LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Five Threats Series: Threat 5 – Attacks Against Connected Medical Devices

April 2019

In Partnership With

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

Agenda

Time	Topic	Speaker
5 Minutes	Opening Remarks & Introductions	405(d) Team
5 Minutes	CSA Section 405(d)'s Mandate, Purpose, and Desired Goals	Aftin Ross
5 Minutes	HICP Overview	Aftin Ross
10 Minutes	Using HICP and Supporting Resources	Aftin Ross
40 Minutes	Threat 5 – Attacks Against Connected Medical Devices and Mitigating Practices	Dale Nordenberg/Aftin Ross
5 Minutes	Looking Forward	405(d) Team
5 Minutes	Upcoming HICP Engagements	405(d) Team
15 Minutes	Questions	

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

CSA Section 405(d)'s Mandate, Purpose, and Desired Goals

Cybersecurity Act of 2015 (CSA): Legislative Basis

CSA Section 405

Improving Cybersecurity in the Health Care Industry

- Section 405(b): Health care industry preparedness report
- Section 405(c): Health Care Industry Cybersecurity Task Force
- **Section 405(d): Aligning Health Care Industry Security Approaches**

Industry-Led Activity to Improve Cybersecurity in the Healthcare and Public Health (HPH) Sector

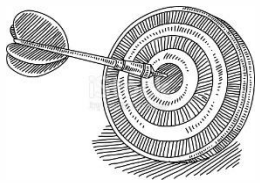
WHAT IS THE 405(d) EFFORT?

An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.

WHO IS PARTICIPATING?

The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?



With a targeted set of applicable & voluntary practices that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations.

WHY IS HHS CONVENING THIS EFFORT?

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

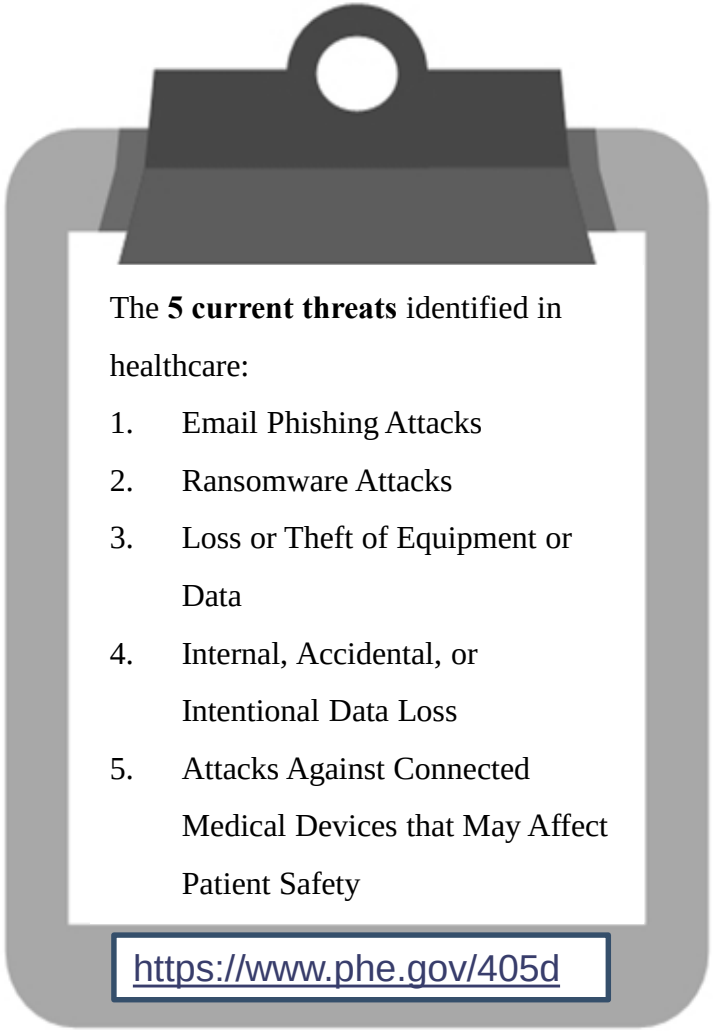
OFFICE OF THE CHIEF INFORMATION OFFICER

HICP Publication Overview

Document - Content Overview (1/2)

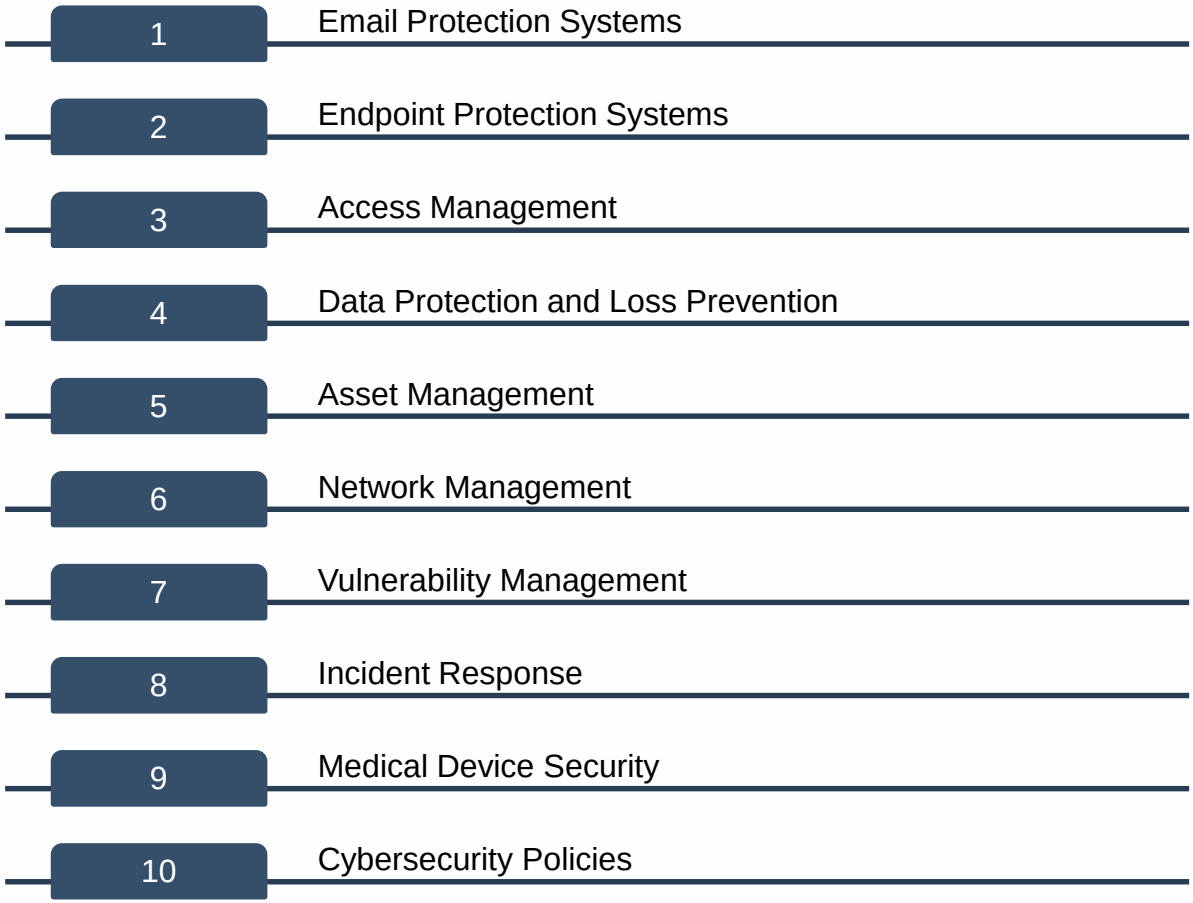
After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.
- *Technical Volume 1* discusses these ten cybersecurity practices for **small** healthcare organizations.
- *Technical Volume 2* discusses these ten cybersecurity practices for **medium and large** healthcare organizations.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.



Document - Content Overview (2/2)

The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Using HICP and Supporting Resources

Introduction and Executive Summary

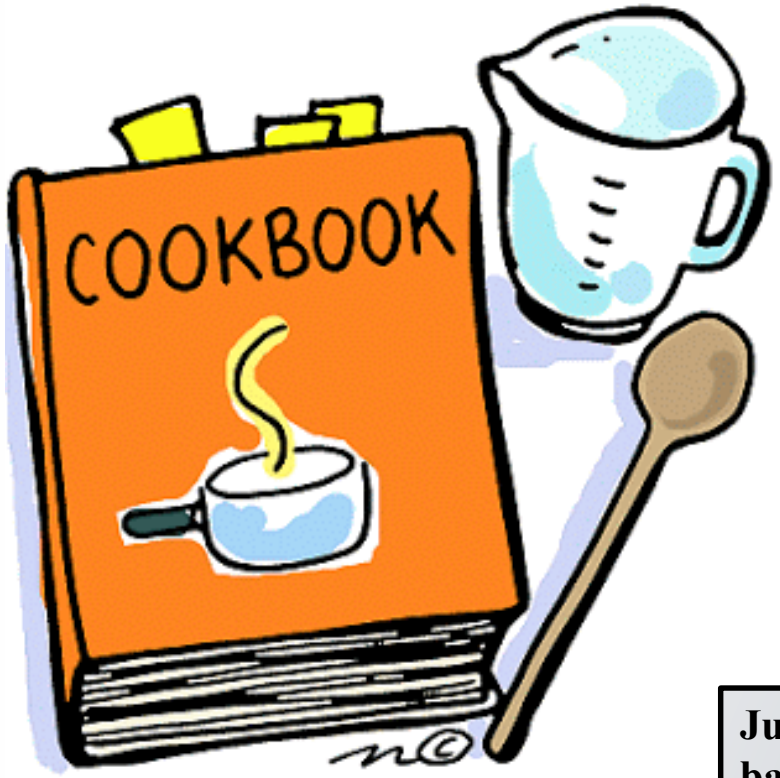
HICP is…

- A call to action to manage real cyber threats
- Written for multiple audiences (clinicians, executives, and technical)
- Designed to account for organizational size and complexity (small, medium and large)
- A reference to "get you started" while linking to other existing knowledge
- Aligned to the NIST Cybersecurity Framework
- Voluntary

HICP is **not**…

- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of "reasonable security measures" in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in place that are more effective than what was outlined!
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

HICP is a Cookbook!



So you want a recipe for managing phishing?

1. 5 oz of Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 2 cups of Workforce Education (1.M.D)
4. 1 cup of Incident Response plays (8.M.B)
5. 1 tsp of Digital Signatures for authenticity (1.L.B)
6. Advanced and Next General Tooling to taste (1.L.A)

Preheat your email system with some basic email protection controls necessary to build the foundation of your dish. Mix in MFA for remote access, in order to protect against potential credential theft.

Let sit for several hours, while providing education to your workforce on the new system, and how to report phishing attacks. While doing so, ensure to provide education on how digital signatures demonstrating authenticity of the sender. When finished baking, sprinkle with additional tooling to provide next level protection.

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not:

- **Instruct you how to cook**
- **Instruct you on what recipes to use**
- **Limit your ability for substitutions**

The skill of the cook is what makes the dish!

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

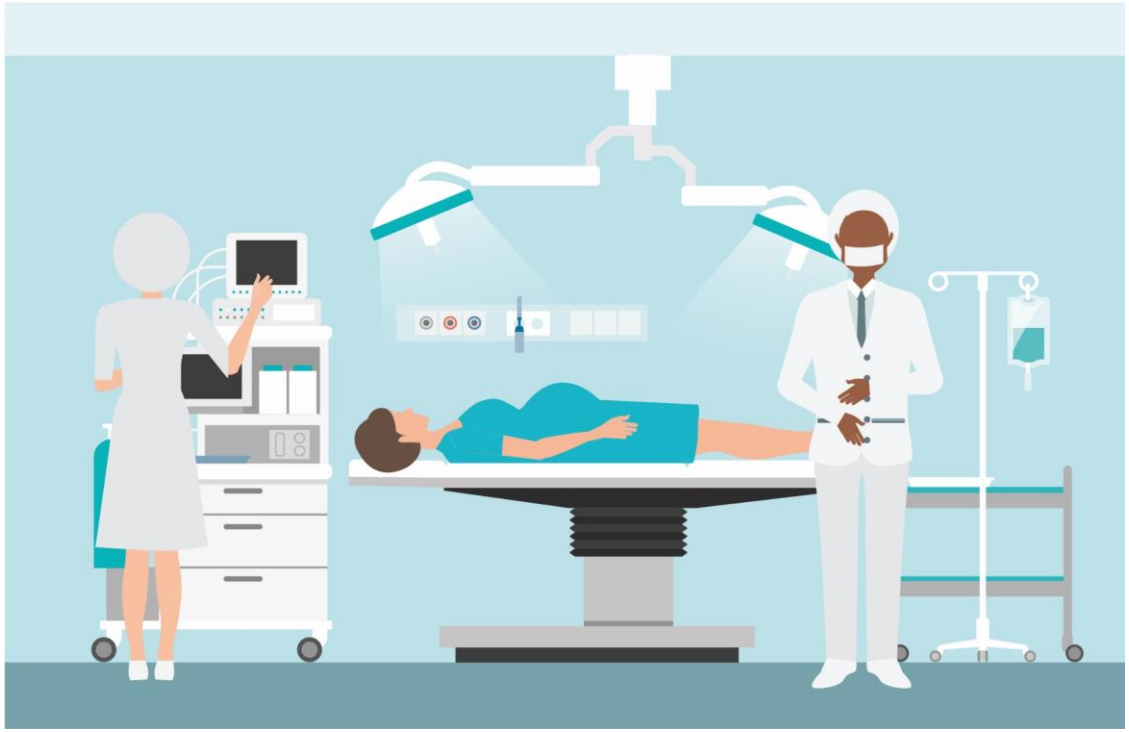
OFFICE OF THE CHIEF INFORMATION OFFICER

Threat 5 – Attacks Against Connected Medical Devices

Cybersecurity Practice #5: Asset Management

Attacks Against Connected Medical Devices?

The Food and Drug Administration (FDA) defines a medical device as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease.”



Attacks Against Connected Medical Devices Scenario

- **Real-World Scenario:** A cyber attacker gains access to a care provider's computer network through an e-mail phishing attack and takes command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.
- **Impact**: Patients are at great risk because an attack has shut down heart monitors, potentially during surgery and other procedures.

What is Asset Management

- The process by which organizations manage IT assets is generally referred to as *IT asset management* (ITAM). ITAM is critical to ensuring that proper cyber hygiene controls are in place across all assets in the organization. ITAM increases the visibility of cybersecurity professionals in the organization and reduces unknowns.
- ITAM processes should be implemented for all endpoints, servers, and networking equipment. ITAM processes enable organizations to understand their devices, and the best options to secure them. The practices described in this section of the publication may be used to support many of the practices described in other sections of this volume.

Tin Zaw, "2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter," Verizon Digital Media Service, last modified July 26, 2017, https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.
Ian Murphy, "How Susceptible Are You to Enterprise Phishing?" Enterprise Times, last modified December 1, 2017, https://www.enterprisetimes.co.uk/2017/12/01/susceptible-enterprise-phishing/.

Attacks Against Connected Medical Devices Mitigating Practices - Small Organizations

Technical Volume 1 provides health care cybersecurity practices for small health care organizations. For the purpose of this volume, *small organizations* generally do not have dedicated information technology (IT) and security staff dedicated to implementing cybersecurity practices due to limited resources.

Although it can be difficult to implement and sustain ITAM processes, such processes should be part of daily IT operations and encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device. The Asset Management practices in *Technical Volume 1* can be found in **Cybersecurity Practice 6# &9**

Cybersecurity Practice #6: Network Management

Network Segmentation

Cybersecurity Practice #9: Medical Device Security

Medical Device Security

Attacks Against Connected Medical Devices Mitigating Practices - Small Organizations

For each Sub-Practice, *Technical Volume 1* provides, considerations your organization can take to enhance the security posture

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #6 & #9.**

Cybersecurity Practice #6 Sub Practice A: Network Segmentation

- Configure networks to restrict access between devices to that which is required to successfully complete work. This will limit any cyberattacks from spreading across your network.
  - Disallow all Internet bound access into your organization's network. If you host servers that interface with the internet, consider using a third-party vendor who will provide security as part of the hosting service. Restrict access to assets with potentially high impact in the event of compromise. This includes medical devices and internet of things (IoT) items (e.g., security cameras, badge readers, temperature sensors, building management systems).

Cybersecurity Practice #9 Sub Practice A: Medical Device Security

- Configure networks to restrict access between devices to that which is required to successfully complete work. This will limit any cyberattacks from spreading across your network.
  - Disallow all Internet bound access into your organization's network. If you host servers that interface with the internet, consider using a third-party vendor who will provide security as part of the hosting service.

Attacks Against Connected Medical Devices Mitigating Practices for Medium/Large Organizations

Technical Volume 2 provides health care cybersecurity practices for Medium/Large health care organizations. For the purpose of this volume,

- Medium-sized health care organizations generally employ hundreds of personnel, maintain between hundreds and a few thousand information technology (IT) assets, and may be primary partners with and liaisons between small and large health care organizations.
- Large health care organizations perform a range of different functions. These organizations may be integrated with other health care delivery organizations, academic medical centers, insurers that provide health care coverage, clearinghouses, pharmaceuticals, or medical device manufacturers. In most cases, large organizations employ thousands of employees, maintain tens of thousands to hundreds of thousands of IT assets, and have intricate and complex digital ecosystems.

Attacks Against Connected Medical Devices Mitigating Practices for Medium/Large Organizations

The e-mail protection practices in *Technical Volume 2* can be found in **Cybersecurity Practice #1 & #9**. Medium sub-practices apply to both medium-sized and large organizations. Large sub-practices apply primarily to large organizations, but could also benefit any other organization that interested in adopting them.

Cybersecurity Practice #1: Email Protection

- Advanced and Next Generation Tooling

Cybersecurity Practice #9: Medical Device Security

- Endpoint Protections
- Identity and Access Management
- Asset Management
- Network Management
- Vulnerability Management (Large)
- Security Operations and Incident Response (Large)
- Procurement and Security Evaluations (Large)

Attacks Against Connected Medical Devices Mitigating Practices - Medium Organizations

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #1 & 9.**

Cybersecurity Practice #1 Sub Practice A: Advanced and Next Generation Tooling

- Many sophisticated solutions exist to help combat the phishing and malware problem. These solutions are called *advanced threat protection services*. They use threat analytics and real-time response capabilities to provide protection against phishing attacks and malware.
  - *URL click protection via analytics:* In a modern phishing attack, the hacker will create a web page on the internet for harvesting credentials or delivering malware. Next, the hacker will conduct an e-mail campaign, sending e-mails with a link to a web page that does not have malicious content. Because the linked page is not malicious, traditional spam and AV protections clear the e-mail for delivery to the user.

Cybersecurity Practice #9 Sub Practice B: Endpoint Protections

- *Local firewalls:* Medical devices should be configured to communicate only with required systems. Unused services and ports should be disabled if they are supported by the manufacturer.
  - *Encryption:* If supported by the manufacturer, medical devices should have local encryption enabled in the case the device is stolen.
  - *Application whitelist:* Configure medical devices, or implement software, to only allow known processes and executables to run on the devices. This control alone can significantly reduce the exploitability of devices.

Cybersecurity Practice #9 Sub Practice C: Identity and Access Management

- As much as feasible, medical devices should have the following controls enabled:
  - *Authentication:* If supported by the manufacturer, the device should bind its authentication capabilities with systems enterprise authentication domains. This automates termination of access to the device upon termination of employment for the user.

Attacks Against Connected Medical Devices Mitigating Practices - Medium Organizations

Threat 5: Attacks Against Connected Medical Devices That May Affect Patient Safety | Sub-Practices For Medium Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
9 – Medical Device Security	9.M.B Endpoint Protections	Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested	PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1
9 – Medical Device Security	9.M.C Identity and Access Management	Implement access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, MFA, and minimum necessary or least privilege	PR.AC, PR.AC-7, PR.AC-4
9 – Medical Device Security	9.M.D Asset Management	Assess inventory traits such as IT components that may include the Media Access Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks	ID.AM, ID.AM-1, PR.IP-6
9 – Medical Device Security	9.M.E Network Management	Assess current security controls on networked medical devices	PR.AC-5

Attacks Against Connected Medical Devices Mitigating Practices - Large Organizations

Threat 5: Attacks Against Connected Medical Devices That May Affect Patient Safety | Sub-Practices For Large Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
1 – E-mail Protection Systems	1.L.A Advanced and Next Generation Tooling	Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities	PR.DS-2, DE.CM-5, DE.CM-7
9 – Medical Device Security	9.L.A Vulnerability Management	Establish and maintain communication with medical device manufacturer's product security teams	ID.RA-1, PR.IP-12, ID.RA-5, RS.CO-5, DE.CM-8
9 – Medical Device Security	9.L.B Security Operations and Incident Response	Implement security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities	PR.IP-9, DE.CM-8, DE.CM-1, DE.CM-7
9 – Medical Device Security	9.L.C Procurement and Security Evaluations	• Implement pre-procurement security requirements for vendors • Engage information security as a stakeholder in clinical procurements • Use a template for contract language with medical device manufacturers and others	ID.SC

Attacks Against Connected Medical Devices Mitigating Practices Metrics for Organizations

Specifically for Medium/Large Organizations **Technical Volume 2** contains a series of suggested metrics to measure the effectiveness of the cybersecurity practice. The metrics for each Cybersecurity Practice can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for **Cybersecurity Practice #9:**

Number of medical devices not currently segmented on wireless or wired networks, trended over time	Number of unmitigated high-risk vulnerabilities on connected medical devices, trended over time	Number of medical devices that do not conform to basic endpoint protection cybersecurity practices, trended over time	Number of devices that have unknown risks due to lack of manufacturer-disclosed information, trended over time
• The goal is to limit medical devices on the general access network, data center network, or other locations that do not meet the requirements of specific network segmentation strategies	• The goal is to reduce the number of unmitigated risks to as near zero as possible. Each high-risk vulnerability should have a remediation action plan, as defined in **Cybersecurity Practice #7: Vulnerability Management**.	• The goal is to reduce the number of medical devices that do not meet basic hygiene management practices or to implement practices for these devices. It is not always possible to reduce this number to zero. Mitigating factors should be employed to keep it as low as possible.	The goal is to ensure that device manufacturers have vulnerability disclosure programs and that your organization is privy to them.

Looking Forward

Looking Forward

CSA 405(d) aims to be the leading collaboration center of OCIO/OIS, in partnership with relevant HHS divisions, and the healthcare industry focused on the development of resources that help align health care cybersecurity practices

- **Immediate Next Steps**
  - Over the course of the next year the 405(d) Team plans to continue to develop awareness of the HICP publication and engage with stakeholders by:
    - Building additional supporting materials/resources to spotlight the HICP publication and related content
    - Develop means to collect feedback and implementation of HICP practices and methods
    - Hosting additional outreach engagements

Questions

Thank you for Joining Us

Visit us at: www.405d.hhs.gov

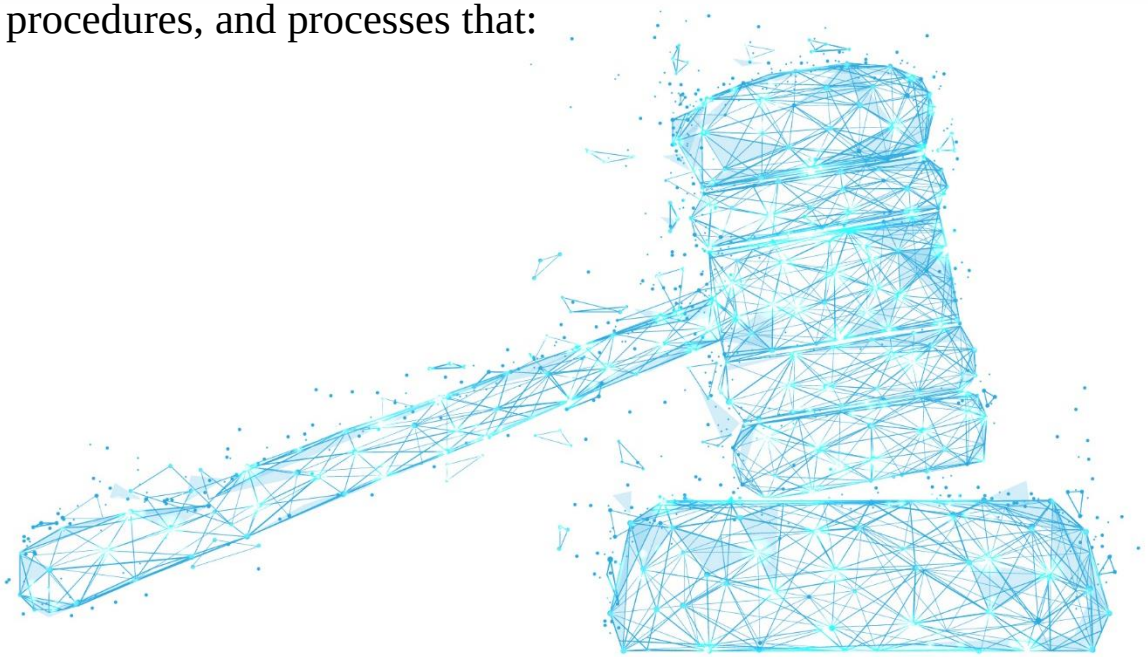
Contact Us at: CISA405d@hhs.gov

APPENDIX

CSA Section 405(d): Legislative Language (1/2)

Authority: Cybersecurity Act of 2015 (CSA), Section 405(d), *Aligning Health Care Industry Security Approaches*

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that:



CSA Section 405(d): Legislative Language (2/2)

A. Serve as a resource for *cost-effectively reducing cybersecurity risks* for a range of health care organizations;
B. Support *voluntary adoption and implementation* efforts to improve safeguards to address cybersecurity threats;
C. Are consistent with—
   i. The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));
   ii. The security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and
   iii. The provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and
D. Are updated on a regular basis and applicable to *a range of health care organizations*.

How to Evaluate Your Organization's Size

HICP is designed to assist organizations of various sizes implement resources and practices that are tailored and cost effective to their needs.

- How "large and complex an organization you might be relates to several factors:
  - Health Information Exchanges
  - IT Capability
  - Cybersecurity Investment
  - Size (provider)
  - Size (acute/post-acute)
  - Size (hospital)
  - Complexity
- Determining where you fit is your decision

Medium

[Main Document](), p. 11

Best Fit		Small	Medium	Large
Common Attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	Size (provider)	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Table 1. Selecting the "Best Fit" For Your Organization

How to Use Practices and Sub-Practices

- There are a total of **10** Cybersecurity Practices, and **89** Sub-Practices.
- Each Cybersecurity Practice has a corresponding set of Sub-Practices, risks that are mitigated by the Practice, and suggested metrics for measuring the effectiveness of the Practice
- Medium Sized orgs can review the Medium Sub-Practices
- Large Sized orgs can review the Medium **and** Large Sub-Practices
- Each Practice is designed to mitigate one or many threats

Cybersecurity Practice 2: Endpoint Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	2.M.A	Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A	Automate the Provisioning of Endpoints
	2.L.B	Mobile Device Management
	2.L.C	Host Based Intrusion Detection/Prevention Systems
	2.L.D	Endpoint Detection Response
	2.L.E	Application Whitelisting
	2.L.F	Micro-segmentation/virtualization strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data	

Sample Metrics

- Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly.
- Percentage of endpoints that meet all patch requirements each month.
- Percentage of endpoints with active threats each week.
- Percentage of endpoints that run non hardened images each month.
- Percentage of local user accounts with administrative access each week.

Prioritize Your Threats (with Example)

- Implementing all Practices within HICP could be daunting, even for a Large Sized Organization
- Recommendation: Review the threats and implement the most impactful practices first
  - A toolkit will be released shortly to assist with this process

Factor		
Select your organizations size		Medium
Prioritize the threats (5 being highest priority, 1 being lowest priority)		
A	Email Phishing Attack	1
B	Ransomware Attack	4
C	Loss or Theft of Equipment or Data	5
D	Insider, Accidental or Intentional Data Loss	3
E	Attacks Against Connected Medical Devices that may affect Patient Safety	2

CP #	Cybersecurity Practices	Priority Rank Based on Threat Model Inputs
8	Incident Response	28
3	Access Management	23
2	Endpoint Protection Systems	23
5	Asset Management	20
6	Network Management	16
7	Vulnerability Management	16
10	Cybersecurity Policies	15
1	Email Protection Systems	13
9	Medical Device Security	11
4	Data Protection and Loss Prevention	11

Attacks Against Medical Devices That May Affect Patient Safety: Direct Mitigating Sub-Practices (S)

The below table lists all of the **direct** Sub-Practices for small organizations to mitigate Threat 5: Attacks Against Medical Devices That May Affect Patient Safety, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
6.S.A	Network Segmentation	Segment devices into various networks, restricting access
9.S.A	Medical Device Security	Secure medical devices within your practice

Attacks Against Medical Devices That May Affect Patient Safety: Indirect Mitigating Sub-Practices (S)

The below table lists all of the **indirect** Sub-Practices for small organizations to mitigate Threat 5: Attacks Against Medical Devices That May Affect Patient Safety, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures
5.S.A	Inventory	Conduct and manage an inventory of IT Assets
5.S.B	Procurement	Keep asset inventory up to date with procurement of new devices
5.S.C	Decommissioning	Securely remove devices from the circulation
6.S.B	Physical Security and Guest Access	Physically secure servers and network devices, and segment guest access from regular network
6.S.C	Intrusion Prevention	Implement and operate an IPS system to stop well known cyber attacks
7.S.A	Vulnerability Management	Discover technical vulnerabilities (host and web) and remediate
8.S.A	Incident Response	Establish procedures for managing cyber-attacks, especially malware and phishing
8.S.B	ISAC/ISAO Participation	Join an Information Sharing Analysis Center/Organization and receive cyber intel
10.S.A	Policies	Establish cybersecurity policies and a default expectation of practices

Attacks Against Medical Devices That May Affect Patient Safety: Direct Mitigating Sub-Practices (M)

The below table lists all of the **direct** Sub-Practices for medium organizations to mitigate Threat 5: Attacks Against Medical Devices That May Affect Patient Safety, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources
6.M.A	Network Profiles and Firewalls	Deploy firewalls throughout the network
6.M.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones
9.M.A	Medical Device Management	Set a strategy for managing the security of medical devices, utilizing existing processes
9.M.B	Endpoint Protections	Configure and secure medical devices based on 6 steps
9.M.C	Identity and Access Management	Ensure authentication and remote access is managed
9.M.D	Asset Management	Inventory hardware and software of medical devices
9.M.E	Network Management	Segment medical devices on dedicated, highly restrictive networks

Attacks Against Medical Devices That May Affect Patient Safety: Indirect Mitigating Sub-Practices (M)

The below table lists all of the **indirect** Sub-Practices for medium organizations to mitigate Threat 5: Attacks Against Medical Devices That May Affect Patient Safety, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP#	SP Title	Short Description
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts
5.M.B	Procurement	Keep asset inventory up to date with procurement of new devices
5.M.C	Secure Storage for Inactive Devices	Ensure unused devices are physically secure
5.M.D	Decommissioning Assets	Securely remove devices from the circulation
6.M.C	Intrusion Prevention Systems	Deploy intrusion prevention systems to protect against known cyber attacks
6.M.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies
6.M.E	Physical Security of Network Devices	Physically secure the network devices
7.M.A	Host/Server Based Scanning	Discover host based technical vulnerabilities
7.M.D	Patch Management, Configuration Management, Change Management	Routinely patch and mitigate vulnerabilities
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices

Attacks Against Medical Devices That May Affect Patient Safety: Direct Mitigating Sub-Practices (L)

The below table lists all of the **direct** Sub-Practices for large organizations to mitigate Threat 5: Attacks Against Medical Devices That May Affect Patient Safety, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources
6.M.A	Network Profiles and Firewalls	Deploy firewalls throughout the network
6.M.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones
9.M.A	Medical Device Management	Set a strategy for managing the security of medical devices, utilizing existing processes
9.M.B	Endpoint Protections	Configure and secure medical devices based on 6 steps
9.M.C	Identity and Access Management	Ensure authentication and remote access is managed
9.M.D	Asset Management	Inventory hardware and software of medical devices
9.M.E	Network Management	Segment medical devices on dedicated, highly restrictive networks
9.L.A	Vulnerability Management	Carefully identify vulnerabilities on medical devices, and remediate accordingly
9.L.B	Security Operations and Incident Response	Ensure IR playbooks account for patient safety implications of connected medical devices
9.L.C	Procurement and Security Evaluations	Conduct security evaluations for newly purchased medical devices
9.L.D	Contacting the FDA	Contact the FDA for risk security issues that are unresolved

Attacks Against Medical Devices That May Affect Patient Safety: Direct Mitigating Sub-Practices (L)

The below table lists all of the **indirect** Sub-Practices for large organizations to mitigate Threat 5: Attacks Against Medical Devices That May Affect Patient Safety, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

Attacks Against Medical Devices That May Affect Patient Safety: Indirect Mitigating Sub-Practices (L)

SP#	SP Title	Short Description
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts
5.M.B	Procurement	Keep asset inventory up to date with procurement of new devices
5.M.C	Secure Storage for Inactive Devices	Ensure unused devices are physically secure
5.M.D	Decommissioning Assets	Securely remove devices from the circulation
6.M.C	Intrusion Prevention Systems	Deploy intrusion prevention systems to protect against known cyber attacks
6.M.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies
6.M.E	Physical Security of Network Devices	Physically secure the network devices
7.M.A	Host/Server Based Scanning	Discover host based technical vulnerabilities
7.M.D	Patch Management, Configuration Management, Change Management	Routinely patch and mitigate vulnerabilities
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices
2.L.E	Application Whitelisting	Permit only known good and authorized applications
3.L.B	Authorization	Authorize access based on role (RBAC) or attribute (ABAC)
3.L.C	Access Governance	Review access periodically to ensure user access still appropriate
3.L.D	Single-Sign On (SSO)	Authenticate against central credential repositories and ease access burdens
5.L.A	Automated Discovery and Maintenance	Leverage automation to keep asset inventory details up to date
5.L.B	Integration with Network Access Control	Catch endpoints on the network that fall out of compliance or are outliers
6.L.A	Additional Network Segmentation	Further implement segmentation strategies for remote VPN access to data center
6.L.B	Command and Control Monitoring of Perimeter	Monitor for malicious outbound Command and Control traffic
6.L.C	Anomalous Network Monitoring and Analytics	Monitor for anomalous network traffic based on analytics and baselines
6.L.D	Network Based Sandboxing/Malware Execution	Monitor common transfer protocols to discover malicious attachments
6.L.E	Network Access Control (NAC)	Ensure endpoints are secure on the network through automated tools
7.L.A	Penetration Testing	Actively exploit your environment to uncover vulnerabilities and risks
7.L.B	Remediation Planning	Implement formal mechanisms for remediating vulnerabilities and risks
8.L.A	Advanced Security Operations Center	Expand the SOC to a dedicated team that operates 24x7x365
8.L.B	Advanced Information Sharing	Share and receive threat intelligence information from partner organizations
8.L.C	Incident Response Orchestration	Automate the manual response of IR playbooks through advanced tools
8.L.D	Baseline Network Traffic	Establish digital footprints on systems and alert when they deviate
8.L.E	User Behavior Analytics	Establish baseline patterns of user access and alert when they deviate
8.L.F	Deception Technologies	Establish 'tripwires' or honeypots on your network and alert when they are tripped