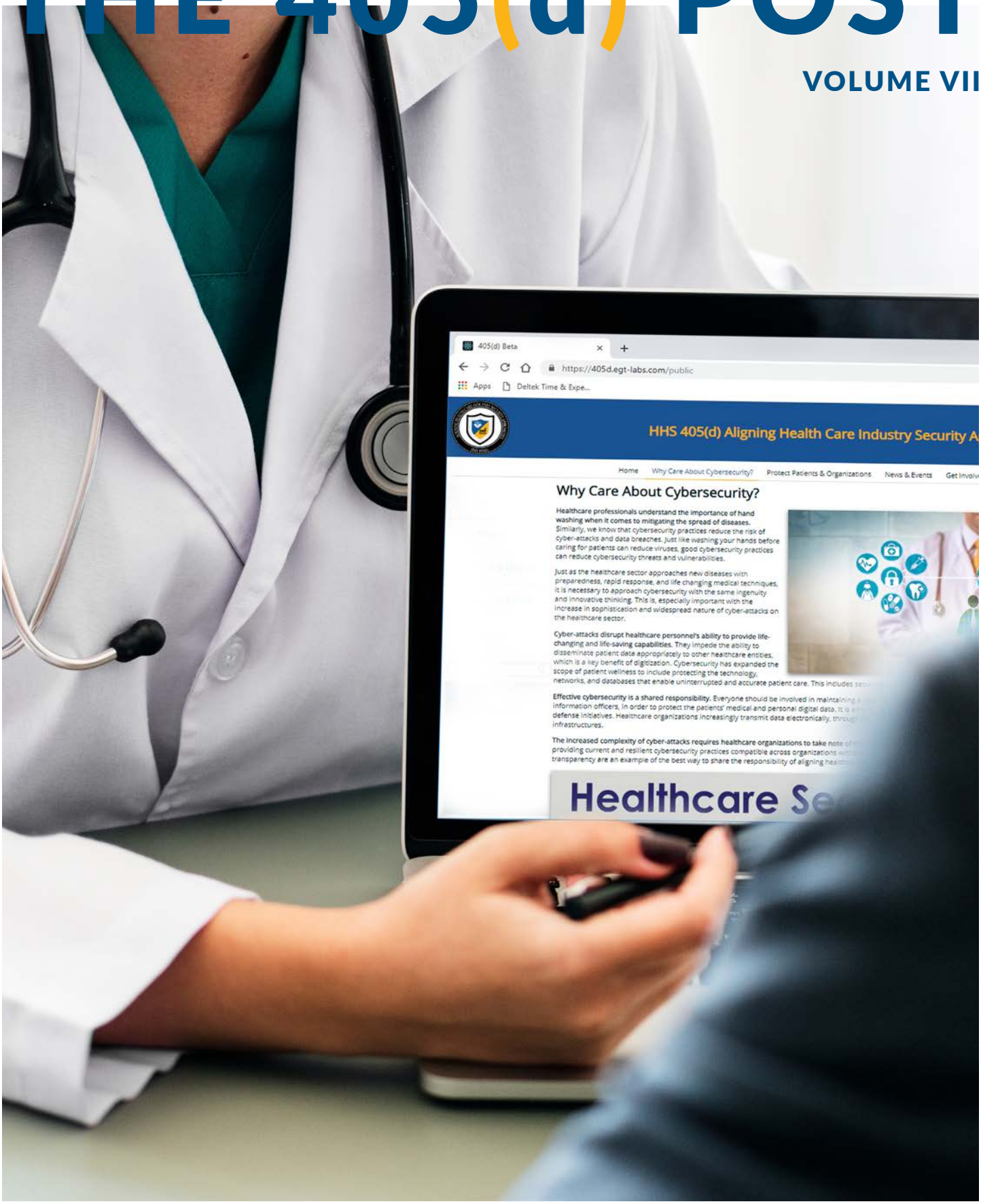
THE 405(d) POST

VOLUME VII



HHS 405(d)
Aligning Health Care
Industry Security Approaches

Why Providers Should Care About Cybersecurity

By Mark Jarett, MD, MBA, MS405(d) Task Group Member

Providers are inundated with rules, regulations, laws, and other external competing requirements that often compromise their time and abilities in trying to deliver care in a safe and timely fashion. Concerns about cybersecurity are thus often relegated to the worlds of compliance and *"it won't happen to me."* In addition, there is a whole lexicon of cybersecurity terms that make it difficult for non-technically oriented providers to understand what warnings may mean. Unfortunately, providers must not only be aware of cybersecurity issues, they must practice cyber hygiene, applying cyber 'universal precautions' just as they do when caring for patients. The risk is two-fold; to patients with their security risks, and to providers, because compromised personal information can affect their personal lives and cause harm to their practice.

Providers don't distribute the keys to their house, or their alarm code, to strangers. The same concepts apply to the patient care environment. **In the U.S. over 89% of people wear seatbelts, but less than 28% use multi factor authentication.** The healthcare sector, like other critical infrastructure sectors that have become electronically dependent, is now exposed to multiple bad actors and groups that can pick the lock and unlock the door. There is a diversity of potential exploiters from teenagers who see hacking as a fun challenge and nation states which commit espionage, whether industrial or on the basis of a cyber attack. The recent reports of hacking of COVID-19 vaccine research is a prime example of the latter. In between these groups are criminals who want to make money by acquiring and then selling information, as well as hackers who may want to cause harm to patients. The final group can be terrorists who also use hacking as a means to cause damage or harm.

No provider comes to work wanting to harm a patient. So you, as a provider, might ask: *What can be the harmful impact to a patient of a breach in security?* The most obvious one is the loss of personal identifiable information (PII). Providers collect a large amount of PII and personal health information (PHI) both for patient care and for billing purposes. *On the dark web PHI is actually worth three times that of PII.* A breach of the office system will make PII and PHI available to criminals for credit card fraud and stealing the patient's identity to obtain healthcare. The latter can result in a patient incurring copays and having wrong information in their medical record. *This will impact the care they receive in the future and prevent them from obtaining insurance.* Hacking can also produce changes to the medical record

such as deleting allergy information or critical past medical history. If the PHI contains sensitive information that is made public, it can embarrass a patient or be used for extortion.
Finally, if the provider is using Wi-Fi/internet connected equipment for treatment, the settings can be changed delivering wrong doses of medication or even radiation.

Poor cyber hygiene can also result in a ransomware attack, usually through phishing emails as entry links into the system. They will lock all of the patient information making it inaccessible unless you pay a ransom. *Remember, it may not be your system that is attacked, but one of your business associates, such as a billing company, that will let them inside your firewall.* Finally, denial of service attacks can bring down the internet. Having "go-to-paper" emergency procedures and system back ups will help allow continuity of care.

Bad actors not only cause financial harm, but actually cause physical harm to patients. A hacker, or someone who has just stolen password access to the EHR, can change orders on medications. This can result in patients receiving wrong dosages or fatal combinations of drugs. Hacking into a linear accelerator can result in dosages of radiation that can deliver a lethal dose to a patient. Hacking of a WiFi network, especially when the username is admin and the password is admin1, can take over an infusion pump and deliver a fatal dosage of medication. These seem almost like from a spy thriller, or the TV show 24, but have been proven to be real possibilities (Healthcare Finance News).

These threats not only affect patients, but also can bleed into the providers life. Insurance companies have a host of personal information on the provider from tax ID numbers to social security numbers. An attack on a billing system may result in cyber fraud that compromises the provider's identity. Lack of proper cyber hygiene can result in both regulatory and personal liability exposure with fines, sanctions, and civil lawsuits.

Therefore, when you are told to use complex passwords, and not keep them under your keyboard, please listen. Most cyber-attacks are due to insider actions. It can be nefarious behavior, such as selling information, or due to human error, such phishing or social engineering. Your staff must be trained to follow the same safe practices as you do. Check and audit what they do. We all want and expect the same protection of our information as we do for our physical safety.

Conclusion

One resource that can be useful to both physicians and IT professionals is the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients Publication.* This document lays out the top 5 cybersecurity threats facing the industry and the top 10 practices to mitigate them. It is also useful in that is was written for all audiences of the healthcare in mind: IT and Non-IT.

Above all, cyber hygiene is a patient safety tool that we all must adopt. All providers have the same essential mandate: Primum non nocere- First do no harm. For years we have understood this to be as our interaction with patients, but what we must realize is cybersecurity is now part of our practice- and our experience with our patients. This requires an active process of protecting the PII and PHI of our patients in every electronic exchange in which we are involved. Doing this will ultimately protect our patients and will also protect ourselves.

HEALTH INDUSTRY CYBERSECURITY PRACTICES:
Managing Threats and Protecting Patients

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication aims to raise awareness, provide vetted cybersecurity practices, and moves toward consistency in mitigating the current most pertinent cybersecurity threats to the sector. The main document examines cybersecurity threats and vulnerabilities that affect the health industry. Technical volumes 1 & 2 discuss ten cybersecurity practices for small, medium and large healthcare organizations. Lastly the resources and templates volume provides additional cybersecurity resources and references. **CLICK HERE TO DOWLOAD DOCUMENTS!**

405(d) In the Spotlight

In the past year the 405(d) Program has grown its reach and continues to pursue its mission of Aligning Healthcare Industry Security Approaches. The 405(d) program is now able to assist in many of your cybersecurity needs. Whether it is instituting cybersecurity practices using HICP, or educating your staff on cybersecurity, we are here for you! Check out the list below of the many different ways you can utilize the 405(d) Program and its available resources!

405(d) Awareness Materials

Need cybersecurity awareness posters for your organization? We've got you covered! The 405(d) Program creates cyber awareness products year round in the hopes we can provide you with a rotating assortment of cybersecurity tips and best practices that you can share with your staff. Our uniquely crafted cybersecurity awareness posters and materials are designed with you in mind and can be used as posters, email blasts, or print outs.

405(d) Guest Webinars

Does your organization have a standing webinar series that is missing a cybersecurity element? The 405(d) Program will come to you! The 405(d) Program will curate a webinar specifically for your organization's cybersecurity needs and invite other federal partners where appropriate to help educate and inform your workforce on cybersecurity issues.

405(d) Social Media

Looking for ways to stay up to date on the latest 405(d) cybersecurity topics and products? We are now active on Instagram, Facebook, and Twitter at @ask405d! Our Social Media accounts highlight new 405(d) awareness products and also provide cybersecurity best practices and tips that you can use in your organization. To stay connected have your organization follow us and re-share our content with your employees!

405(d) Spotlight Webinar

Interested in learning more from industry about cybersecurity? The 405(d) Spotlight Webinar spotlights a new topic and Task Group Member each time and they produce content based on insight on how their organizations have used the HICP publication, real-world scenarios and lessons learned, industry cybersecurity best practices, proven cybersecurity procedures and techniques, and other topics involving cybersecurity in the healthcare industry.

Happening Around Us

Cybercriminals Exploited COVID-19

Microsoft

Microsoft released a study depicting how cybercriminals behaved during the first few months of the COVID-19 outbreak. Worldwide, Microsoft observed COVID-19 themed attacks peaked in the first two weeks of March. That coincided with many nations beginning to take action to reduce the spread of the virus and travel restrictions coming into effect. By the end of March, every country in the world had seen at least one COVID-19 themed attack. The COVID-19 outbreak has truly been a global event. Cybercriminals have taken advantage of the crisis to lure new victims using existing malware threats. In examining the telemetry, these attacks appear to be highly correlated to local interest and news. Overall, COVID-19 themed attacks are just a small percentage of the overall threats that Microsoft has observed over those first four months. To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

COVID-19 Home Monitoring Tools Pose Patient Privacy, Safety Risks

Health IT Security

HealthITSecurity reports a study published in Nature Medicine reveals potential risks caused by the rapid adoption of home monitoring tools in light of COVID-19, including risks to patient privacy and safety. The COVID-19 pandemic spurred the rapid adoption of remote patient monitoring tools to support patient care in light of social distancing needs. But the accelerated development of these technologies potentially increased risks to patient safety and privacy, among other regulatory concerns. Published in Nature Medicine, a group of Harvard University researchers assessed the adoption of these home monitoring technologies amid the pandemic and needed interventions to ensure patient safety and compliance with regulatory requirements, privacy laws, and Emergency Use Authorizations (EUAs). Privacy concerns are prevalent with home monitoring technologies as they collect health-related data and require adequate security to ensure

autonomy and maintain trust. Researchers stressed that without trust, patients won't use these crucial platforms. "The rapid development of new products also poses challenges ranging from safety and liability to privacy," they concluded. "The motto 'ethics by design, even in a pandemic' should guide makers in the development of home monitoring products to combat this public-health emergency." To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

Researcher Discovers Healthcare Info of 3.1M Patients Online

Becker's Health IT

Becker Hospital Review reports that Security researcher Bob Dianchenko discovered millions of peoples' healthcare data available online. A medical software company's database containing the personal information of more than 3.1 million patients was left exposed online without the need for a password or other authorization. The database appears to be owned by a vendor specializing in online booking and patient management software for medical and dental practices. The database contained full patient names, email addresses, contact information, marital statuses, sex, and practice names: all of which can be used by cybercriminals in targeted phishing attempts to gain more information for later fraud or to scam patients. What's more concerning is that the data was destroyed 10 days later on July 22 and could have potentially been stolen by a malicious bot known as "meow bot." The database contained information for a host of companies, and involved analytics reports, internal presentations, client requests, business intelligence, and mailing list with relevant personally identifiable information, among other sensitive details. More research is being done to understand the reach of this breach. To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

405(d) Events and Announcements!

National Cybersecurity Awareness Month!
This October is National Cybersecurity Awareness Month and to celebrate the 405(d) Program will be developing a series of awareness materials and events that individuals in all areas of an organization can utlize. Keep a look out for our kick-off on October 1st and Do Your Part #BeCyberSmart!

405(d) Spotlight Webinar: - NCSAM Edition! October 22nd at 2pm EST
Guest speakers include representatives from: Cybersecurity and Infrastructure Security Agency (CISA), Health Sector Coordinating Council (HSCC) Health Sector Cybersecuity Coordination Center (HC3) and More!

Additional Resources

CISA Guidance on Essential Critical Infrastructure Workers

Risk Management for COVID-19

CISA Telework Guidance and Resources Webpage

HC3 Website Announcement!

In an effort to address cybersecurity threats to the sector, reach a wider audience, and to facilitate large scale knowledge sharing, the HC3 has developed a website that is an asset to the sector and beyond. Check it out! http://www.hhs.gov/hc3

Happening Around Us Sources

1. Microsoft
2. Health IT Security
3. Becker's Health IT

About The 405(d) Post
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.

Need To Contact Us? Email us at cisa405d@hhs.gov