



# 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
<i>10 minutes</i>	Opening Remarks and Introductions	Julie Chua, HHS
<i>30 Minutes</i>	The Internet of Medical Things: Making Them Secure	Mark Jarrett
<i>15 Minutes</i>	Q&A	All
<i>5 Minutes</i>	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](mailto: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!



## 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 ransomware 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. 38 million healthcare sector records exposed in 2017. 7 million records exposed in 2018. 91% of hospital administrators consider the security of data on a top focus. 42% feel inadequately prepared to respond to cyber risks that may impact their organization.

\$3.35 million in ransomware payments. \$3 trillion in administrative cost. \$5 trillion in total healthcare cost.

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

Follow us on social media: @ask4056

## Small, Medium and Large Executive Cards

HHS 405(d) Health Care Industry (any) Risk Index  
 Health & Public Sector Coordinating Council  
 For more information on how to Obtain a Copy of the HICPP Publication, please visit the 405(d) website at [www.hhs.gov/ask4056](http://www.hhs.gov/ask4056) or email [G405d@hhs.gov](mailto:G405d@hhs.gov)

Em	Ins	Loss	AI	Ransomware Attack
<p><b>What is an Email Phish</b></p> <p>Email phishing is a common new information security risk. Threat actors can use a legitimate source to collect identifiable email for one sensitive information or practice provided information stored on</p> <p><b>Real-World Scenario:</b></p> <p>Members of your workforce are logged in as an IT support person. They receive an email from a legitimate source, which contains a link to a website. The threat actor accesses your organization's financial records and steals sensitive information.</p> <p><b>IMPACT</b></p> <p>Phishing attacks can compromise of both, medical records, sensitive information, and financial records. The threat actor accesses your organization's financial records and steals sensitive information.</p> <p><b>How Can HICPP Help?</b></p> <p>The publication, Health Industry Cybersecurity Practices, and more. Visit a section of the publication.</p>	<p><b>What is Insider: Accidental</b></p> <p>Insider threats occur when an employee or contractor, either intentionally or unintentionally, accesses, modifies, or destroys data. This can be done through a variety of means, including a data breach, a data leak, or a data breach.</p> <p><b>Real-World Scenario:</b></p> <p>An employee with access to patient data, accidentally uploads a file to a public website. The threat actor accesses the file and steals sensitive information.</p> <p><b>IMPACT</b></p> <p>Insider threats involve people who have legitimate access to your systems and networks, which can be used to steal sensitive information or to cause a data breach.</p> <p><b>How Can HICPP Help?</b></p> <p>The publication, Health Industry Cybersecurity Practices, and more. Visit a section of the publication.</p>	<p><b>What is Loss or Theft of</b></p> <p>Every day, sensitive data such as the health of patients, is lost or stolen. This can be done through a variety of means, including a data breach, a data leak, or a data breach.</p> <p><b>Real-World Scenario:</b></p> <p>A physician steals a coffee cup to use as a USB drive. The threat actor accesses the data and steals sensitive information.</p> <p><b>IMPACT</b></p> <p>Loss of sensitive data may lead to a data breach, and can be used to steal sensitive information or to cause a data breach.</p> <p><b>How Can HICPP Help?</b></p> <p>The publication, Health Industry Cybersecurity Practices, and more. Visit a section of the publication.</p>	<p><b>What is a Connect</b></p> <p>The threat actor connects to a patient's device, such as a mobile phone, and steals sensitive information. This can be done through a variety of means, including a data breach, a data leak, or a data breach.</p> <p><b>Real-World Scenario:</b></p> <p>A patient's mobile phone is stolen. The threat actor accesses the data and steals sensitive information.</p> <p><b>IMPACT</b></p> <p>Connect attacks involve people who have legitimate access to your systems and networks, which can be used to steal sensitive information or to cause a data breach.</p> <p><b>How Can HICPP Help?</b></p> <p>The publication, Health Industry Cybersecurity Practices, and more. Visit a section of the publication.</p>	<p><b>What is a Ransomware Attack?</b></p> <p>Ransomware is a type of 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 actor then demands ransom payments in exchange for the "key" required to perform decryption and regain access to the encrypted data.</p> <p><b>Real-World Scenario:</b></p> <p>A small town's family medical practice went from treating its patients, to being locked out of patient records, equipment, and payment information. The attacker demanded \$1000 for the key to decrypt the files, or they would delete all of the data. The practice owners were left with no choice but to pay the ransom, as the key was not guaranteed and the attackers could just demand more money.</p> <p><b>IMPACT</b></p> <p>Ransomware attacks have become more destructive and impactful in nature and scope. They can result in data loss, equipment downtime, and payment information. The attacker demands \$1000 for the key to decrypt the files, or they would delete all of the data. The practice owners were left with no choice but to pay the ransom, as the key was not guaranteed and the attackers could just demand more money.</p> <p><b>How Can HICPP Help?</b></p> <p>The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICPP), aims to raise awareness, provide best practices, and more towards cybersecurity in the current most pertinent cybersecurity threats to the sector. The content on this flyer is a section of the publication that addresses cybersecurity threats and vulnerabilities that affect the healthcare industry.</p>

## Five Threat Flyers



# Threat Mitigation Matrix

Threat 1: E-mail Phishing Attack							
CP	Org	SP#	PC# [Tech. Vol. 1 or 2]	SP Title	Short Description	NIST CSF XWALK	
<b>Small Direct</b>							
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	
<b>Small Indirect</b>							
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	
<b>Medium Direct</b>							
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	
<b>Medium Indirect</b>							
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-3, 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/SAOs	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	
<b>Large Direct</b>							

Email us! [CISA405d@hhs.gov](mailto: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

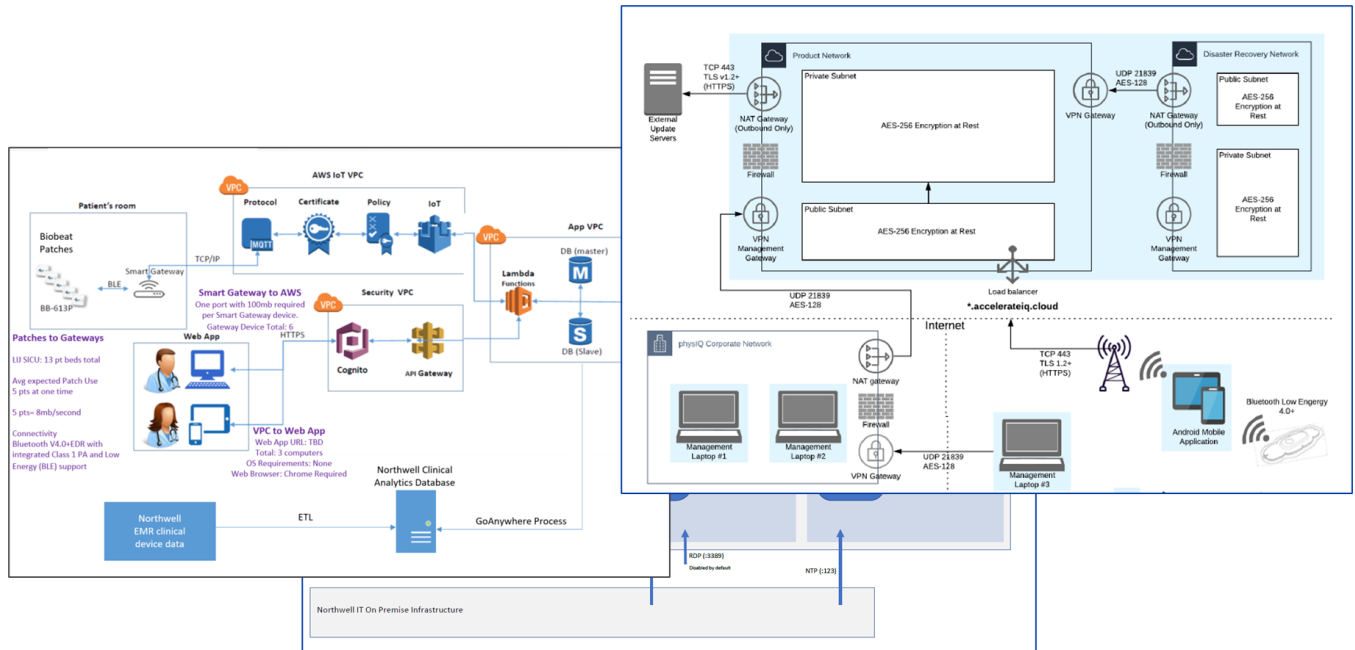


# What Can Happen?

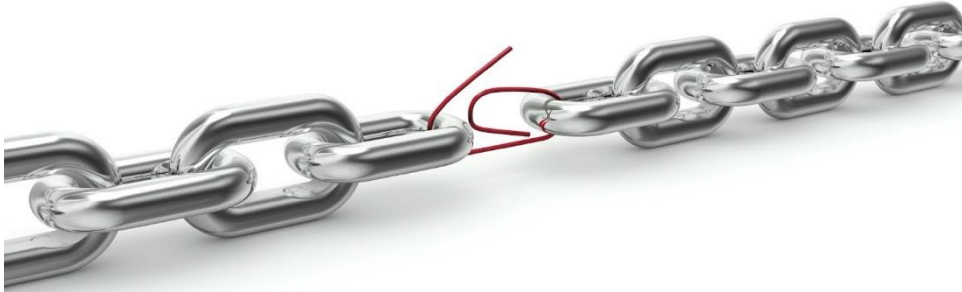
- Stealing of PHI or PII
- Altering Data
- Ransomware
- Infiltrate Hospitals, Physician Offices, etc.



# Continuous Biosensors: Architecture

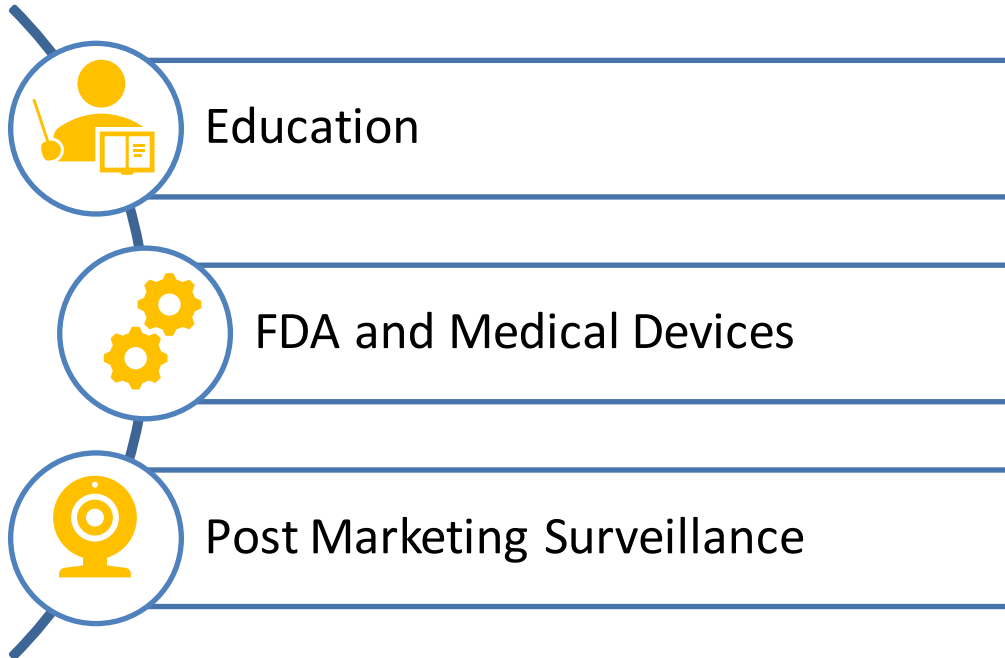


# What Are The Weak Links?



- Home/Public WiFi
- Username/Passwords
- Bluetooth Vulnerabilities
- Communication Strategy
- Digital literacy
- Software Design

# Next Steps



# 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](https://www.rand.org/content/dam/rand/pubs/research_reports/RR3200/RR3226/RAND_RR3226.pdf)
- [www.phe.gov/205d](http://www.phe.gov/205d)



# Questions?



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



[Linkedin.com/company/hhs-ask405d](https://www.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](http://www.phe.gov/405d).