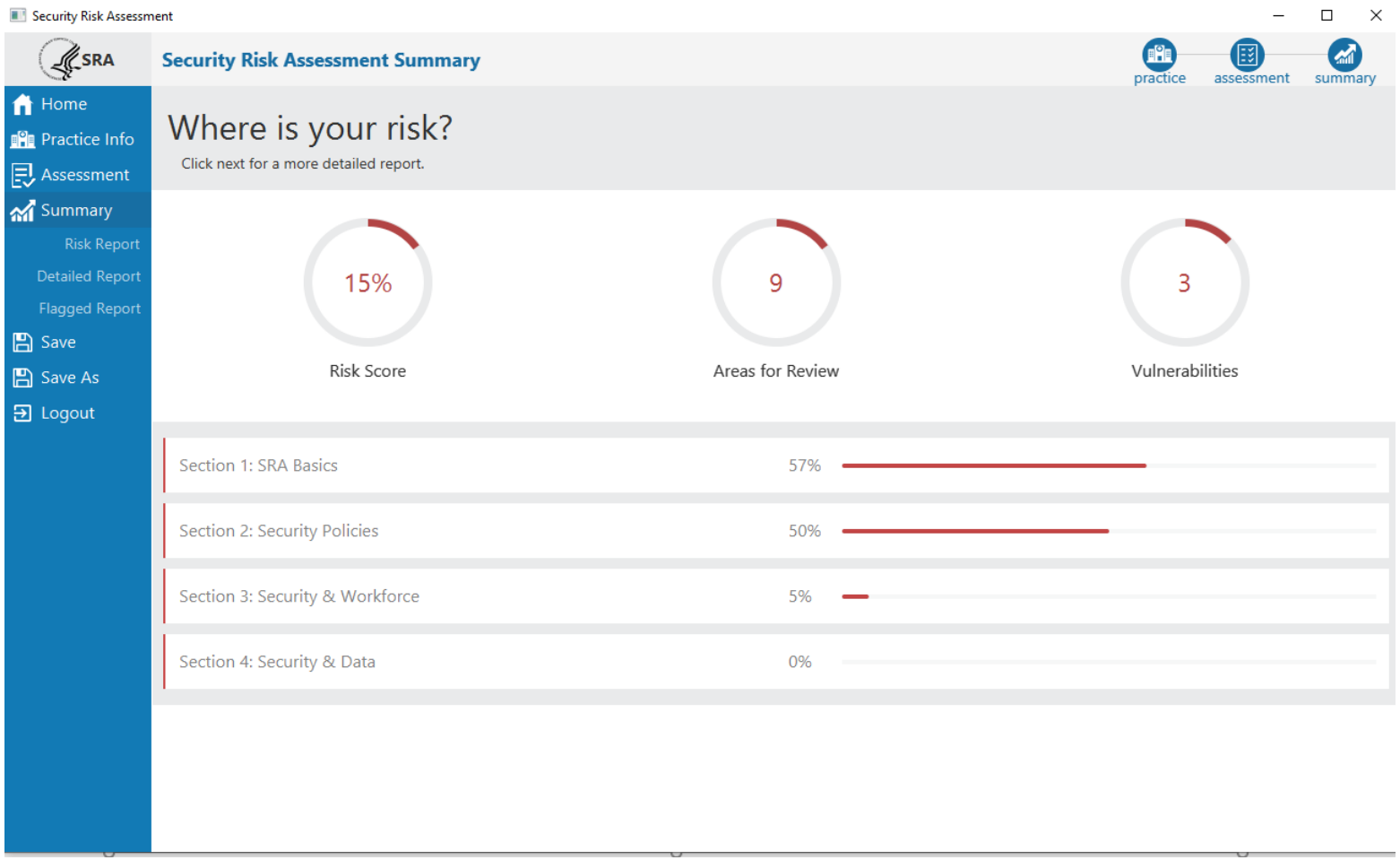
ONC SRA Tool Interview



ONC SRA Section by Section Guidance



SRA Dashboard



OCR Audit Schedule

- OCR has been enforcing HIPAA since 2003
- The OCR conducted its first set of audits in 2012
- The second phase began in 2016
- Provider compliance with Security, Privacy, and
- Breach Rules is audited
- Most common Security deficiencies from 2012-2013 pilot audits:
  - Lack of or incomplete SRA (47 out of 59 (79%))
  - Unaware of Security Rule requirements
- 2017 onward Comprehensive onsite audits to begin

Reference: Source: IAPP Conference March 7, 2013

Reasons for Compliance

- Covered entities that suffer a breach and have not performed a SRA, or otherwise do not have an effective risk management program, face the steepest penalties from the OCR
- A lack of or incomplete SRA is the main reason providers fail Meaningful Use (MU) audits, resulting in loss of incentive money
- Further costs due to ineffective security plans may include:
  - Breach victims may pursue legal action for damages
  - Many healthcare providers have lost access to their data due to ransomware attacks or contract disputes

Reference: Michigan Center for Effective IT Adoption

SRA Checklist

There are many ways to conduct a SRA but methods should at the very least encompass facets such as:

- Scope must include all ePHI in organization
- Data collection and methods must be documented
- Identify and document anticipated threats and vulnerabilities
- Assess current security measures in place
- Establish likelihood of threat occurrence
- Establish potential impact of threat occurrence
- Determine level of risk
- Document complete risk analysis
- Periodic review and update

SRA Summary

- Security Risk Assessments required for compliance with HIPAA and Meaningful Use
- Risk and regulatory oversight increasing and expected to continue
- Practices are expected to take security seriously and put forth a good faith effort
- Required: Hard work, diligence, integrity
- An SRA is the first step of a continuous, comprehensive Risk Management Program that will benefit your patients and your practice

Strengthening Breach Mitigation and Response Plans

HIPAA – Security Incident Response

Security Incident Procedures - §164.308(a)(6)

"Implement policies and procedures to address security incidents."

RESPONSE AND REPORTING (R) - §164.308(a)(6)(ii)

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

Security Incident Response Plan

NIST SP 800-53 (IR-8) Incident Response Plan:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability

Response Maintenance Plan

- Maintenance:
  - Test Incident Response Plan through Tabletop Exercises
    - Test likely scenarios (e.g. Ransomware, Phishing, Theft)
  - Improve based on lessons learned
  - Review documentation of security incidents to identify improvements
  - Update/Review annually

Readiness Questions

Questions to ask yourself:

- How are we documenting security incidents?
- What is our communications plan? Internal/External?
- Who are the decision makers? For example, who has ultimate authority to shut down critical systems such as EMR in order to prevent further infection of malware?
- Do all employees know how to recognize a security incident, know their obligation to report, and know how to report?

Post Incident Response Due Diligence

- Exactly what happened and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What new or different resources do we now need in order to improve the emergency planning/response process?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- In what ways can the organization prepare external audiences for a situation like this, in an effort to minimize the amount of damages or losses?

Incident Response Wrap-up

Increased threats are creating a higher number of attacks making incident response capabilities a requirement of organizational information security programs.

Prepare (Pre-Incident)	• Plan ahead for the incident events
Respond (Active Incident Response)	• Determine what you are fighting • How to stop it from spreading • How to get rid of it • Coordinated response requires following established processes
Report (Post-Incident)	• Remediate the root cause to minimize future issues • Learn from every opportunity and update your plan for future improvement

Healthcare Cybersecurity Implications during a Pandemic

Cybersecurity Concerns Specific to Working Remotely

Growth and Development of COVID-19 Phishing Templates

- "New Templates" means new and unique COVID-19 phishing templates encountered for the first time. This data from KnowBe4 shows that there has been high growth in new templates as spread of the pandemic increased.

- This illustrates just how actively hackers are trying to take advantage of the situation which means we have to be extra vigilant when working with email messages

Week	New Templates
Jan. 19 - Jan. 25	0
Jan. 26 - Feb. 1	1
Feb. 2 - Feb. 8	5
Feb. 9 - Feb. 15	6
Feb. 16 - Feb. 22	5
Feb. 23 - Feb. 29	3
Mar. 1 - Mar. 7	16
Mar. 8 - Mar. 14	16
Mar. 15 - Mar. 21	36
Mar. 22 - Mar. 28	94

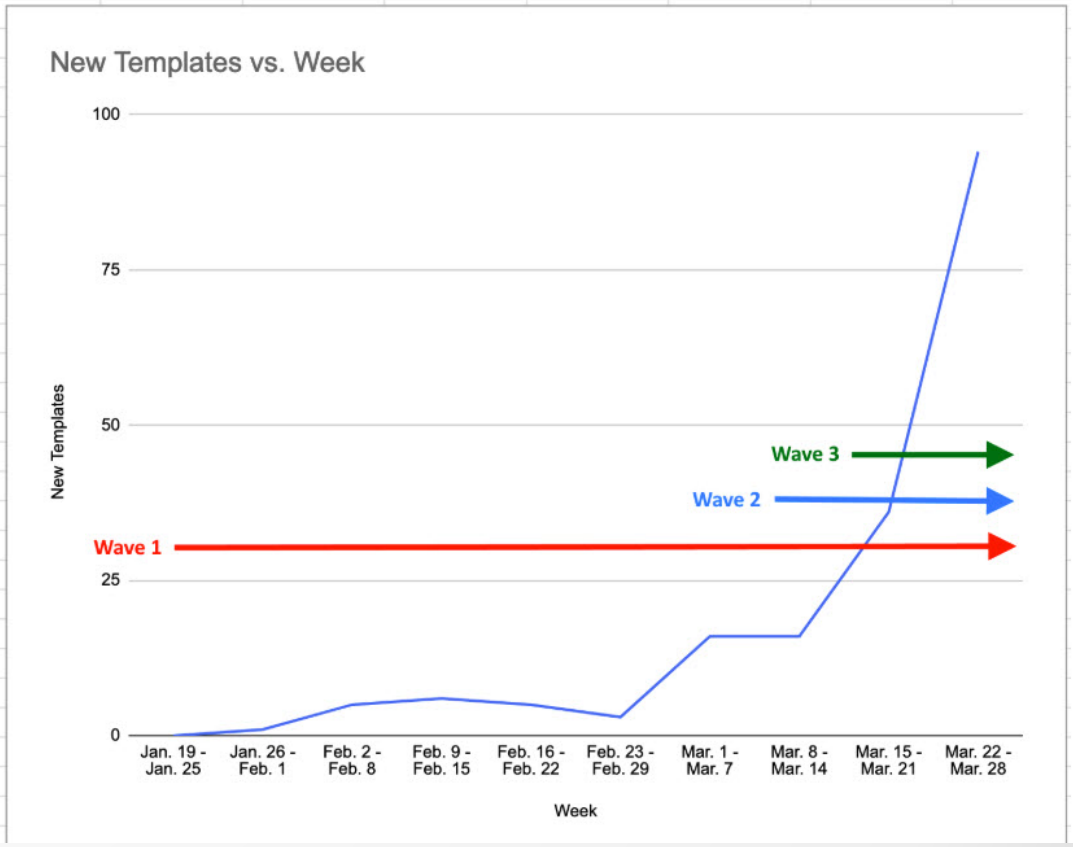
Note: "New Templates" means new and unique COVID-19 phishing templates encountered for the first time. Templates can be considered "new and unique" even if they are minor variations of earlier templates. Templates classified as "spam / scam" are not considered or included in this number.

The Three Waves of Templates

Wave 1: Spoofs of authoritative sources of information (CDC/WHO/HHS/HR) purportedly offering information and updates on the outbreak.

Wave 2: New and novel templates designed exclusively for COVID-19 that move beyond merely offering new information on the outbreak.

Wave 3: Re-purposed older templates and social engineering schemes modified and updated to include a COVID-19 theme or angle.

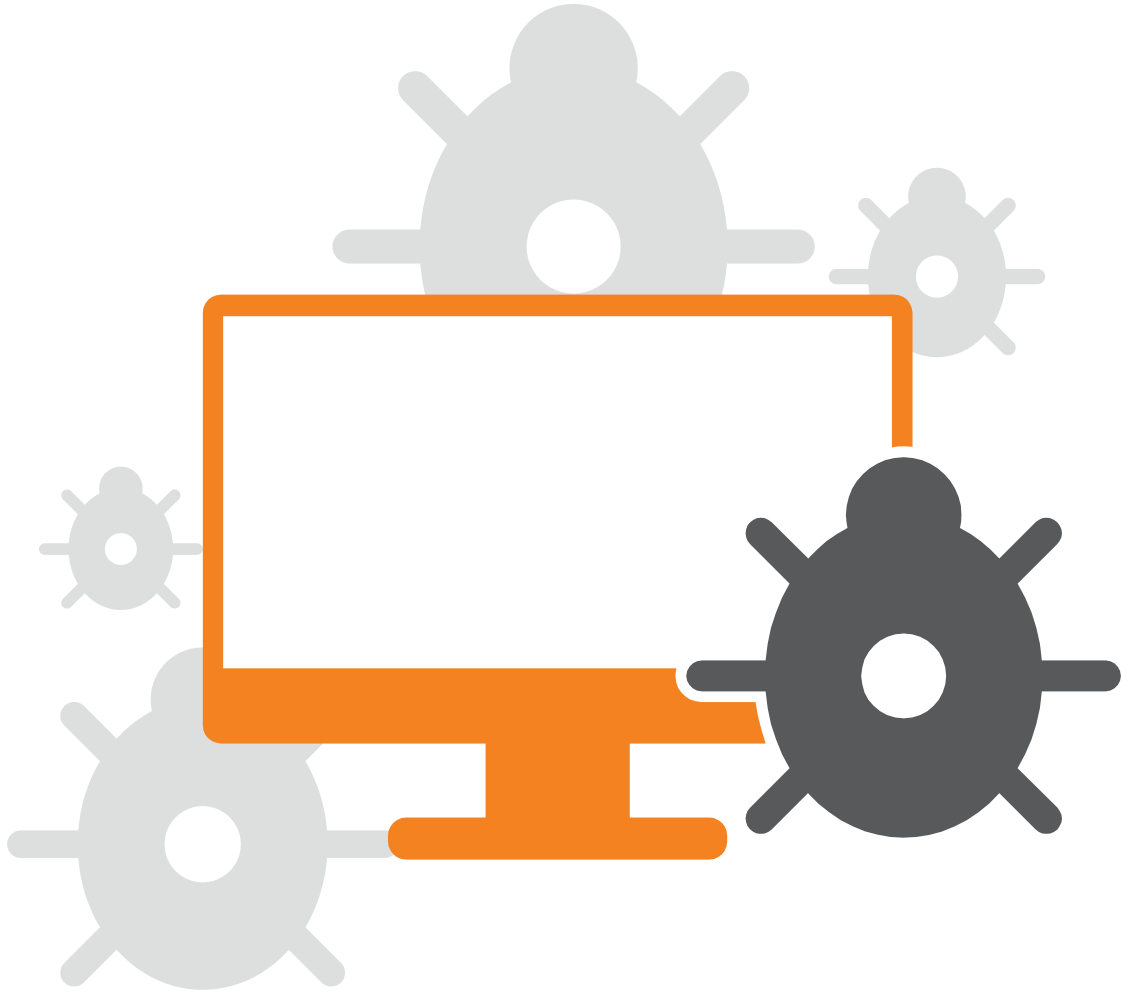


Reference: https://blog.knowbe4.com/the-dilemma-should-you-phish-test-during-the-covid-19-pandemic

A Compromised State of Affairs

The number of COVID-19 cases continue to increase throughout the United States, requiring more and more of our health systems to rely on employees working from home at times.

While some of us are required to "shelter-in-place," unfortunately that shelter can create increased risks such as cyber security breaches.



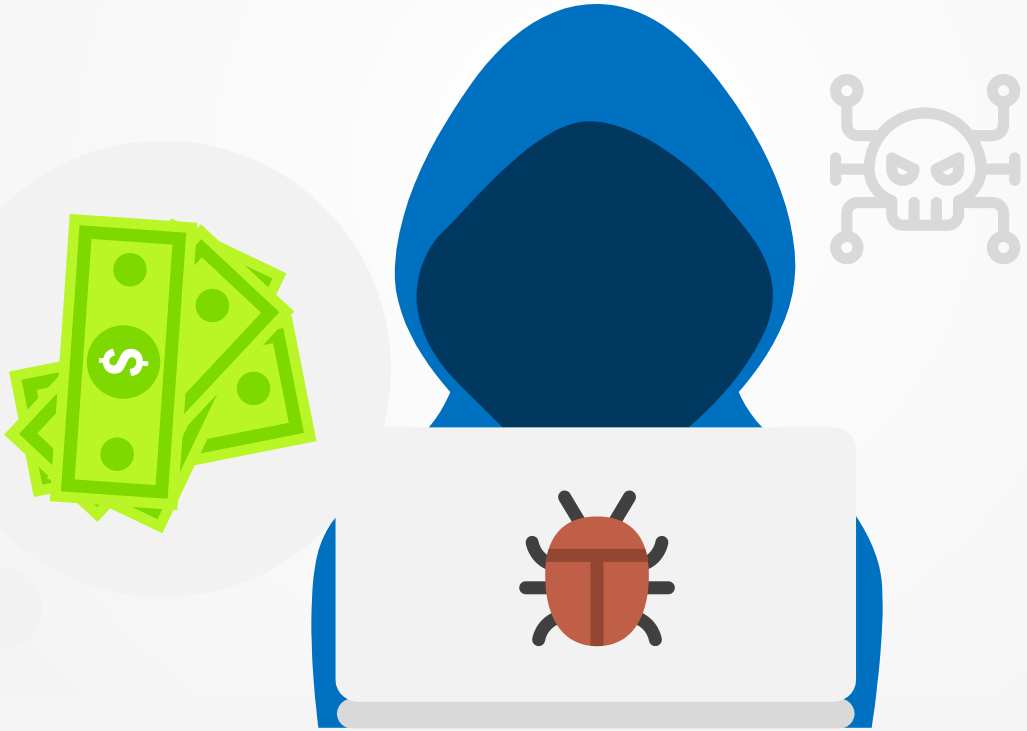
Health Care Workers are Targets of Interest

Sad but true

Having health care workers work from home creates a very opportunistic situation for hackers and phishers.

Every family member, home device or wireless connection is a **potential entry point** into the health center's network if not activel, protected.

Sadly enough, as we try to prevent the spread of the COVID-19 virus, "bad guys" are only trying that much harder to take advantage of us through new types of cyberattacks so that they can make money from the disruption.



There has been an increase in COVID-19-related phishing attacks, where hackers are taking advantage of individuals' fear and need for health, safety, and financial aid information.

Remaining Vigilant When Working Remotely

When working from home, people are often distracted by many other things than work (e.g., children, pets, health concerns, finances, etc.) – data security is understandably not always the number one concern and creates a matter of high risk.

Unfortunately for health centers this can result in a loss of control over their data and make them subject to significant legal liability due to a single email click or transmission of its data over an unsecured network.

With good planning, policies, and employee and family education, health centers can minimize risk and support their employees while working remotely.

Remote Worker Cyber Security Basics

01

Secure Your Router

This is a key gateway to the internet that needs to be protected.

02

Secure Your Computer

An updated computer is a safe computer.

03

Stop Phishing Attacks

It is still the number one attack vector.

04

Make Good Choices

Small details can make for big differences

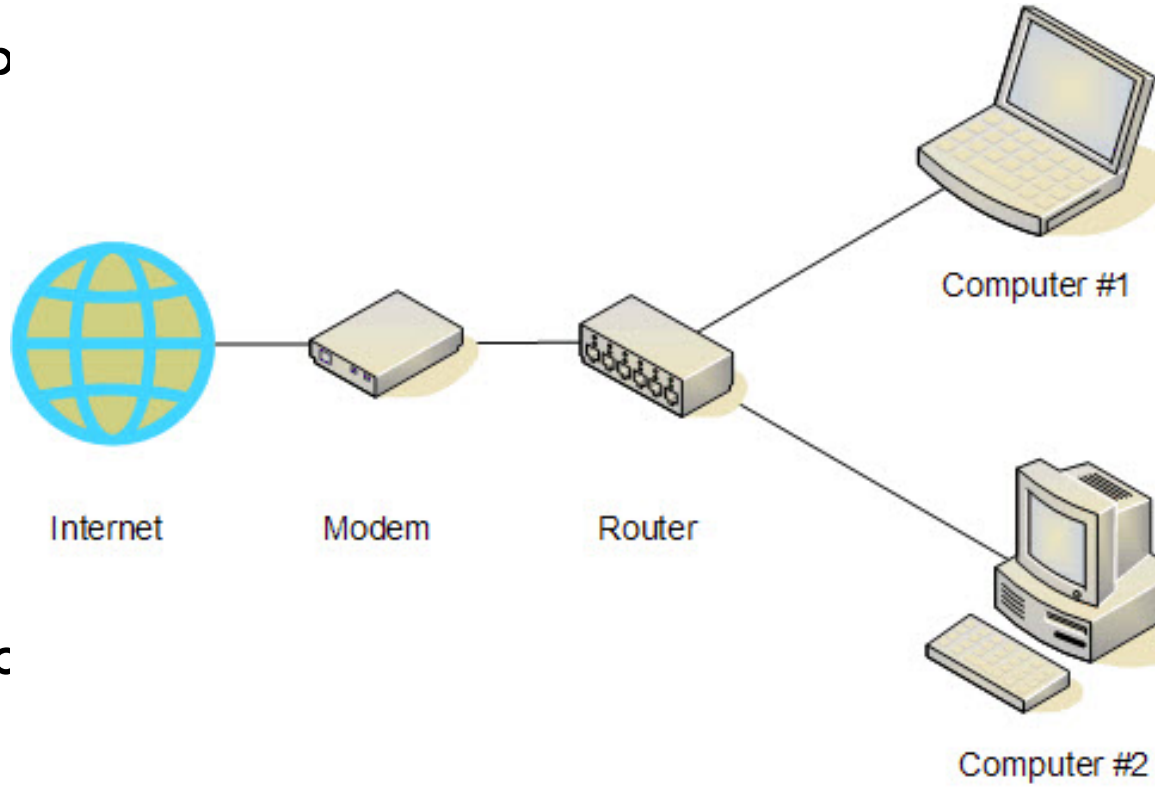
Making sure your router is secure – Part 1

At its most basic a home network is made up of a **modem,** a **router,** and the **computers** and **devices** connected to it.

One of the key pieces to address is the device called the “router”. If you have WiFi then you have one.

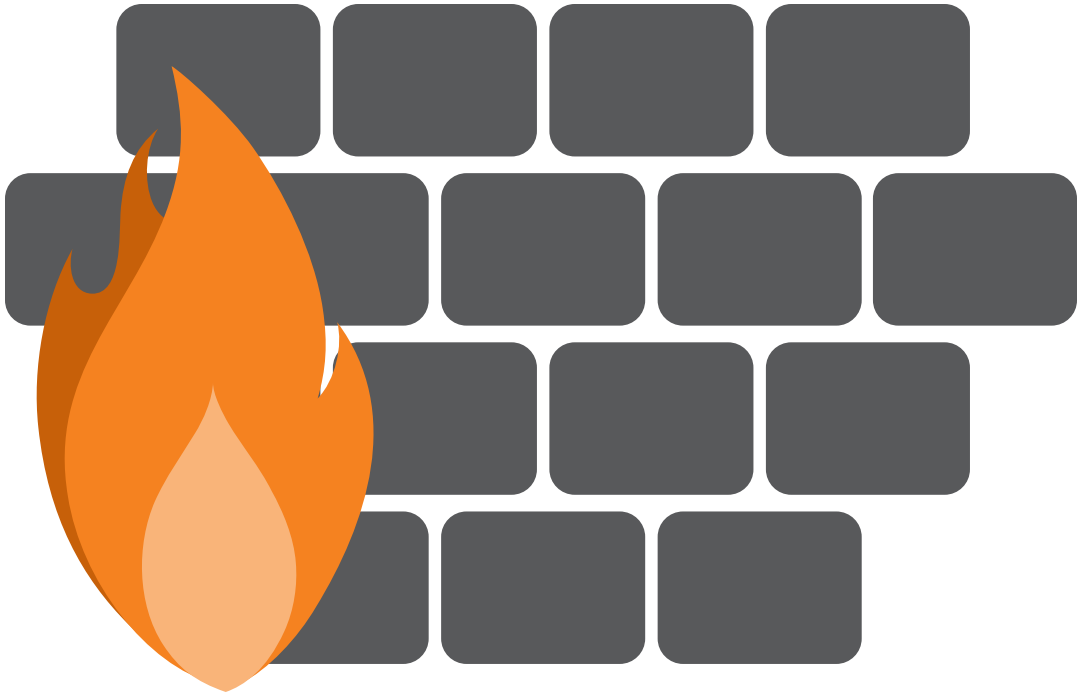
Most modern routers also include a firewall that helps block bad internet traffic

Making sure that your router software is up to date and that you are not using default passwords is a key element to your cyber security at home.



Making sure your router is secure – Part 2

- Your router should be using WPA2 (data encryption)
    - Check this by clicking on your WiFi icon, right clicking on the WiFi network you're connected to, and going to Properties. Then look for Security Type to be WPA2
- Find the name of your router, the brand generally found on the router itself, and start by searching on how to update it (e.g., Google 'update Netgear router')
- These steps can take some time if you are unfamiliar, but they are critical for increasing your cyber security when at home!
- This site has some good information on securely configuring your router and related concepts: https://www.comparitech.com/blog/information-security/secure-home-wireless-network/



Firewalls are as important at home as they are at work!

Virtual Private Networks (VPNs)

- A VPN encrypts your internet connection and hides your local ip address which can help protect your data, identity and network location from hackers
- Many people use VPNs as a part of their work procedures, but using VPNs for your personal activities online can help to increase the overall security of your home network.
- There are fairly low-cost VPNs (from $5 monthly to free) that are available for house-holds: https://pixelprivacy.com/vpn/no-log-vpn/
- Watch this video to learn a little bit more about how VPNs work and why they are important: https://www.youtube.com/watch?v=DsPsFdpZUlA

VPN services can help encrypt your internet traffic no matter where you happen to be working from!

Making Sure Your Computer is Up to Date

Regular software updates are one of the most effective steps you can take to improve the overall cybersecurity posture of your home networks and systems.

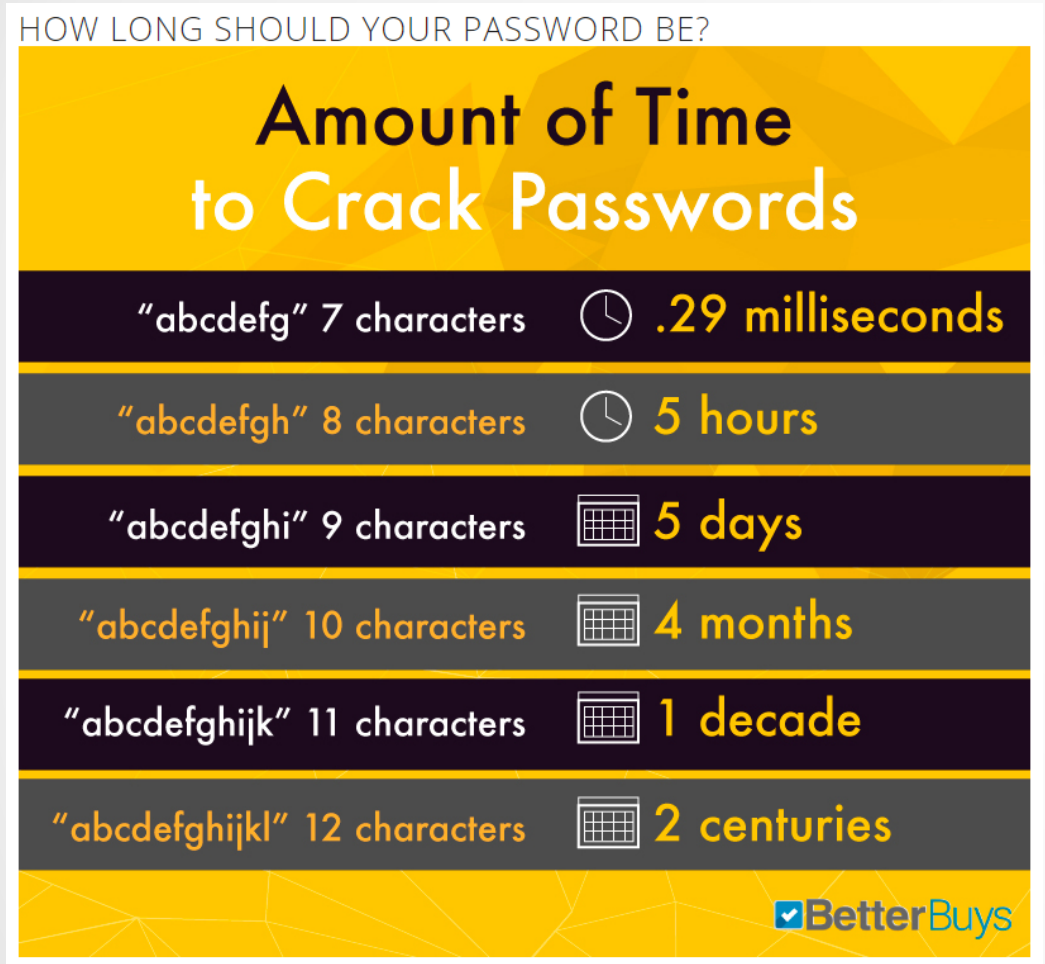
This means you need to make sure all of the computers in your house are updated not just your work computer. Any computer that has not been updated poses a risk to your home network that could open up a compromise to your work computer.

- Windows - Open Windows Update by clicking the Start button in the lower left corner. In the search box, type Update, and then, in the list of results, click either Windows Update or Check for updates. Click the Check for updates button and then wait while Windows looks for the latest updates for your computer.
- Apple - On your Mac, choose Apple menu > System Preferences, then click Software Update. To automatically install macOS updates, select "Automatically keep my Mac up to date."

Make sure your browser is up to date and configured correctly. This is a key virus entry point. Have your IT staff help you secure it.

Of course, make sure that your antivirus software is up to date on all computers on your network as well. This is something that needs to be run *daily* due to the increased number of threats that we are experiencing.

The Importance of Password Length



Adding a single character to a password boosts its security exponentially.

Combining numbers and letters rather than sticking with one type of character dramatically enhances password security.

A string of nine letters or numbers takes milliseconds to crack. Add a single letter, and your password may become cryptic enough to thwart password crackers for nearly four decades.

Stop the Phishing Attacks – Call Before You Click

Health center staff member working from home are likely dealing with a lot of emails and are trying to navigate all of the COVID-19 and related emails being sent your way.

You are probably tired of being told to be careful about phishing attacks, BUT, phishing emails continue to be one of the most common initial attack vectors employed by for malware delivery and credential harvesting (where a hacker steals login information, for example).

Read this article on avoiding phishing attacks from the US Department of Homeland Security: https://www.us-cert.gov/ncas/tips/ST04-014

If you are unsure about a message do not click! Call and ask someone to find out if it is safe before you try to download an attachment or click on a link.

Attackers often take advantage of current events and certain times of the year, such as:

- Natural disasters (e.g., Hurricanes)
- Epidemics and health scares (e.g., H1N1, COVID-19)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

Make Good Choices When Working Remotely

Do not use personal emails to send or receive company emails

Do not send or share data through personal file sharing or sending tools (e.g. a personal Dropbox account)

Make sure to not discuss Health Center matters through social media

Always make sure you are using a secure connection when communicating patient data.

If you have to use a public internet connection talk to your IT staff and make sure you know how to do so securely (e.g., VPN), contact IT to get access.

Make sure company devices are secured in the home at all times, and not left out where others could access them

If you have shared your password for your wireless network with family and friends, then change it. Not because you mistrust them, but because they could be using compromised equipment on your network. Update it and then confirm with people that there computers, phones, game systems, etc are up to date before passing it out.

Teleconference Privacy & Security Considerations

Check your environment to ensure that the video stream you are sharing does not contain sensitive information.

Set a meeting password, typically an option when creating the meeting, which adds a randomly generated password that invitees will need to input.

Enforce encrypted traffic. Do not take it for granted that systems have this option enabled by default for video communications. Some services encrypt chat by default but not video unless specifically requested.

When screen sharing, **only share the application needed,** as opposed to the whole desktop. Even an icon or name of a file on a desktop can give away sensitive information.

Take the time to work through all the options in the settings of the videoconferencing system you are using or are thinking of using.

COVID-19 Break the Glass Scenario

OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients.

This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19.

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Using Non-Traditional Telehealth During the COVID-19 Pandemic

- During this public health emergency, the Office for Civil Rights has eased regulations on the use of some non-traditional telehealth technologies that can be used for any services, not only those specific to COVID-19.
- Visit this resource to make sure you understand what you can and cannot do: https://hiteqcenter.org/Resources/Privacy-Security/HIPAA/using-non-traditional-technology-for-telehealth-during-covid-19-pandemic

DO NOT USE FOR TELEHEALTH

Any video communication applications that are public facing (such as live streaming) should not be used in the provision of telehealth by health care providers. These include the following:

- Facebook Live
- Instagram Live
- Twitch
- TikTok

PERMISSIBLE DURING THIS PUBLIC HEALTH EMERGENCY

Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.

- Apple FaceTime
- Facebook Messenger video chat
- Google Hangouts video
- Skype
- Zoom

Conclusion

- Health Center Privacy and Security is everyone's responsibility
- Security Risk Analysis is your #1 tool for protecting your health information systems from breach
- There are known best practices and frameworks that can be followed to help ensure information security is addressed appropriately
- Effective incident response is about planning and practice
- Help defend your Health Centers against the Dark Web!

Get Your Badge!

1. Visit: http://bit.ly/hiteq-defender
2. Read through the suggested resources:
   - Ransomware Guidance Presentation for Health Centers
   - Creating and Managing Strong Passwords at Your Health Center
   - The Health Center CIO's Guide to HIPAA Compliant Text Messaging
   - Health IT Privacy & Security Skill Sets
   - Breach Protection Overview Presentation for Health Centers
3. Fill out the Health Center Defender Against the Dark Web Badge Confirmation form
4. Receive your badge!

Comments, Questions, and Discussion

Questions? Feedback?

Email: hiteqinfo@jsi.com

Phone: 1-844-305-7440

Email: gparent@mepca.org

The HITEQ Center project is/was supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $535,717 with 0 percent financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.