



AMERICAN ACADEMY™
OF OPHTHALMOLOGY

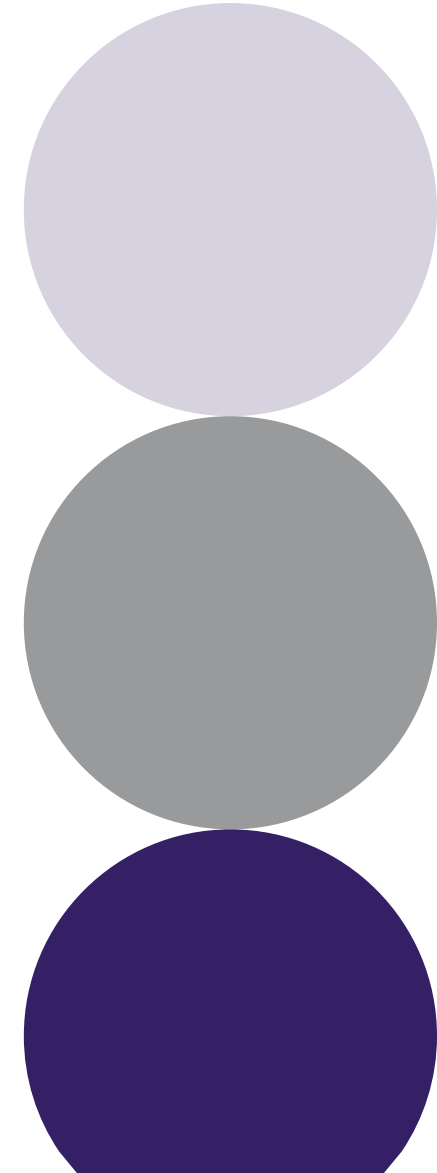
Protecting Sight. Empowering Lives.™

Cybersecurity – Change Healthcare Changes Healthcare

Ravi D Goel, MD
Senior Secretary for Ophthalmic Practice



Regional Eye Associates





Financial Disclosure

- I have the following financial interests or relationships to disclose:
 - DORC, LLC: Lecture Fees/Speakers Bureau
 - Alcon Laboratories, Inc.: Lecture Fees/Speakers Bureau
 - Evolve Medical Education, LLC: Lecture Fees/Speakers Bureau
 - iVeena Delivery Systems Inc.: Equity/Stock Holder - Private Corp



The good old days

CC
HPI
ROS

VA
IOP

Anterior
Segment

Testing

Posterior
Segment

A/P

10-10 RDG

Date: AUG 19 2013 Name: _____ DOB: _____ Age: 76
 Last Exam: 4/15/13 Sent by: _____ Oc Meds: OD OS
 CC/HPI: blurry O.D. (1/1/13) 10/10/13 10/10/13 10/10/13 10/10/13 10/10/13 10/10/13 10/10/13 10/10/13 10/10/13
 glaucoma eval, HVF Bion-BID-OU

FH: mom AMD
 PMD: Dr. Kazowski
 ALL: sulfa, PCN, Ammax. (NKDA)
 Meds: Dexam, Atenolol, HCTZ, Fish oil, vit D, CA, gluc chem.

POH: APE-OS, gl(s), mild NS, ↑ old OS/OD
 ROS: (see intake sheet) BP, arthritis

EOM: D & V Full OU VF: FTCTF OU P: RR RAPD O Neuro: & o x3 or
 Sterco: _____ Color: _____

VA:

	sc	cc (spec/CL)	ph	near	(cm)	OR
OD		10/9+1				
OS		10/9+1				

PC: OD: _____ OS: _____ MRx OD: _____ OS: _____
 CRx OD: _____ OS: _____

Myd 0.5%/1.0% Neo 2.5% C 1% OD/OS/OU at _____ by _____ T_s < 16 (at _____) T (p dil) < _____

External:

SLE:

	OD	OS
L/L	<input type="checkbox"/> wnl	<input type="checkbox"/> wnl
Conj/Scl	<input type="checkbox"/> w&q	<input type="checkbox"/> w&q
K	<input type="checkbox"/> clear	<input type="checkbox"/> clear
TBUT	<input type="checkbox"/> wnl	<input type="checkbox"/> wnl
AC	<input type="checkbox"/> D & Q	<input type="checkbox"/> D & Q
Iris	<input type="checkbox"/> reg	<input type="checkbox"/> reg
Lens	<input type="checkbox"/> clear	<input type="checkbox"/> clear
AVit	<input type="checkbox"/> no cells	<input type="checkbox"/> no cells

Gonio: *AS/M* Last HVF: *full* Last HRT: *4/13*

DFE:

	OD	OS
Media	<input type="checkbox"/> PVD	<input type="checkbox"/> PVD
Disc	<input type="checkbox"/> pink/sharp	<input type="checkbox"/> pink/sharp
Macula	<input type="checkbox"/> wnl	<input type="checkbox"/> wnl
Vessels	<input type="checkbox"/> wnl	<input type="checkbox"/> wnl
Periphery	<input type="checkbox"/> flat	<input type="checkbox"/> flat

Assessment & Plan: *10/10/13* *glaucoma suspect* *field's*

Discussed: Sunspecs MVI Amsler W/C L/H AT () RDW BS control BP/chole R/B/A cat's YAG cap RTD: *4/13/13* Full/Ref CatV Caps V PO IOPV HRT HVF Pachy Macula CL Ref FU Sign: *[Signature]*



EMR 2024



CHANGE
HEALTHCARE



AMERICAN ACADEMY™
OF OPHTHALMOLOGY



Protecting Sight. Empowering Lives.™

CHANGE HEALTHCARE



Change Healthcare cyberattack impact Key takeaways from informal AMA survey

Over 1,400 individuals responded to an informal AMA survey of the Federation of Medicine (state medical associations and national medical specialty societies) on the impact of the [Change Healthcare cyberattack](#) on physician practices. The survey was open to respondents from March 26 – April 3, 2024. Respondents could skip questions; not all questions have 1,400 respondents.

Practice demographics: Most responses came from practices with fewer than 10 physicians.

1,297	Practices with 99 or fewer physicians
74	Practices with 100 to 999 physicians
30	Practices with 1,000+ physicians
Additional details:	
432	Single-provider practices
1,097	Practices with ≤ 10 physicians

Over 77% of respondents have experienced service disruptions since Feb. 21 and are still feeling the effects of the cyberattack (N=1,353).

Respondents reported that several functionalities have been suspended, resulting in a substantial use of workarounds (N=940).

- Restricted functionality has resulted in:
 - 36% have experienced suspension in claim payments
 - 32% have not been able to submit claims
 - 39% have not been able to obtain electronic remittance advice
 - 22% have not been able to verify eligibility for benefits
- Considerable use of both manual and electronic workarounds:
 - 31% have employed both workarounds to be paid for claims
 - 31% have had to use both workarounds to submit claims
 - 25% have had to use both workarounds to obtain electronic remittance advice
 - 25% have had to use both workarounds to verify eligibility for benefits
- In addition, the survey revealed that many practices reported **disruptions in electronic lab ordering.**

"Not being able to send paper claims to the insurance companies that require electronic billing for this time in need"

Service disruptions from the cyberattack have led to severe consequences for physician practices (N=923).

- 80% have lost revenue from unpaid claims
- 85% have had to commit additional staff time/resources to complete revenue cycle tasks
- 78% have lost revenue from claims that they have been unable to submit
- 51% have lost revenue from the inability to charge patient co-pays or remaining obligations

"...may bankrupt our practice of 50 years in this rural community."
 "This cyberattack is leading me to bankruptcy and I am just about out of cash"
 "I am now going to get acquired by a hospital system because I just can't bear the financial responsibility"

"...may bankrupt our practice of 50 years in this rural community..."

"This cyberattack is leading me to bankruptcy and I am just about out of cash"

"I am now going to get acquired by a hospital system because I just can't bear the financial responsibility"

"SOOOO much overtime dealing with this. Cost me additional \$50,000 in payroll."

"...estimated \$100,000 in unexpected costs."

"All of our expenses are being paid from my personal account"

"This crippled our brand new practice. I am keeping the lights on using personal funds."

"I have not taken a salary for a month and am borrowing from personal funds to keep practice going"

Physician practices are resilient, but disruptions from the cyberattack have forced practices to adapt (N=786).

- 55% of respondents had to use personal funds to cover practice expenses
- 44% were unable to purchase supplies
- 31% were unable to make payroll
- However, even facing all these payment and claim disruptions, only 15% of practices have reduced office hours

"Payroll taxes and gross receipts are not able to be paid, resulting in penalties. Other overhead costs are not able to be paid, also resulting in late fees."
 "Our bank account is not going to cover payroll soon. We have cut back on supply ordering."
 "...We are barely able to pay employees and can't pay our vendors"

Physician practices are being forced to enter new, and potentially costly, arrangements with alternative clearinghouses (N=772).

- 48% of respondents have engaged alternative clearinghouses to conduct electronic transactions

"We couldn't afford the cost of doing this. Other clearinghouses are taking advantage of this and small practices like mine who are already suffering without funds coming in can't afford to pay three times as much to take the time to switch clearinghouses."
 "Approximately \$10,000 just for the set-up of a 'back-up' clearinghouse. Additionally, one of our payers has changed clearinghouses, and they have told us that we are going to have an additional 2% charge on all claims, which will cost the organization approximately \$1,000,000"

Some practices are taking advantage of advance payments, temporary funding assistance, and loans, but issues persist (N=443).

- 55% of respondents said they used personal finances
- 12% of respondents have received assistance from CMS/Medicare
- 0.7% have received assistance from State Medicaid Plans
- Nearly 25% have received assistance from UnitedHealth Group/Optum
- 4.5% have received assistance from other health plans

"SOOOO much overtime dealing with this. Cost me additional \$50,000 in payroll."
 "...estimated \$100,000 in unexpected costs."
 "All of our expenses are being paid from my personal account"
 "This crippled our brand new practice. I am keeping the lights on using personal funds."
 "I have not taken a salary for a month and am borrowing from personal funds to keep practice going"

Many respondents are concerned about the negative impact this attack has had on patient care.

"Severely affected our ability to manage pain care with our cancer patients"
 "...patients had procedures delayed due to lack of access"
 "...anyone needing prior authorization has been unable to get their medicines. I have on patient that was unable to get her biological for two months as she was unable to afford the cash cost and her disease flared significantly."
 "...inability to verify and accept patient insurance prior to visits, which then don't happen."
 "...patients are suffering from delays in medical care and increased medical bills because alternative options could not be given with an appropriate estimate because of this attack."
 "Cannot access lab order or get results"

The informal survey demonstrates that significant problems continue, especially for small practices. The survey was conducted after UnitedHealth Group (UHG) said that claims would be flowing by the weekend of March 23rd. Despite UHG's assurances, serious disruptions continue. The survey is also a reminder of the fragility of physician practices. [Visit the AMA website for more information.](#)



IRIS, MIPS, & Security Analysis



AMERICAN ACADEMY OF OPHTHALMOLOGY®

2023 IRIS® Registry
Preparation Kit

Protecting Sight. Empowering Lives.®

Quality Payment PROGRAM

**Merit-Based Incentive Payment System (MIPS)
Promoting Interoperability Performance Category
Measure
2023 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.

1

The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Security Risk Assessment Tool v3.4

User Guide

DISCLAIMER
The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights (OCR) Health Information Privacy website at: www.hhs.gov/oc/privacy/hipaa/understanding/index.html

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

Updated: September 5, 2023

1



Meaningful Use & Security Risk Assessment



HealthIT.gov

Newsroom - FAQs - Multimedia - Implementation Resources

Providers & Professionals | Patients & Families | Policy Researchers & Imp

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Success Case

HealthIT.gov > For Providers & Professionals > Privacy & Security > Security Risk Assessment > Top 10 Myths of Security Risk Analysis

Security Risk Assessment

Guide to Privacy and Security of Electronic Health Information

Health IT Privacy and Security Resources

Mobile Device Privacy and Security

Model Notices of Privacy Practices

Patient Consent for eHIE

Privacy & Security Training Games

Cybersecurity

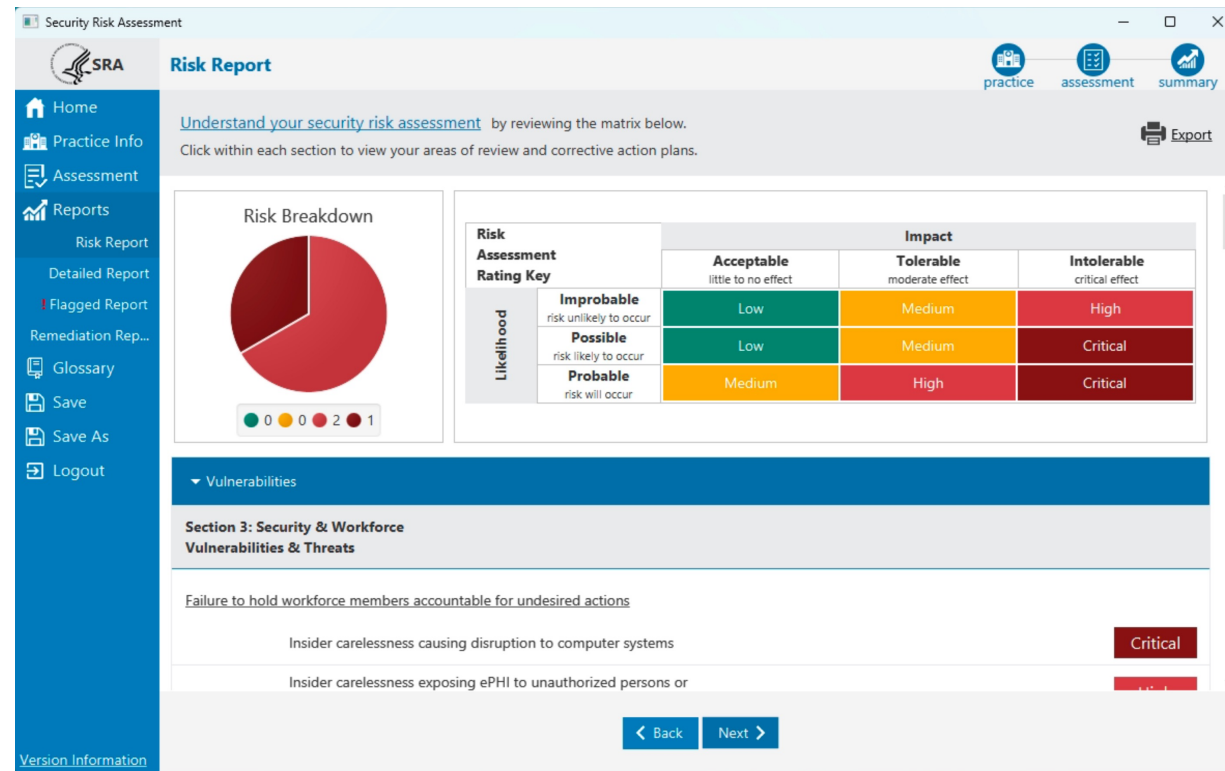
Security Risk Assessment

Security Risk Assessment Tool

Top 10 Myths of Security Risk Analysis

As with any new program or regulation, there may be misinformation making the rounds. The following is a top 10 list distinguishing fact from fiction.

- 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.
- I have to outsource the security risk analysis.
 - False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a



Security Risk Assessment

SRA Risk Report

practice assessment summary

Home

Practice Info

Assessment

Reports

Risk Report

Detailed Report

Flagged Report

Remediation Rep...

Glossary

Save

Save As

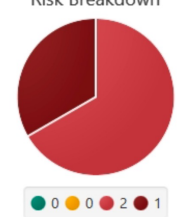
Logout

Version Information

Understand your security risk assessment by reviewing the matrix below. Click within each section to view your areas of review and corrective action plans.

Export

Risk Breakdown



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

Vulnerabilities

Section 3: Security & Workforce Vulnerabilities & Threats

Failure to hold workforce members accountable for undesired actions

Insider carelessness causing disruption to computer systems **Critical**

Insider carelessness exposing ePHI to unauthorized persons or **Critical**

Back Next





Security Risk Analysis

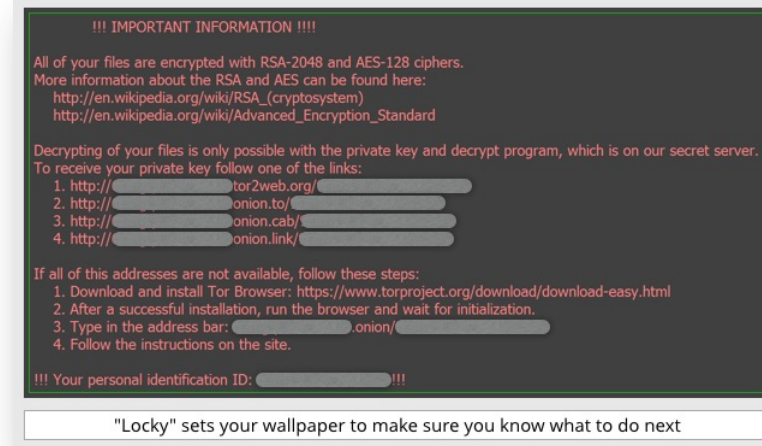
- Pearl #1 – Define Scope of Security Risk Analysis
- Pearl #2 – Gather data
- Pearl #3 – Identify potential threats
- Pearl #4 – Assess Existing Security Measures
- Pearl #5 – Determine Likelihood of Threat Occurrence
- Pearl #6 – Determine the Level of Risk
- Pearl #7 – Identify and Document Improved Security Measures



Hollywood Presbyterian Medical Center



wikipedia (Junkyardsparkle)



AMERICAN ACADEMY™
OF OPHTHALMOLOGY

Sophos.com screenshot - for **identification and critical commentary** relating to the website in question)



Protecting Sight. Empowering Lives.™

“Locky” cryptolocker ransomware

WHAT TO DO?

- **Backup regularly and keep a recent backup copy off-site.** There are dozens of ways other than ransomware that files can suddenly vanish, such as fire, flood, theft, a dropped laptop or even an accidental delete. Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands.
- **Don't enable macros in document attachments received via email.** Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of malware infections rely on persuading you to turn macros back on, so don't do it!
- **Be cautious about unsolicited attachments.** The crooks are relying on the dilemma that you shouldn't open a document until you are sure it's one you want, but you can't tell if it's one you want until you open it. If in doubt, leave it out.
- **Don't give yourself more login power than you need.** Most importantly, don't [stay logged in](#) as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you have administrator rights.
- **Consider installing the Microsoft Office viewers.** These [viewer applications](#) let you see what documents look like without opening them in Word or Excel itself. In particular, the viewer software doesn't support macros at all, so you can't enable macros by mistake!
- **Patch early, patch often.** Malware that doesn't come in via document macros often relies on security bugs in popular applications, including Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for the crooks to exploit.

Follow @NakedSecurity 50.2K followers

Follow @duckblog 8,779 followers



AMERICAN ACADEMY™
OF OPHTHALMOLOGY

(Sophos.com screenshot - for **identification and critical commentary** relating to the website in question)



Protecting Sight. Empowering Lives.™

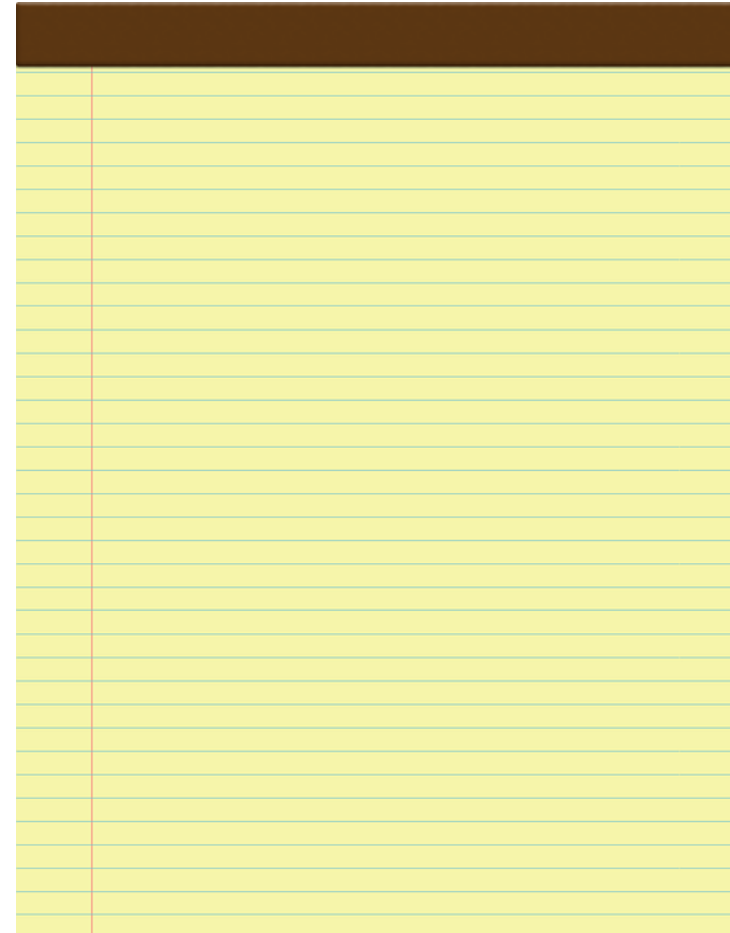
T. Boone Pickens Idea of Cybersecurity ...

T. Boone Pickens **Following**
@boonepickens

What's my secret to cyber security? The only think I use is a yellow notepad.
pickensplan.com/?p=11550

RETWEETS **10** LIKES **19**

10:02 AM - 1 Oct 2016





Top 10 Tips for Cybersecurity in Health Care



1. Establish a Security Culture
2. Protect Mobile Devices
3. Maintain Good Computer Habits
4. Use a Firewall
5. Install and Maintain Anti-Virus Software
6. Plan for the Unexpected
7. Control Access to Protected Health Information
8. Use Strong Passwords and Change Them Regularly
9. Limit Network Access
10. Control Physical Access



Cybersecure – Your Medicare Practice



Cybersecure
Your Medical Practice

HealthIT.gov
Advancing America's Health Care

DEPARTMENT OF HEALTH & HUMAN SERVICES • USA

This game module is intended to raise awareness and increase understanding of common privacy and security issues related to health information technology. It is not an exhaustive representation of all the privacy and security issues a practice may encounter. The information contained in this game module is not intended as legal advice nor should it substitute for legal counsel. For additional information or advice specific to the needs of your organization, consult an attorney or IT professional.

continue

Cybersecure
Your Medical Practice

50
Your Score

At a conference, I learned about the importance of securing the network and hardware infrastructure in my office. I know what I should do next!

Research network security in order to select and implement the best configurations for the needs of the office.

Buy the hardware and/or software to secure your network and ask around for someone willing to do the installation.

60
Your Score

Research network security in order to select and implement the best configurations for the needs of the office.

Buy the hardware and/or software to secure your network and ask around for someone willing to do the installation.

Hire technical support to assess your current network configuration, recommend and explain upgrades/improvements, and secure your network.

Assign an office staff member to secure your network.

continue

Round 2 Week 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16





Ravi's Practical Pearls 2024

- Pearl #1 – Who is your IT specialist? Could you text them right now?
- Pearl #2 – Who backs up the data? How often? On-site or off site?
- Pearl #3 – Does your team use internet from desktops or server?
- Pearl #4 – Are all mobile devices encrypted? Wifi secure?
- Pearl #5 – How often is your security software backed up?
- Pearl #6 – Don't outsource cybersecurity!





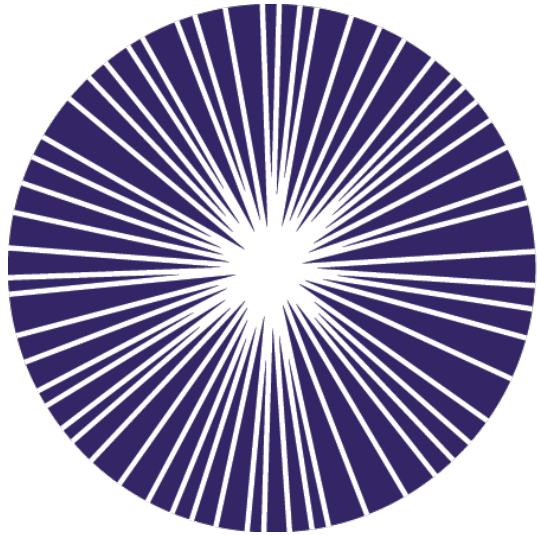
RaviGoelMD@gmail.com

 @RaviGoelMD 

www.ProtectingSight.com



AMERICAN ACADEMY™
OF OPHTHALMOLOGY



AMERICAN ACADEMY™
OF OPHTHALMOLOGY

Protecting Sight. Empowering Lives.