Protecting Your Practice From Cyber Threats

Introductions

Mohamed Yassin, MD, FAAAAI, FACAAI
Member of the Association of Certified Fraud Examiners
Allergy, Asthma, & Pulmonary Associates
Saint Cloud, MN
(320) 654-8266

Michael Rogers, MS in Cyber Security, SANS GDAT, GOSI, GCIA
Director – Technical Advisory Services at MOXFIVE
(833) 568-6695

Disclosure

Nothing to disclose

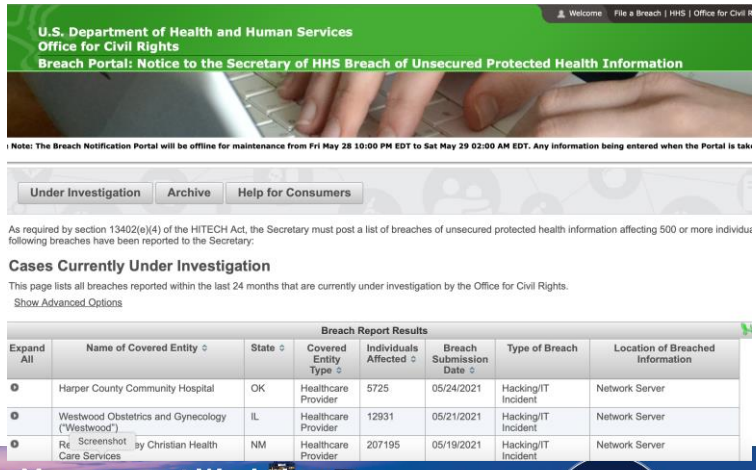
Is Cybersecurity a Threat For Medical Practices?

- YES, it is a real and imminent threat to any medical practice and hospitals
- 34% of all data breaches in 2021 were in the Healthcare Industry

  (2021 ForgeRock Consumer Identify Breach Report)
- Since 2018 Cyber Attacks are the number 1 way health records are breached

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

U.S. Department of Health and Human Services Office for Civil Rights 2021



Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

U.S. Department of Health and Human Services Office for Civil Rights 2021

	Cornerstone Municipal Advisory Group LLC dba Manquen Vance	MI	Business Associate	7018	04/02/2021	Hacking/IT Incident	Email
	Belden Inc.	MO	Health Plan	6348	04/02/2021	Hacking/IT Incident	Network Server
	Squirrel Hill Health Center	PA	Healthcare Provider	23869	04/02/2021	Hacking/IT Incident	Network Server
	Fort HealthCare Inc.	WI	Healthcare Provider	784	04/01/2021	Hacking/IT Incident	Network Server, Other
	Med-Data Incorporated	TX	Business Associate	135908	04/01/2021	Unauthorized Access/Disclo	Other
	Health Prime International	MD	Business Associate	17562	03/31/2021	Hacking/IT Incident	Network Server
	University Medical Center Southern Nevada	NV	Healthcare Provider	1833	03/31/2021	Unauthorized Access/Disclo	Network Server
	Memorial Hermann Health System	TX	Healthcare Provider	1893	03/31/2021	Unauthorized Access/Disclo	Other
	Memorial Sloan Kettering Cancer Center	NY	Healthcare Provider	18913	03/31/2021	Unauthorized Access/Disclo	Network Server
	Three Lower Counties Community Services, Inc. d/b/a Chesapeake Health Care	MD	Healthcare Provider	2505	03/31/2021	Unauthorized Access/Disclo	Other Portable Electron Device
	Epilepsy Florida	FL	Healthcare	1832	03/30/2021	Hacking/IT Incident	

(Displaying 1 - 100 of 774) 1 2 3 4 5 6 7 8 100

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

OCR (Office of Civil Rights) Data Breach Financial Penalties

- Penalties range from hundreds of thousands to millions
- Even business associates can pay millions
- Bankruptcy may not protect you from the financial penalties if any of your patients claim “potential harm”
- HIPAA Omnibus modifications grant state attorneys general the ability to bring civil action and seek damages on behalf of their residents for HIPAA violations.

Is Cybersecurity a Threat For Medical Practices?

- Now we agree Cybersecurity is a real threat how can we do and what are the best practices related to cybersecurity?

Cybersecurity Best Practices for Your Medical Practice

- Fact: you are practice is no longer “data secured” because you are practicing in a small town in North Dakota or Idaho
- Fact: your office computers via the internet are potentially accessible to any hacker from Russia, Nigeria or Timbuktu

Cybersecurity Best Practices for Your Medical Practice

- There are three parts to securing in your office:
  - Personnel (employees and business associates e.g. billing company, transcription companies, IT staff….)
  - Hardware (computer terminals, network server, firewall)
  - Software (EMR, Microsoft, WordPerfect, Financial….)

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

Cybersecurity Best Practices for Your Medical Practice

- Personnel:
- Establish policies regarding
  - Email; no employee should be allowed to open personal emails using office computers or office network on personal devices
  - Personal devices; no one should be allowed to connect personal devices "computers, tablets, smart phones, removable hard drives and USB drives,..)
  - No internet access to any site in the web for staff except purchasing department/manager
  - Good physical access controls (leaving passwords where they can easily be seen – such as on a sticky note)

Cybersecurity Best Practices for Your Medical Practice

- Personnel:
- Train your staff, update training 5-10 minutes every staff meeting at least every 4 months
- Office manager or designated staff should have HIPAA agreements with all business associates, and update yearly

Business Associate Definition

- Business Associates (BA's) are individuals or entities who ***create, receive, maintain,*** *or* ***store*** private health information on behalf of a covered entity.
- Example:

  Answering Services, Medical Transcription, IT groups, Billing companies, shredding services are clearly under the auspices of "Business Associate".

Business Associate

- The OMNIBUS Rule requires business associates to comply directly with HIPAA regulations themselves.
- BA's must now:
  - Develop policies and procedures for HIPAA – train staff
  - Conduct risk analysis
  - Be subjected to federal inspections
  - Monitor covered entities where a BA exists – have BA's with sub-contractors
  - Be subjected to the Breach Notification Rule

Cybersecurity Best Practices for Your Medical Practice

- Hardware:
  - Computers; update security upgrade and patches, anti virus software. Example: the recent government hack was successful because they had few Windows XP professional in the network (no security updates available)
  - Server; must have the most recent software version with automatic updates, virus updates
  - Very important to have the best firewall with updated firmware / software
  - Don't allow any personal computers to access the main office internet and the server
  - Make sure wireless printers are not viewable for any computer or device not part of the office network

Avoiding Risks

- Back up important files using the ***3-2-1*** rule— *create 3 backup copies on 2 different media with 1 backup in a separate location*
- Regularly update software, programs, and applications to protect against the latest vulnerabilities (especially the browser, anti- virus program, and operating system)

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

Avoiding Risks

- Access controls must be in place (i.e. who are you granting access into the system)
- Very strong password policies in place
- Business associate access controls
- Cheap anti-virus (don't do it!)
- Cheap (non-robust) firewalls (don't do it!)

Avoiding Risks

- Avoid unsecure websites
- Good physical access controls (leaving passwords where they can easily be seen – such as on a sticky note)
- Non-secured data transmissions of sensitive access controls
- Be sure to have a backup copy of your system (full image)

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

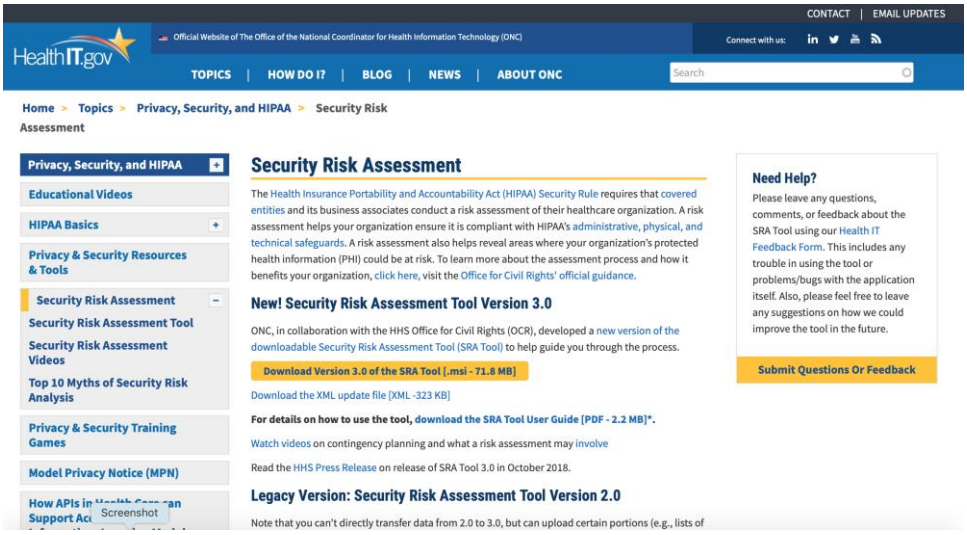
RISK ASSESSMENT

- A risk assessment is not only required by HIPAA but it's the best way problems can be found within your practice/business and the issues can be mitigated.
- There is no surefire way to do the assessment but just make sure all areas are covered.
- THE RISK ASSESSMENT IS THE FIRST THING THE FEDS WILL WANT TO SEE IN THE EVENT OF A BREACH!!
- RISK ASSESSMENT MUST BE DONE ANNUALLY (AT LEAST)

MUST CONDUCT RISK ASSESSMENT

- As quoted in from HIPAA's Security Rule (CFR) 164.308(a)(6), a covered entity is required to conduct a Risk Assessment:
  - "identify and respond to suspected or known security incidents; mitigate, to the ***extent practicable***, harmful effects of security incidents known to the covered entity; and document security incidents and their outcomes."
  - "*implement security measures sufficient to reduce risks and vulnerabilities to a* ***reasonable and appropriate*** *level to comply with 164.306 (a) [(the general requirements of the security rule)]"*
- The Risk Assessment is the building blocks for your policies and procedures. In fact, conducting a Risk Assessment is a "required" part of the HIPAA Security Rule!**

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology



Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

Responding to an Incident/Breach

Common misconceptions:

- **Recovery Time: "***The business will be back up and running within a couple days."*
- **Cyber Insurance:** "*Planning isn't required, I have insurance."*
- **Impact:** *"We can just rebuild if needed."*
- **Security Confidence:** *"We are secure because of XYZ software."*
- **Preparation/Defense Costs:** *"Cyber security is too expensive to invest in."*

MOXFIVE

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

Preparing for an Incident/Breach

1. **Backup Isolation:**
   Have the ability to isolate backups immediately.
2. **Priority Asset Listing:**
   Critical hosts identified to restore for the business.
3. **Data Governance:**
   Knowledge of where your sensitive data is stored.
4. **Communication Plan:**
   POCs of vendors, legal, insurance, and internal team members to assist with an incident.
5. **Disaster Plan:**
   If possible, have a plan that will enable you to keep the lights on while the investigation and recovery process is playing out.

MOXFIVE

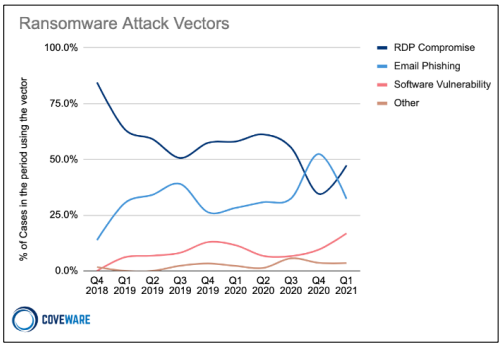
Top Recommended Actions

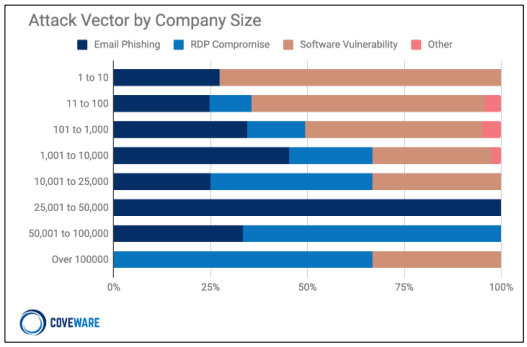
1. **Security Gap Assessment**
2. **Multi-Factor Authentication | Two Factor Authentication**
3. **Password Vaults**
4. **Security Awareness and Phishing Training/Testing**
5. **Active Directory Hardening**
6. **Unique Local Administrator Passwords**
7. **Protect Backups**
8. **EDR**

MOXFIVE

Top Threat: Ransomware

Average Ransom Payment: $220,298 (+43% from Q4 2020)





MOXFIVE

Resources

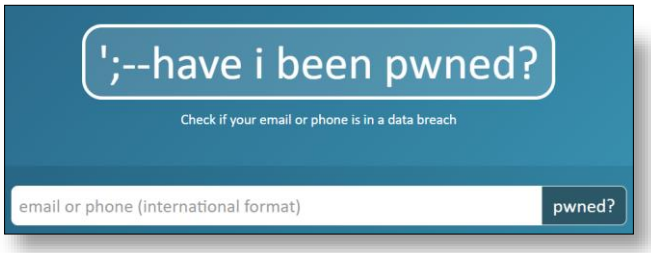
- **To build use cases and buy in leverage the following resources:**
  - **Coveware, CrowdStrike, MOXFIVE, PhishLabs Blogs and Reports**
- **General Cyber Security Resources:**
  - **Microsoft Security Compliance Toolkit 1.0**
  - **Security Technical Implementation Guides (STIGs)**
  - **NIST Check List**
  - **NSA Logging Recommendations**
  - **Center for Internet Security**

MOXFIVE

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology

Resources

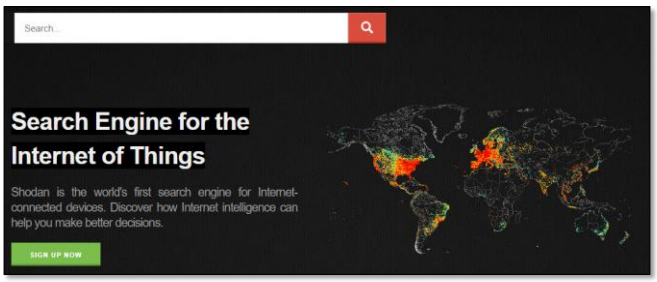
- **Quick checks:**
  - **https://haveibeenpwned.com/**



MOXFIVE

Resources

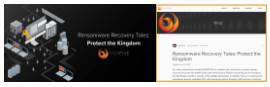
- **Quick checks:**
  - **https://www.shodan.io/**



MOXFIVE

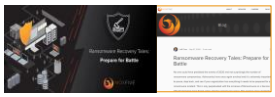
MOXFIVE Blogs

Blog: The Key to Successful Business Recovery



Blog: Ransomware Recovery Tales: Protect the Kingdom

Blog: Backups: Ahh! To Zzz



Blog: Ransomware Recovery Tales: Prepare for Battle

MOXFIVE

Closing Remarks

- The threat is real and evolving
- Being proactive is essential
- Prepare an action plan
- Leverage external resources and your community

Virtual Practice Management Workshop
JULY 23-24, 2021
Accessible, affordable, applicable
American Academy of Allergy Asthma & Immunology