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

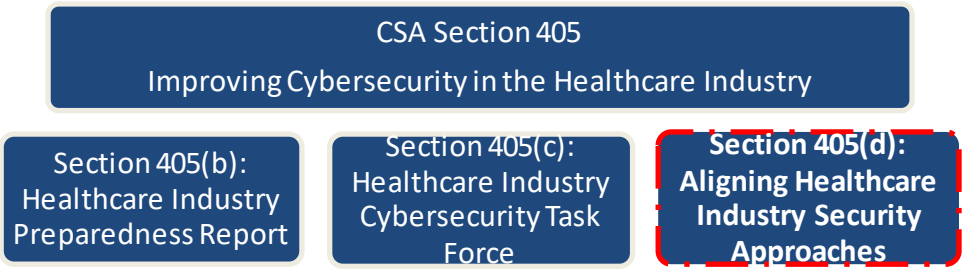
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Julie Chua, HHS
30 Minutes	The Internet of Medical Things: Making Them Secure	Mark Jarrett
15 Minutes	Q&A	All
5 Minutes	Closing	405(d) Team

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 !



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!

405(d) Social Media

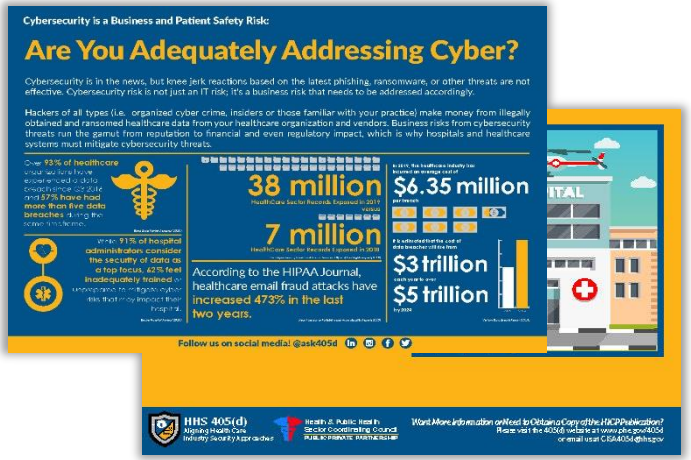
The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

NEW RESOURCES ALERT

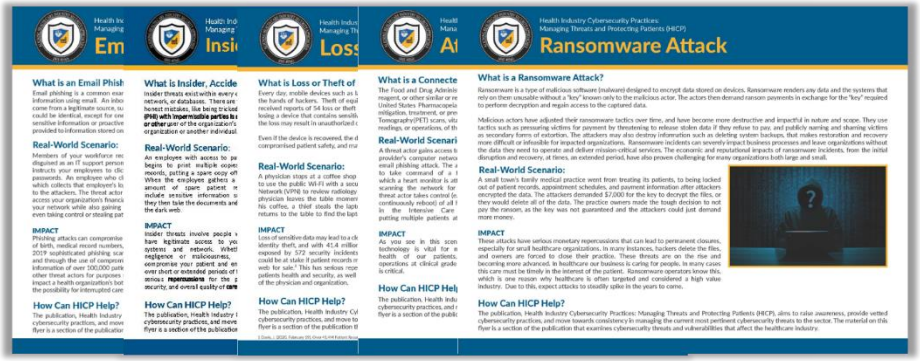
405(d) "That Seems Risky" Campaign

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

Resources from the Task Group



Small, Medium and Large Executive Cards



Five Threat Flyers

Threat Mitigation Matrix

K41

	A	B	C	D	E	F	G	H
1	Threat 1: E-mail Phishing Attack							
2		CP	Org	SP#	PG# [Tech. Vol.1 or 2]	SP Title	Short Description	NIST CSF XWALK
3	Small	Direct						
4		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
5		1	Small	1.S.B	Page 8	Education	Training of workforce on phishing attacks	PR.AT-1
6		1	Small	1.S.C	Page 8	Phishing Simulations	Conduct phishing campaigns to test and training users	PR.AT
7		8	Small	8.S.A	Page 22	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-9
8		Indirect						
9		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
10		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
11		8	Small	8.S.B	Page 23	ISAC/ISAO Participation	Join an Information Sharing Analysis Center/Organization and receive cyber intel	ID.RA-2
12		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
13	Medium	Direct						
14		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
15		1	Medium	1.M.B	Page 17	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access	PR.AC-7
16		1	Medium	1.M.D	Page 18	Workforce Education	Educating workforce on spotting and reporting email based attacks	PR.AT-1
17		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
18		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
19		8	Medium	8.M.A	Page 73	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks	RS.RP
20		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
21		Indirect						
22		3	Medium	3.M.A	Page 31	Identity	Establish a unique identifier for all users, leveraging systems of record	PR.AC-1
23		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
24		6	Medium	6.M.A	Page 57	Network Profiles and Firewalls	Deploy firewalls throughout the network	PR.AC-5, PR.AC-6
25		6	Medium	6.M.B	Page 58	Network Segmentation	Establish a network segmentation strategy with clearly defined zones	PR.AC-5
26		6	Medium	6.M.C	Page 60	Intrusion Prevention Systems	Deploy intrusion prevention systems to protect against known cyber attacks	DE.CM-1
27		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
28		10	Medium	10.M.A	Page 98	Policies	Establish cybersecurity policies and a default expectation of practices	ID.GV-1
29	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

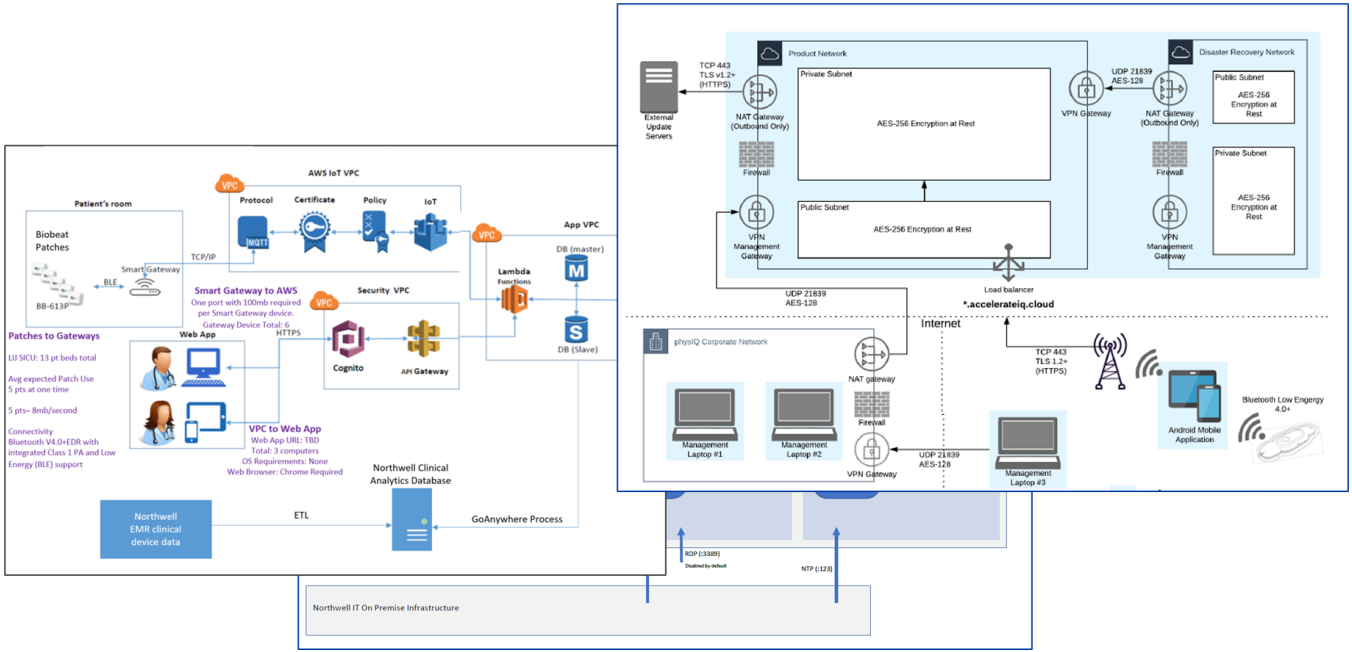
Types of Devices

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

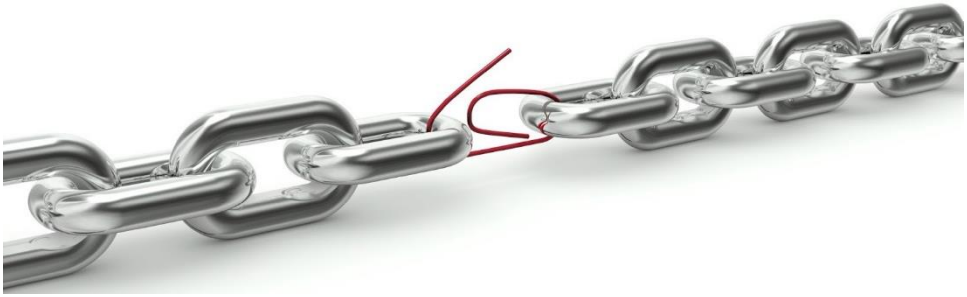
What Can Happen?

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

Continuous Biosensors: Architecture



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/S1532046415000074X
- 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

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.