THE 405(d) POST

Volume 3

A Word From the Task Group

An Ounce of Prevention: Cyber Security for the Small Medical Practice in Ten Minutes

By: Philip A. Smith, MD, FAAFP, 405(d) Task Group Member

I know you're busy. I ran my family practice office for years. So, why should you take ten minutes to read this article? Because I know what you're thinking. "Cyber Security? I have an IT person for that!" or "I don't have time!"

Funny. We used to think we didn't have time to wash our hands. Then came Pasteur and Semmelweis with that whole germ theory and hand hygiene stuff.

Maybe this is our 21st century plague…

In This Issue

Imagine being on the front page of your local paper blaring, **"Data Breach Devastates Dr. Smith's Practice".** What would be the cost... to your reputation, your patients' trust, your financial viability? There's never any mention of who manages your computer network. Your name is on the "shingle."

The Public Health Model for Cyber Security

Cyber security translates well to our medical model. Here's a quick primer.

- *There are threats to our well-being (like microbes). The most common are:*
  1. *E-mail phishing attacks*
  2. *Ransomware attacks*
  3. *Loss or theft of equipment or data*
  4. *Insider (accidental or intentional) loss of data*
  5. *Attacks against connected medical devices that may affect patient safety*
- *Vulnerabilities (like a weak immune system) make us more susceptible to these threats*
- *Our practices (like good handwashing, sanitation, and immunizations) create defenses*

Cyber security is like public health – while technology plays a role, knowledge and behavior are determinants. It is really about building a culture of awareness, prevention, and responsiveness.

Practice Owners are the Key to Prevention

It takes everyone in a practice working together to ward off the “bad actors”. Practice Owners set the stage for effectiveness. When you become the champion, everyone else will come along. You don’t have to spend a fortune to get there.

You now have the FREE resources necessary to get started: **“Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients”.** It’s available to you at: *http://www.phe.gov/405d*

After you make a quick read through the first ten pages, you will see that there are cost-effective practices that you and your staff can implement in any size practice. You won’t get it done in a day, but why not get started?

Start with raising awareness. Every member of your team plays a part in reducing your practice’s risk. Remember the teachings of Benjamin Franklin, “An ounce of prevention is worth a pound of cure.” The threats are real. The “bad actors” come from every corner of the world.

This is just another way we work together to protect the health of our nation – as you protect the health of your practice. Get started. There’s no better time than today.

HICP Spotlight

Endpoint Protection Systems

Noted as one of the 10 practices in *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, Endpoint Protection Systems can be used as a first line of defense against cyber-attacks. Endpoints are the assets the workforce uses to interface with an organization’s digital ecosystem, which include desktops, laptops, workstations, and mobile devices.

Current cyberattacks target endpoints as frequently as networks. Implementing baseline security measures on these assets provides a critical layer of threat management. With the modern workforce becoming increasingly mobile, it is essential for these assets to interface and function securely.

An effective way to ensure the safety of endpoints is to limit administrative accounts. Most users in an organization do not need to be authorized as system administrators with expanded system access and capabilities. Removing unnecessary administrative access on endpoints can mitigate the damage an attacker can cause when compromising an endpoint. Also, only authorized personnel within an organization should be allowed to install software applications. Another effective tactic, is to always ensure endpoints are properly patched. Patching (i.e., regularly updating) systems removes vulnerabilities that can be exploited by attackers. Each patch modifies a software application, rendering it more difficult for hackers to compromise programs that are aligned with the most current version of that software application. Configure endpoints to patch automatically and ensure that third-party applications (e.g., Adobe Flash) are patched as soon as possible. Lastly, it is always important to install anti-virus protection software on all endpoints in an organization. Antivirus software is readily available at low cost and is effective at protecting endpoints from computer viruses, malware, spam, and ransomware threats.

To check out more tips for Endpoint Protection access *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients here!*

Happening Around Us

Nursing Home Patients at Risk Due to Widespread Ransomware Attack

An IT Services company was hit with a Ryuk Ransomware infection affecting over 100 nursing homes in its network. The hackers are demanding $14 million and the breach is deeply impacting the nursing home's ability to access patient records which in some cases can be life threatening. One facility is reporting that they cannot put in orders for drugs for their patients which will delay patient's receiving their medication. Healthcare organizations and the third-party companies that serve them are seen as potentially lucrative targets for ransomware attackers as they may have less to spend on cybersecurity but are running mission critical services that they simply can't afford to lapse[1]. To learn more about Ransomware and the ten best practices to mitigate this threat access Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients here!

405(d) Events and Announcements!

North Carolina Department of Health and Human Services and HHS 405(d) Cybersecurity Town Hall Event 1/22/20 in Raleigh, NC!

405(d) Spotlight Webinar featuring Greater New York Hospital Association February 19th at 1pm!

Happy Birthday HICP! December 28th!

Insider Threat Targets Medical Records In Nebraska

A Hospital network in Nebraska has disclosed a data breach after a former employee accessed sensitive patient data – including medical records and Social Security numbers.

On Oct. 1, during an audit of its electronic medical record system, a Nebraska Hospital discovered that an employee had accessed patient records "outside of the employee's job responsibilities." The employee was terminated the next day. After further investigation, the company determined that the unauthorized access occurred between July 11, 2018 and Oct. 1, 2019, and that the employee was able to view some patients' medical records. The information that was viewed may have included patients' demographic information (such as name, address, date of birth, medical record number, Social Security number, license number); and clinical information, such as physician notes, laboratory results or imaging data[2]. Insider threats continue to be an issue for the Healthcare Sector, and ensuring administrative rights are limited among an organizations workforce and are continually audited for misuse is paramount to patient safety. To find out more tips on how to protect your organization from insider threats, access Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.

DHS Launches "Cyber Essentials" for Small Businesses and Small SLTT Governments

The Cybersecurity and Infrastructure Security Agency (CISA) has launched Cyber Essentials, an effort to assist small organizations in understanding and addressing cybersecurity risks. Developed in partnership with small businesses and small state, local, tribal, and territorial (SLTT) governments, Cyber Essentials aims to equip these organizations with basic steps and resources to improve their cybersecurity resilience. As many small and medium-sized provider organizations struggle with basic security mechanisms given limited resources, the guidance can prove useful for those in the healthcare sector looking for ways to close some of those gaps. The guide focuses on six key areas: driving cybersecurity strategy, investment, and culture; developing security awareness and vigilance; protecting critical assets and applications; access control; backups and avoiding critical data loss; and limiting damage and improving recovery time[3]. To access the full Cyber Essentials Click here!

HHS Ransomware Resources

HC3 Sodinokibi Ransomware Whitepaper

https://content.govdelivery.com/attachments/USDHSCIKR/2019/09/12/file_attachments/1284515/Sodinokibi-Aggressive%20Ransomwware_Whitepaper.pdf

HHS HC3 Briefing: Ransomware Threat to State and Local Governments

https://content.govdelivery.com/attachments/USDHSCIKR/2019/06/04/file_attachments/1224512/TLPWHITE_UNCLASSIFIED_20190530_State%20Local%20Gov%20Ransomware.pdf

Office for Civil Rights

HHS Office For Civil Rights Update on Preventing, Mitigating and Responding to Ransomware

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html

HHS Office For Civil Rights Ransomware Guidance

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

HHS Office for Civil Rights Cyber Attack Check-List and Response Infographic

https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif

HAPPY BIRTHDAY, HICP!

HELP US CELEBRATE THE FIRST YEAR OF HEALTH INDUSTRY CYBERSECURITY PRACTICES: MANAGING THREATS & PROTECTING PATIENTS BY CONTINUING TO SPREAD AWARENESS, SHARING THE PUBLICATION, AND FOLLOWING US ON SOCIAL MEDIA!

WE WOULD ALSO LIKE TO THANK EVERYONE INVOLVED IN THE 405(D) PROGRAM FOR AN OUTSTANDING YEAR.

Introducing 405(d) Social Media!

The 405(d) Program is taking our mission of aligning healthcare security approaches to Twitter, Facebook, and Instagram! Follow Us, the 405(d) initiative @Ask405d to learn about cybersecurity best practices and the five main cybersecurity threats, plus upcoming events and engagements.

Check us out!

Verizon
22:47
405(d)
3,959
8,936
443
Follow
Health and Human Services 405(d) Initiative
"Cyber Safety is Patient Safety"
405d.hhs.gov

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Contact Us!

www.405d.hhs.gov

CISA405d@hhs.gov

[1] https://www.infosecurity-magazine.com/news/nursing-home-patients-risk/l

[2] https://threatpost.com/nebraska-medicine-breached-rogue-employee/150823/

[3] https://www.cisa.gov/cisa/news/2019/11/06/cisa-releases-cyber-essentials-small-businesses-and-governments

*DISCLAIMER: This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The news articles represented in this newsletter are chosen at random to foster awareness and are not in promotion of any news organization. The "A Word from the Task Group" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter.