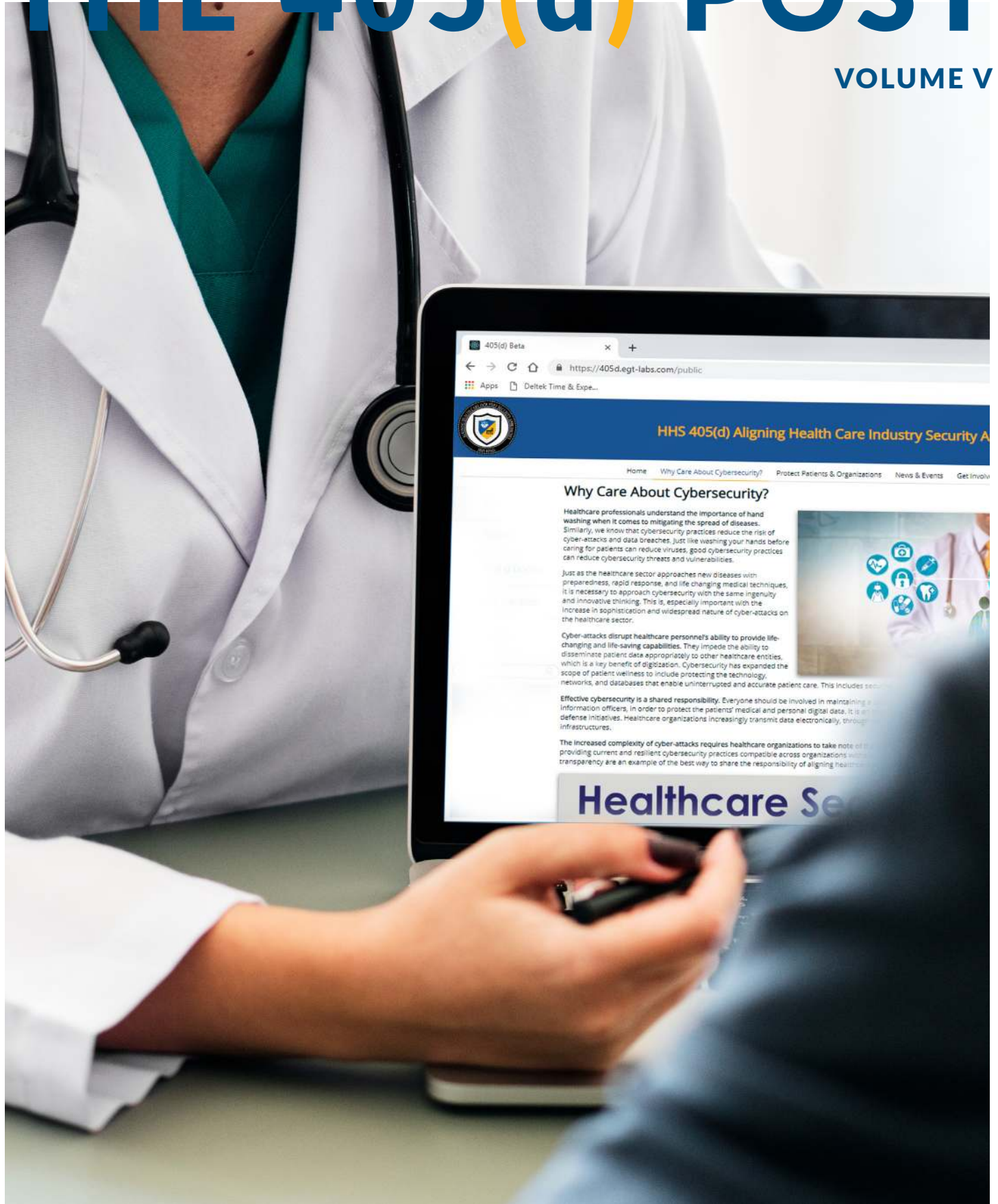


THE 405(d) POST

VOLUME V



HHS 405(d)
Aligning Health Care
Industry Security Approaches



Telework During COVID-19 Good Practices To Protect From Cyberattacks

By Sekar Thanigaimani, 405(d) Task Group Member

As the COVID-19 pandemic spreads around the world, the World Health Organization (WHO) has made the suggestion that organizations introduce more teleworking. Many organizations are considering work from home options to reduce the risk of their staff getting infected. Typically, when employees are working inside the corporate network, the enterprise security team can monitor and protect them. But working from home exposes the employee's devices and through them, the organization's network to various threats.

Attackers are taking advantage of the fact that many employees who are working from home have not applied the same security on their own networks that would be in place in a corporate environment. There have been multiple cases of malicious COVID-19 mobile applications and malicious emails that give attackers potential access to data or the ability to encrypt devices for ransom. Organizations should continue to assess the security controls in the context of telework which can include: implementation of single sign-on, multi-factor authentication, encryption of data, protecting the home Wifi network, VPN to connect to the organization's network, and monitoring and applying security patches regularly. However, there are ways to protect and mitigate risks from cyberattacks using the Health Industry Cybersecurity Practices (HICP) Publication. HICP focuses on five threats and ten best practices that help organizations improve the strength of their security controls.

The two things I like most about the HICP framework is that, it is designed to be used by healthcare organizations of all sizes (small to large enterprises), and the best practices are documented at a granular level which serve as an easy tool for a quick assessment which helps organizations improve their security posture. For example, "Deploy multifactor authentication (MFA) before enabling access to your e-mail system. MFA prevents hackers who have obtained a legitimate user's credentials from accessing your system". I was able to do a quick assessment using HICP and implement the recommended best practices.



HICP calls out ten best practices that an organization can implement to mitigate cybersecurity risks

In the current situation of COVID-19, organizations should pay attention to the following Key Practices immediately and focus on the other HICP Practices as well:

Cybersecurity Policies:

It is important for the organization to publish and spread awareness on teleworking policies and all associated policies and governance with their employees. In addition, performing an assessment with reference to the ten practices published by HICP would help organizations understand the current strength of controls and mitigate the risks accordingly.

Access Management:

Organizations should implement virtual “check-in” and check-out” from the location where the employee is working and connecting to the organization’s network through a VPN. Organizations may also enforce two-factor authentication across all assets and for all employees. Security functions should monitor the network traffic that comes from different locations outside of the locations that are registered through virtual check-in.

Asset Management:

Organizations should consider implementation of virtual desktop as part of an overall IT strategy. Sensitive company data including PHI / PII data stored on laptops, desktops, and mobile devices can be lost or stolen very easily. With Virtual Desktop Infrastructures (VDIs), the data is stored in a centralized environment and antivirus and malware software status updates are easier to do and track. In the absence of a VDI





environment, organizations should implement a centralized tool for managing security vulnerabilities to mitigate risks.

Virtual tools:

Use of organization-authorized cloud-based collaboration tools, such as video conferencing, call, chat, white board, emails, word processing software, project management tools and timesheet etc., help organizations mitigate the risks and threats related to vulnerabilities.

Conclusion

Cybercriminals are seeking to exploit this COVID-19 situation to target organizations and employees. It is important for organizations to perform a comprehensive risk assessment for their employees that work from home or other remote locations and mitigate the risks to protect patient data. To this, the HICP publication is a great place to start. If you have questions you can reach out to the 405(d) Team at cisa405d@hhs.gov

Click Below to Download a Copy of Each Technical Volume

TECHNICAL VOLUME I
PRACTICES FOR SMALL ORGANIZATIONS

TECHNICAL VOLUME II
PRACTICES FOR MEDIUM & LARGE ORGANIZATIONS

Equipment
Many cybercriminals gain access to healthcare organizations through stolen or lost laptops, phones, tablets and other equipment. Always encrypt sensitive data on your devices and immediately report to your IT department if your equipment is missing!

Passwords
Passwords are the gateway to your organization's network and connectivity. Use strong passwords for your work and personal accounts and change default passwords for equipment and network access to keep your patients safe. Always use different passwords that don't contain personal identifiers.

KEEP A BALANCED CYBERSECURITY DIET!
Just as it is important to have a balanced diet it is also important to have a balanced cybersecurity approach in order to protect your patients from all cyber-threats. Have questions? Checkout HICP!

Email Protection
Most Ransomware attacks begin with Email Phishing, therefore, always remember to double check the sender of an email and check hyperlinks by hovering your mouse over them to show the web address prior to clicking

Network Protection
Cyber-attacks on healthcare organization's networks cause serious impact to patient care. Always ensure you are using your organization's Virtual Private Network (VPN) when accessing patient data from home or at the office!

HHS 405(d)
Aligning Health Care Industry Security Approaches

For more information on how to keep a balanced cyber diet check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication to learn about the top 5 threats facing the healthcare industry and ten practices to mitigate them!

10 WAYS TO PROTECT YOUR PATIENTS FROM CYBER THREATS

Cyber-attacks are on the rise in the healthcare industry and it is up to us to keep our patients safe. Being cyber prepared is everyone's responsibility, and to get started, check out the below ten best practices to ensure you are keeping your patients safe!

- 1. SECURE YOUR DATA**
Encrypt sensitive data on all devices, including laptops, tablets, and smartphones. Use strong encryption and protect keys.
- 2. SECURE YOUR NETWORKS**
Use firewalls and intrusion detection/prevention systems. Segment networks to limit the impact of a breach.
- 3. SECURE YOUR DEVICES**
Use mobile device management (MDM) to enforce security policies on all devices. Lock devices and wipe data if lost or stolen.
- 4. SECURE YOUR APPLICATIONS**
Use secure coding practices and conduct regular security testing. Patch vulnerabilities promptly.
- 5. SECURE YOUR SUPPLY CHAIN**
Verify the security of third-party vendors and their products. Conduct regular security assessments.
- 6. SECURE YOUR PHYSICAL ACCESS**
Restrict physical access to servers and networks. Use biometric authentication for sensitive areas.
- 7. SECURE YOUR HUMAN ELEMENT**
Conduct regular security awareness training. Implement phishing simulations.
- 8. SECURE YOUR INCIDENT RESPONSE**
Develop and test an incident response plan. Establish clear roles and responsibilities.
- 9. SECURE YOUR BUSINESS CONTINUITY**
Develop and test a business continuity plan. Ensure critical services can be restored quickly.
- 10. SECURE YOUR COMPLIANCE**
Stay up-to-date on regulatory requirements. Conduct regular audits and assessments.

To best protect your patients, always be in the know of your organization's cybersecurity posture. To learn more contact your cybersecurity professional.

HHS 405(d)
Aligning Health Care Industry Security Approaches

5 TIPS TO CREATE A CYBER SAFE CULTURE

Creating a cyber-safe culture in your organization can prevent serious cyber-attacks that have the potential to shut down care facilities. When we are informed and change our thinking, we ultimately will continue to keep our patients safe.

Creating a cyber-safe culture starts with you! Check out the five tips to create a cyber-safe culture in your organization!

- 1. MAKE THE CYBER THREATS REAL**
Cybersecurity practice reduces the risk of cyber-attacks and data breaches, but we are able to protect our patients from infection, we should work towards protecting patient data to allow physicians and caregivers to treat the patients that enable delivery of quality health care.
- 2. DON'T GUESS AT CHECKING IT**
Email phishing is the number one way that cyber-attacks occur. Always be sure to verify the sender and check hyperlinks before you click them.
- 3. PROTECT YOUR PATIENTS FIRST**
If you never lose an easy thing to do, the best always remember protecting a patient's PHI is also keeping them safe. Be sure to follow your organization's protocols when dealing with patient data, and use the appropriate protections when sending information to other parties.
- 4. MAKE THE RESPONSIBILITY OF CYBERSECURITY Cybersecurity is a shared responsibility, not just an IT issue. Be proactive and work with your IT professionals by sharing responsible activities to a third facility. You are the gateway to your organization and it is important to help your IT team help you, which ultimately protects patients!**
- 5. LEARN YOUR ORGANIZATION'S CYBER PROTOCOLS**
Be an example to your fellow employees and learn your organization's cyber protocols. The best way to combat cyber-attacks is to stay vigilant and ensure everyone in your organization is aware and informed on cybersecurity protocols.

Everyone plays an important role in keeping our patients safe from cyber threats. To learn more about the top five cybersecurity issues facing the healthcare industry and practices you can use to mitigate them, check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication!

HHS 405(d)
Aligning Health Care Industry Security Approaches



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's instituting a cybersecurity risk management structure 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. Check out the examples above!

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

COVID-19 Ransomware Attacks on Healthcare Providers Escalating

HEALTH IT SECURITY NEWS

HealthIT Security reports that Hospitals and other healthcare providers are increasingly being targeted with ransomware attacks amid the COVID-19 pandemic, according to Interpol. The news comes as the FBI alerts all sectors to an expected increase in business email compromise schemes tied to the crisis. According to Interpol's data, the ransomware is primarily spreading through emails that frequently claim to contain information or advice about the Coronavirus from a government agency. US Federal agencies have also recently reported a surge in fraud schemes related to COVID-19. Interpol is currently collecting a list of suspicious Internet domains related to the pandemic, which it will analyze in order to work with relevant countries to take action against the threat.¹ To learn more about how to use mitigating practices to mitigate these threats check out [The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients \(HICP\) Publication](#).



DHS Urges VPN Cybersecurity Best Practices due to COVID-19

[CYBER INFRASTRUCTURE SECURITY AGENCY](#)

Due to the increase in remote work due to COVID-19, The Department of Homeland Security Cybersecurity and Infrastructure Security Agency is urging strong Virtual Private Networks (VPN) protections to mitigate heightened cyber-risks for all organizations. VPNs offer secure remote access to internal networks like databases and are used in healthcare to remotely access and electronically share health data. DHS urges ensuring your organization performs the necessary patches to ensure your VPN is up to date. Another mitigation practice DHS suggests is to inform your employees of increased phishing emails.² To learn more about how to strengthen your VPN and cybersecurity Posture check out [The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients \(HICP\) Publication](#).



Detroit Hospital Network Announces Data Breach

[CYBERSCOOP](#)

Cyberscoop reports a Detroit-area health care organization is alerting patients that their information may have been compromised in a recent data breach. Beaumont Health, a network of eight hospitals throughout the Detroit area, said in a letter Friday that “an unauthorized third party” accessed names, birth dates, Social Security numbers and medical conditions about some 112,000 people. Hackers also accessed bank account data and driver’s license numbers about some of those affected. The incident involves information about less than 5% of the 2.3 million people that the medical organization has treated in the nearly 12 months since the attack occurred, according to Beaumont. The attack against the hospital network occurred months before U.S. facilities started responding to the COVID-19 pandemic. Word of the breach coincides with ongoing concern in the security community about the particular vulnerability of the global medical

sector. As health care workers rush to treat patients affected by the novel coronavirus, opportunistic hackers have sought to capitalize on the urgency by targeting hospitals, sometimes demanding extortion fees to back down.³ To learn more about how to use mitigating practices to mitigate these threats check out [The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients \(HICP\) Publication](#).

405(d) Events and Announcements!



405(d) Spotlight Webinar: Healthcare Cybersecurity: Stay One Step Ahead of the Hackers
June 17 at 1:00 pm

Spring Campaign still ongoing!

Additional Resources



[Fake Online Coronavirus Map Alert](#)

[Access Control for Health Information Systems](#)

[Citric Vulnerabilities and APT 41 Whitepaper](#)



[Telehealth Remote Communications Guidance](#)

Happening Around Us Sources

1. [HEALTH IT SECURITY NEWS](#)
2. [CYBER INFRASTRUCTURE SECURITY AGENCY](#)
3. [CYBERSCOOP](#)

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 or visit our website at 405d.hhs.gov!