405(d) Spotlight Webinar

Aligning Health Care Industry Security Approaches

The Internet of Medical Things: Making Them Secure

Mark Jarrett MD, MBA, MS
Chief Quality Officer
Deputy Chief Medical Officer
Northwell Health

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) Task Group member; each iteration does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.

* This Webinar is being recorded and will be available for future viewing

405(d) Events and Announcements

- **July**
  - Continuation of 405(d) Spring Campaign
  - 405(d) Post 7/22
- **August**
  - Spotlight Webinar 8/12 - “Healthcare’s Enterprise Cyber Risk Management Imperative”

Email: CISA405d@hhs.gov

Agenda

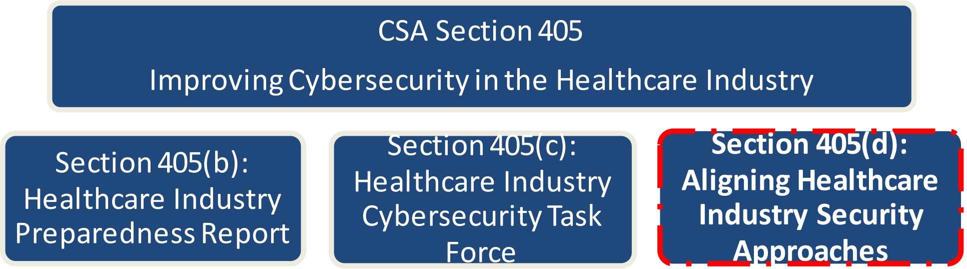
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Julie Chua, HHS
30 Minutes	The Internet of Medical Things: Making Them Secure	Mark Jarrett
15 Minutes	Q&A	All
5 Minutes	Closing	405(d) Team

Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of "Aligning Health Industry Security Approaches" by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



CSA Section 405

Improving Cybersecurity in the Healthcare Industry

Section 405(b): Healthcare Industry Preparedness Report

Section 405(c): Healthcare Industry Cybersecurity Task Force

Section 405(d): Aligning Healthcare Industry Security Approaches

405(d) Resources

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released over 50 awareness products which organizations across the HPH sector can leverage

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, The 405(d) Post, and Spotlight Webinars to increase cybersecurity awareness and present on new and emerging cybersecurity news and topics, as well highlighting the HICP Publication!

CYBERSECURITY TOWN HALL EVENT

October 22-23

PATIENTS TRUST US WITH THEIR LIVES, BUT DO WE PROTECT THEM FROM CYBER THREATS?

Join UChicago Medicine and United States Health and Human Services 405(d) to discuss the five main cybersecurity threats facing the healthcare industry and leading practices to mitigate them.

Town Hall Events:
Practitioners and Practice Managers:
10/22/19 1:30pm-3:00pm
10/23/19 9:00am-10:30am

IT Professionals:
10/22/19 3:30pm-5:00pm
10/23/19 11:00am-12:30pm

405(d) Social Media

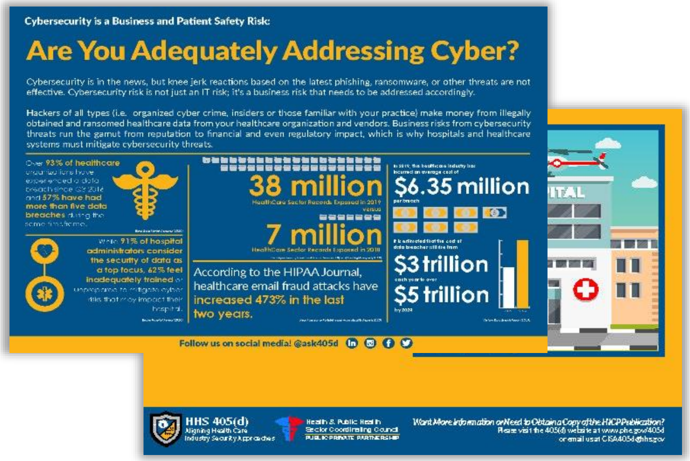
The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

NEW RESOURCES ALERT

405(d) "That Seems Risky" Campaign

405(d) Cybersecurity "Myth vs. Fact" Campaign

Resources from the Task Group



Cybersecurity is a Business and Patient Safety Risk:

Are You Adequately Addressing Cyber?

Cybersecurity is in the news, but knee jerk reactions based on the latest phishing, ransomware, or other threats are not effective. Cybersecurity risk is not just an IT risk; it's a business risk that needs to be addressed accordingly.

Hackers of all types (i.e. organized cyber crime, insiders or those familiar with your practice) make money from illegally obtained and ransomed healthcare data from your healthcare organization and vendors. Business risks from cybersecurity threats run the gamut from reputation to financial and even regulatory impact, which is why hospitals and healthcare systems must mitigate cybersecurity threats.

Over 93% of healthcare organizations have experienced a data breach since Q3 2016 and 57% have had more than five data breaches during the same timeframe.

While 91% of hospital administrators consider the security of data as a top focus, 62% feel inadequately trained or unprepared to mitigate cyber risks that may impact their hospital.

38 million HealthCare Sector Records Exposed in 2019 versus 7 million HealthCare Sector Records Exposed in 2018

According to the HIPAA Journal, healthcare email fraud attacks have increased 473% in the last two years.

In 2019, the healthcare industry has incurred an average cost of $6.35 million per breach

It is estimated that the cost of data breaches will rise from $3 trillion each year to over $5 trillion by 2024

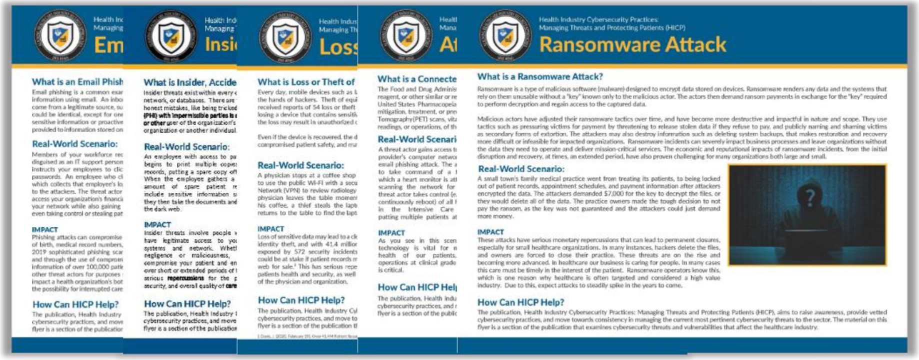
Follow us on social media! @ask405d

HHS 405(d) Aligning Health Care Industry Security Approaches

Health & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

Want More Information or Need to Obtain a Copy of the HICP Publication?
Please visit the 405(d) website at www.phe.gov/405d
or email us at CISA405d@hhs.gov

Small, Medium and Large Executive Cards



Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients (HICP)

Ransomware Attack

What is a Ransomware Attack?

Ransomware is a type of malicious software (malware) designed to encrypt data stored on devices. Ransomware renders any data and the systems that rely on them unusable without a "key" known only to the malicious actor. The actors then demand ransom payments in exchange for the "key" required to perform decryption and regain access to the captured data.

Malicious actors have adjusted their ransomware tactics over time, and have become more destructive and impactful in nature and scope. They use tactics such as pressuring victims for payment by threatening to release stolen data if they refuse to pay, and publicly naming and shaming victims as secondary forms of extortion. The attackers may also destroy information such as deleting system backups, that makes restoration and recovery more difficult or infeasible for impacted organizations. Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The economic and reputational impacts of ransomware incidents, from the initial disruption and recovery, at times, an extended period, have also proven challenging for many organizations both large and small.

Real-World Scenario:

A small town's family medical practice went from treating its patients, to being locked out of patient records, appointment schedules, and payment information after attackers encrypted the data. The attackers demanded $7,000 for the key to decrypt the files, or they would delete all of the data. The practice owners made the tough decision to not pay the ransom, as the key was not guaranteed and the attackers could just demand more money.

IMPACT

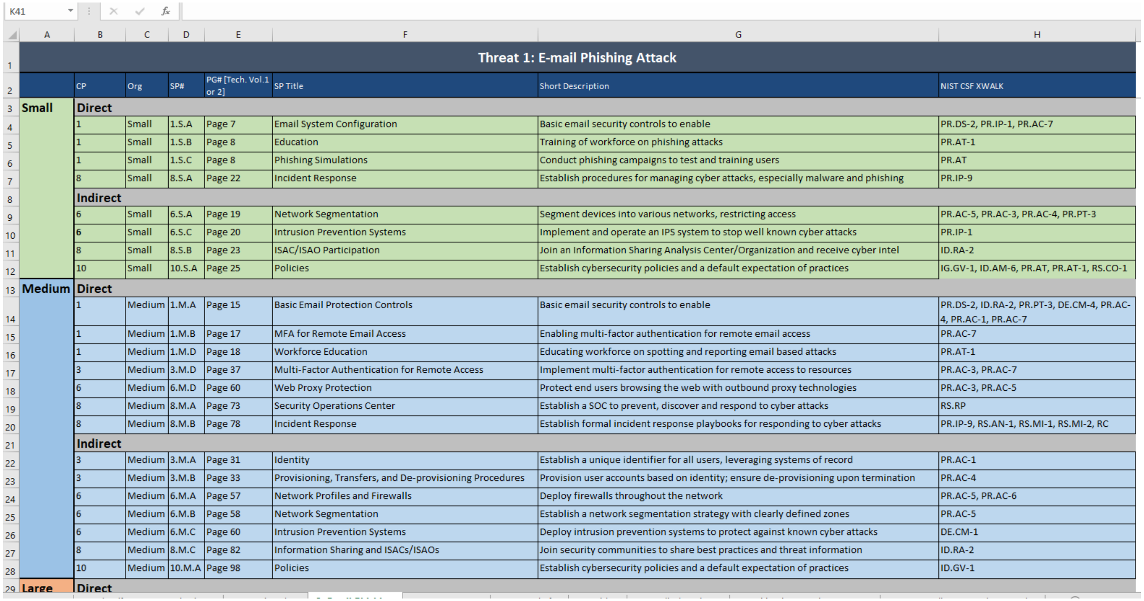
These attacks have serious monetary repercussions that can lead to permanent closures, especially for small healthcare organizations. In many instances, hackers delete the files, and owners are forced to close their practice. These threats are on the rise and becoming more advanced. In healthcare our business is caring for people. In many cases this care must be timely in the interest of the patient. Ransomware operators know this, which is one reason why healthcare is often targeted and considered a high value industry. Due to this, expect attacks to steadily spike in the years to come.

How Can HICP Help?

The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector. The material on this flyer is a section of the publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.

Five Threat Flyers

Threat Mitigation Matrix



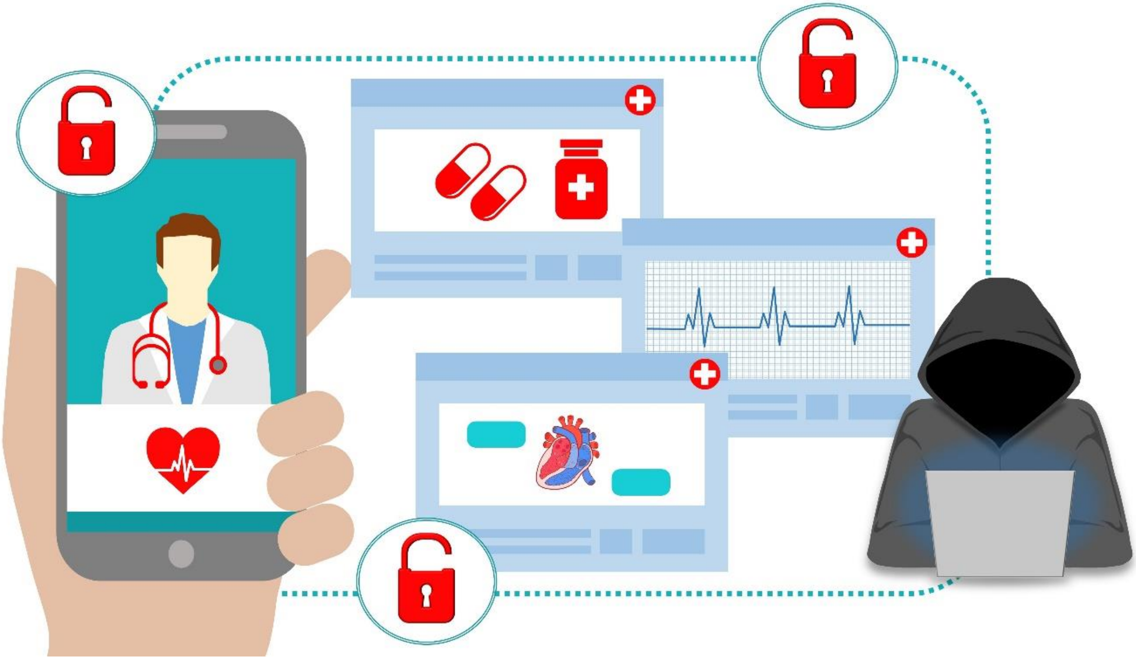
Threat 1: E-mail Phishing Attack

	CP	Org	SP#	PG# [Tech. Vol.1 or 2]	SP Title	Short Description	NIST CSF XWALK
Small	**Direct**						
	1	Small	1.S.A	Page 7	Email System Configuration	Basic email security controls to enable	PR.DS-2, PR.IP-1, PR.AC-7
	1	Small	1.S.B	Page 8	Education	Training of workforce on phishing attacks	PR.AT-1
	1	Small	1.S.C	Page 8	Phishing Simulations	Conduct phishing campaigns to test and training users	PR.AT
	8	Small	8.S.A	Page 22	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-9
	Indirect						
	6	Small	6.S.A	Page 19	Network Segmentation	Segment devices into various networks, restricting access	PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3
	6	Small	6.S.C	Page 20	Intrusion Prevention Systems	Implement and operate an IPS system to stop well known cyber attacks	PR.IP-1
	8	Small	8.S.B	Page 23	ISAC/ISAO Participation	Join an Information Sharing Analysis Center/Organization and receive cyber intel	ID.RA-2
	10	Small	10.S.A	Page 25	Policies	Establish cybersecurity policies and a default expectation of practices	IG.GV-1, ID.AM-6, PR.AT, PR.AT-1, RS.CO-1
Medium	**Direct**						
	1	Medium	1.M.A	Page 15	Basic Email Protection Controls	Basic email security controls to enable	PR.DS-2, ID.RA-2, PR.PT-3, DE.CM-4, PR.AC-4, PR.AC-1, PR.AC-7
	1	Medium	1.M.B	Page 17	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access	PR.AC-7
	1	Medium	1.M.D	Page 18	Workforce Education	Educating workforce on spotting and reporting email based attacks	PR.AT-1
	3	Medium	3.M.D	Page 37	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources	PR.AC-3, PR.AC-7
	6	Medium	6.M.D	Page 60	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies	PR.AC-3, PR.AC-5
	8	Medium	8.M.A	Page 73	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks	RS.RP
	8	Medium	8.M.B	Page 78	Incident Response	Establish formal incident response playbooks for responding to cyber attacks	PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC
	Indirect						
	3	Medium	3.M.A	Page 31	Identity	Establish a unique identifier for all users, leveraging systems of record	PR.AC-1
	3	Medium	3.M.B	Page 33	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination	PR.AC-4
	6	Medium	6.M.A	Page 57	Network Profiles and Firewalls	Deploy firewalls throughout the network	PR.AC-5, PR.AC-6
	6	Medium	6.M.B	Page 58	Network Segmentation	Establish a network segmentation strategy with clearly defined zones	PR.AC-5
	6	Medium	6.M.C	Page 60	Intrusion Prevention Systems	Deploy intrusion prevention systems to protect against known cyber attacks	DE.CM-1
	8	Medium	8.M.C	Page 82	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information	ID.RA-2
	10	Medium	10.M.A	Page 98	Policies	Establish cybersecurity policies and a default expectation of practices	ID.GV-1
Large	**Direct**						

Email us! CISA405d@hhs.gov

The Internet of Medical Things: Making Them Secure

Mark Jarrett MD, MBA, MS



Why Do We Care?

- The Fitbit Story
- Like McDonalds -Billion Devices Sold
- Expansion of Telemedicine
- Hospital at Home Strategy
- Used in Hospitals

Types of Devices

[illegible]

Video Visits require device permissions. Tap to Enable now.

Setup a Mobile Passcode to sign in faster.

You have 1 upcoming appointment in the next two weeks.

You have [illegible] unread messages in your Inbox

Your health record contains new clinical items.

You have 2 new goals

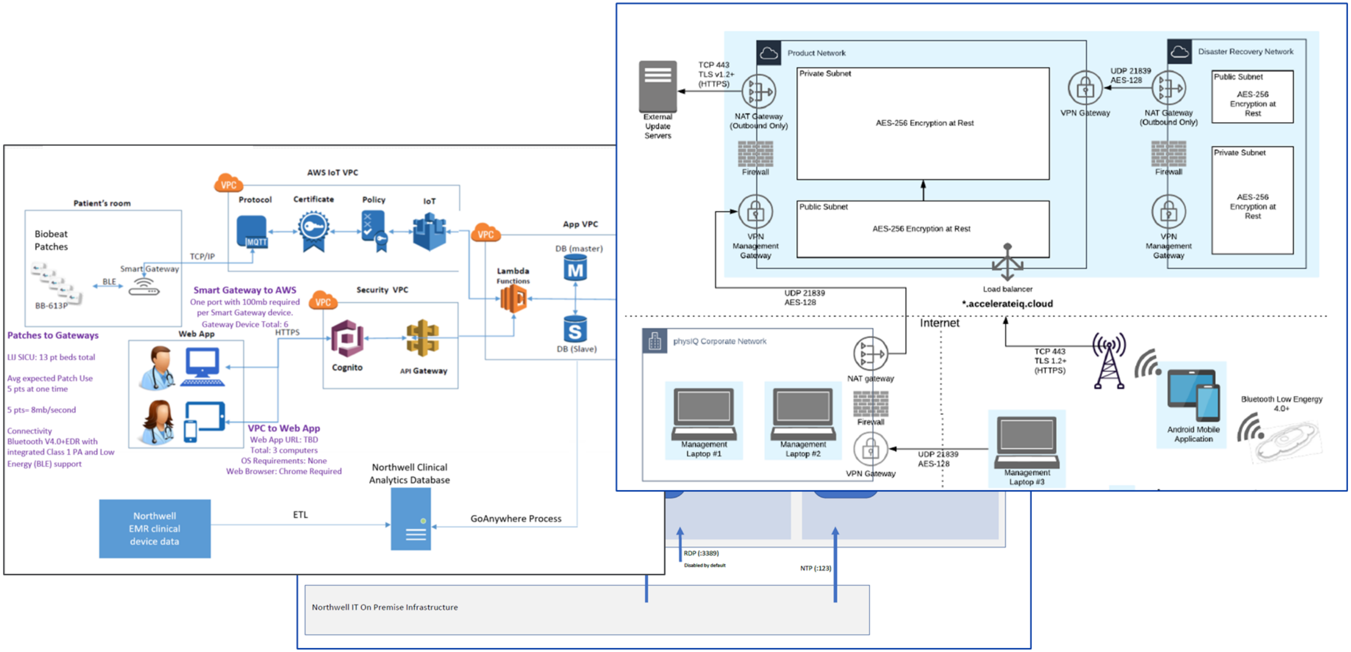
You have 1 form to complete.

- Fitness
- Early Adopters: Scales, Blood Pressure
- Pulse Ox, Heart Monitors
- Health Information Applications: e.g. Follow My Health
- Telemedicine

What Can Happen?

- Stealing of PHI or PII
- Altering Data
- Ransomware
- Infiltrate Hospitals, Physician Offices, etc.

Continuous Biosensors: Architecture



Smart Gateway to AWS
One port with 100mb required
per Smart Gateway device.
Gateway Device Total: 6

Patches to Gateways

LIJ SICU: 13 pt beds total

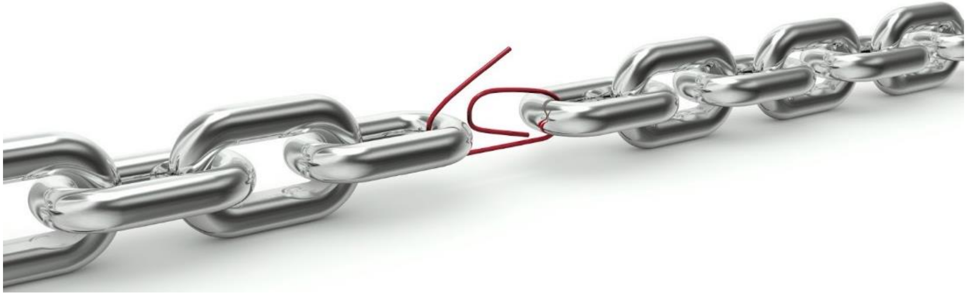
Avg expected Patch Use
5 pts at one time

5 pts= 8mb/second

Connectivity
Bluetooth V4.0+EDR with integrated Class 1 PA and Low Energy (BLE) support

VPC to Web App
Web App URL: TBD
Total: 3 computers
OS Requirements: None
Web Browser: Chrome Required

What Are The Weak Links?



- Home/Public WiFi
- Username/Passwords
- Bluetooth Vulnerabilities

- Communication Strategy
- Digital literacy
- Software Design

Next Steps

- Education
- FDA and Medical Devices
- Post Marketing Surveillance

Resources

- *Sensors* **2019**, *19*(9), 2148; **https://doi.org/10.3390/s19092148**
- https://www.sciencedirect.com/science/article/pii/S153204641500074X
- https://www.rand.org/content/dam/rand/pubs/research_reports/RR3200/RR3226/RAND_RR3226.pdf
- www.phe.gov/205d

Questions?

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d

ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES

HHS 405(d)

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate. Read the entire publication on our website: www.phe.gov/405d.