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 2 – Ransomware Attack

March 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	
5 Minutes	CSA Section 405(d)'s Mandate, Purpose, and Desired Goals	
5 Minutes	HICP Overview	
10 Minutes	Using HICP and Supporting Resources	
40 Minutes	Threat 2 – Ransomware Attack and Mitigating Practices	
5 Minutes	Looking Forward	
5 Minutes	Upcoming 5 Threats	
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

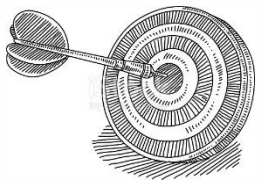
WHAT IS THE 405(d) EFFORT?

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

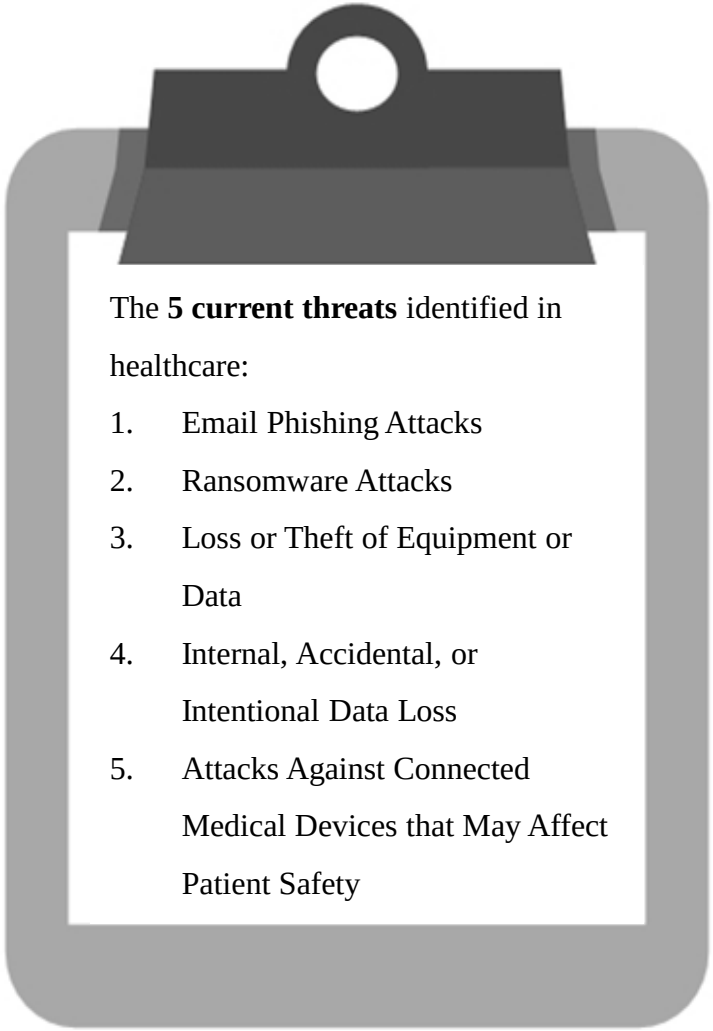
OFFICE OF THE CHIEF INFORMATION OFFICER

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

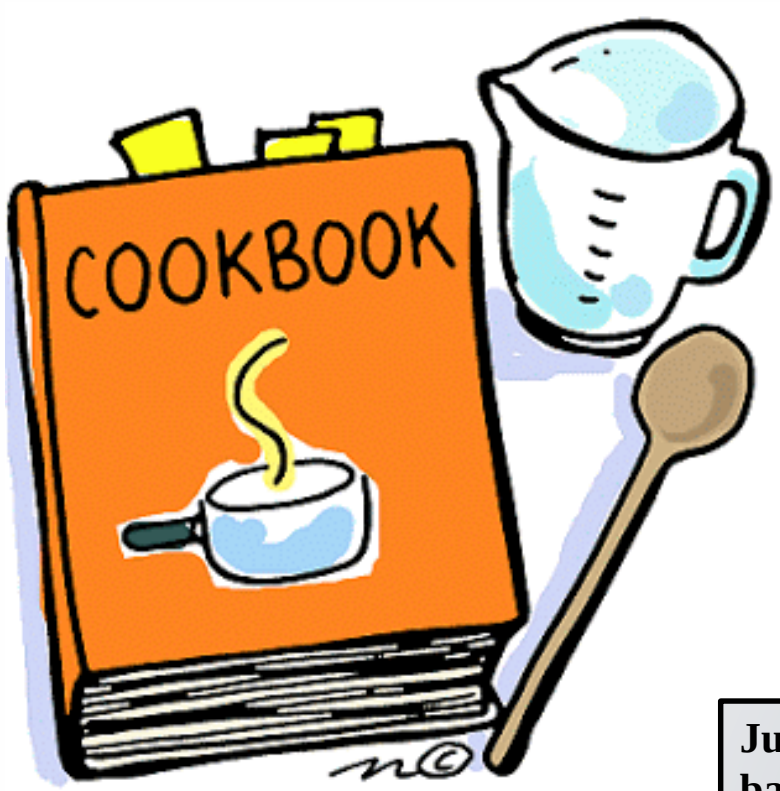
HICP is…

- 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!

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

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Threat 2 – Ransomware Attack & Mitigating Practices

What is a Ransomware Attack?

The HHS Ransomware Factsheet defines ransomware as follows: Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

However, paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats.

Ransomware Attack Scenario

- **Real-World Scenario:** Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called security update is actually a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data
- **Impact**: A practitioner cannot view patient charts because of a ransomware attack that has made the EHR system inaccessible.

Defining Endpoints

Endpoints are the assets the workforce uses to interface with an organization's digital ecosystem. Endpoints include desktops, laptops, workstations, and mobile devices. Current cyberattacks target endpoints as frequently as networks. Implementing baseline security measures on these assets provides a critical layer of threat management. As the modern workforce becomes increasingly mobile, it is essential for these assets to interface and function securely.

The endpoints of which our computing environments largely consist are no longer static devices that exist in the health care organization's main network. Organizations commonly leverage virtual teams, mobility, and other remote access methods to complete work. In some cases, endpoints rarely make it to the corporate network. It is important to build cybersecurity hygiene practices with these characteristics in mind.

CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers," Center for Information Security Controls, accessed September 24, 2018, https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/.

Ransomware Attack Mitigating – Small Organizations

Technical Volume 1 provides 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.

A small organization's endpoints must be protected. Because technology is highly mobile, computers are often connected to and disconnected from an organization's network. Although attacks against endpoints tend to be delivered via e-mail, they can also be delivered as *client-side attacks*. The Ransomware Attack Mitigating practices in *Technical Volume 1* can be found in **Cybersecurity #1, #2, #3, #5, #6, #7, & #8**

Cybersecurity Practice #1: E-mail Protection Systems

- E-mail system configuration

Cybersecurity Practice #2: Endpoint Protection Systems

- Basic Endpoint Protection

Cybersecurity Practice #3: Access Management

- Basic Access Management

Cybersecurity Practice #5: Asset Management

- E-mail system configuration

Cybersecurity Practice #6: Network Management

- Network Segmentation

Cybersecurity Practice #7: Vulnerability Management

- Vulnerability Management

Cybersecurity Practice #8: Incident Response

- Incident Response
- ISAC/ISAO Participation

Ransomware Attack Mitigating Practices – Small Organizations

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

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity #2, #6, and #7**

Cybersecurity #2 Sub practice A: Basic Endpoint Protection Controls

- Remove Administrative Accounts
- Keep you Endpoints Patched
- Implement Antivirus Software

Cybersecurity #6 Sub practice A: Network Segmentation

- Establish and enforce network traffic restrictions. These restrictions may apply to applications and websites, as well as to users in the form of role-based controls. Restricting access to personal websites (e.g., social media, couponing, online shopping) limits exposure to browser add-ons or extensions, in turn reducing the risk of cyberattacks

Cybersecurity #7 Sub practice A: Vulnerability Management

- Vulnerability management practices include:
  - Schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws.
  - Conduct web application scanning of internet-facing webservers, such as web-based patient portals. Specialized vulnerability scanners can interrogate running web applications to identify vulnerabilities in the application design

Ransomware Attack Mitigating Practices – Small Organizations

Threat 2: Ransomware Attack | Sub-Practices for Small Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
1– E-mail Protection Systems	1.S.A E-mail System Configuration	• Use strong/unique username and passwords with MFA	PR.DS-2, PR.IP-1, PR.AC-7
2 – Endpoint Protection Systems	2.S.A Basic Endpoint Protection	• Deploy anti-malware detection and remediation tools	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3
3 – Access Management	3.S.A Basic Access Management	• Limit users who can log in from remote desktops	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7
5 – Asset Management	5.S.A Inventory	• Maintain a complete and updated inventory of assets	ID.AM-1
6 – Network Management	6.S.A Network Segmentation	• Separate critical or vulnerable systems from threats	PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3
7 – Vulnerability Management	7.S.A Vulnerability Management	• Ensure that users understand authorized patching procedures • Patch software according to authorized procedures	PR.IP-12
8 – Incident Response	8.S.A Incident Response	• Implement proven and tested incident response procedures	PR.IP-9
	8.S.B ISAC/ISAO Participation	• Establish cyber threat information sharing with other health care organizations	ID.RA-2

Ransomware Attack Mitigating Practices - 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.

Ransomware Attack Mitigating Practices - Medium/Large Organizations

Ransomware Attack Practices in *Technical Volume 2* can be found in **Cybersecurity #2, #3, #4, #5, #6, & #8** along with their corresponding sub-practices. 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 is interested in adopting them.

Cybersecurity Practice #2: Endpoint Protection	Cybersecurity Practice #3: Access Management	Cybersecurity Practice #4: Data Protection and Loss Prevention	Cybersecurity Practice #5: Asset Management	Cybersecurity Practice #6: Network Management	Cybersecurity Practice #8: Incident Response
Basic Endpoint Protection Controls	Provisioning, Transfers and De-Provisioning Procedures	Data Use Procedures	Inventory of Endpoints and Severs	Network Segmentation	Incident Response
	Authentication	Data Security		Additional Network Segmentation (Large)	Information Sharing and ISACs/ISAOs
	Single-Sign On (Large)				

Ransomware Attack Mitigating Practices -Medium Organizations

Medium-sized organizations should consider, at minimum, implementing the *Sub-Practices for Medium-Sized Organizations* discussed in each cybersecurity practice presented in this volume.

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #2 for Medium Organizations in Technical Volume 2.**

Basic Endpoint Controls

➢Antivirus	▪Push AV packages out using endpoint management systems that interface with Windows and Apple operating systems (OS) ➢Develop metrics to monitor the status of AV engines, signature updates and health
➢Full Disk Encryption	➢Connect encryption management to endpoint management systems that interface with both Windows and Apple OS. ➢Develop metrics to monitor the status of encryption.
➢Hardened Baseline Images	➢Enable local firewalls and limit inbound access to the endpoint to only required ports. ➢Prevent software from auto-running/starting, especially when using thumb drives.
➢Patching	➢Automatically update and distribute patches to third-party applications that are known to be vulnerable, such as internet browsers, Adobe Flash, Acrobat Reader, and Java.
➢Local Administrative Rights	➢Limit local administrative rights deployed to endpoints. Use endpoint management systems to install new programs and patch systems.

Ransomware Attack Mitigating Practices for Medium/Large Organizations

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity #3, and #6**

Cybersecurity #3 Sub Practice B: Provisioning, Transfers and Deprovisioning Procedures

- After you establish digital identities and user accounts, you must provision users with access to information systems prior to using them. HIPAA describes key principle of *minimum necessary*, which states that organizations should take reasonable steps to limit uses, disclosures, or requests of PHI to the minimum required to accomplish the intended purpose. This same principle applies to reducing the attack surface of potentially compromised user accounts.

Cybersecurity #3 Sub Practice C: Provisioning, Transfers and Deprovisioning Procedures Authentication

- User accounts must engage in authentication to properly assert the user's identity in the digital ecosystem. Organizations should develop solid password authentication practices, which include Centralized Authentication, Privileged Account Management, Local Application Authentication, and Monitoring of Authentication Attempts

Cybersecurity #6 Sub Practice A (large): Additional Network Segmentation

- *Required VPN access for data center:* Consider implementing a VPN, or bastion hosts, that must be enabled before access is granted to privileged servers in the data center. These VPN or bastion hosts should be equipped with MFA. Only authorized IT administrators should be granted access. Logs should be routed to the SOC for monitoring

Ransomware Attack Mitigating Practices – Medium Organizations

Threat 2: Ransomware Attack | Sub-Practices for Medium Organizations

Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
2 – Endpoint Protection Systems	2.M.A Basic Endpoint Protection Controls	Deploy anti-malware detection and remediation tools	PR.IP-1, DE.CM-4, PR.DS-1, PR.IP-12, PR.AC-4
3 – Access Management	3.M.B Provisioning, Transfers and De-Provisioning Procedures	Limit users who can log in from remote desktops	PR.AC-4
3 – Access Management	3.M.C Authentication	Limit the rate of allowed authentication attempts to thwart brute-force attacks	PR.AC-7
4 – Data Protection and Loss Prevention	4.M.C Data Security	Be clear which computers may access and store sensitive or patient data	PR.DS, PR.DS-1, PR.DS-2, PR.IP-6, PR.DS-5
4 – Data Protection and Loss Prevention	4.M.D Backup Strategies	• Implement a proven and tested data backup and restoration test • Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up	PR.IP-4
5 – Asset Management	5.M.A Inventory of Endpoints and Servers	Maintain a complete and updated inventory of assets	ID.AM-1
6 – Network Management	6.M.B Network Segmentation	Separate critical or vulnerable systems from threats	PR.AC-5
8 – Incident Response	8.M.B Incident Response	Develop a ransomware recovery playbook and test it regularly	PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC
	8.M.C Information Sharing/ISACs/ISAOs	Establish cyber threat information sharing with other health care organizations	ID.RA-2

Ransomware Attack Mitigating Practices - Large Organizations

Threat 2: Ransomware Attack | Sub-Practices for Large Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
3 – Access Management	3.L.D Single-Sign On	Deploy anti-malware detection and remediation tools	PR.AC-7
6 – Network Management	6.L.A Additional Network Segmentation	Separate critical or vulnerable systems from threats	PR.AC-5, PR.AC-6, PR.PT-4

Ransomware Attack 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. For example, the metrics for **Cybersecurity Practice #2: Endpoint Protection** can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for Endpoint Protection Systems:

Percentage of Endpoints Encrypted 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 Nonhardened Images Each Month
• The first goal is to achieve a high percentage of encryption, somewhere around 99 percent. Achieving 100 percent encryption is nearly impossible, because defects always exist. Additionally, the percentage of endpoints encrypted will vary as you discover new assets, which is why you should measure it weekly.	• The first goal is to achieve a high percentage of success. Secondary goals are to ensure that there are practices to patch endpoints for third-party and OS-level application vulnerabilities, and to be able to determine the effectiveness of those patches. Without the metric, there might not be checks and balances in place to ensure satisfactory compliance with expectations.	• The goal is to ensure that practices are in place to respond to AV alerts that are not automatically quarantined or protected. Such alerts indicate that there could be active malicious action on an endpoint. An endpoint with an active threat should be reimaged using general IT practices and managed using a ticketing system.	• The goal is to check assets for compliance with the full set of IT management practices, identifying assets that do not comply. To do this, place a key or token on the asset indicating that it is managed through a corporate image. Separate practices are necessary for assets that are not managed this way to ensure that they are properly hardened.

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

Upcoming HICP Engagements

Upcoming Five Threats Schedule

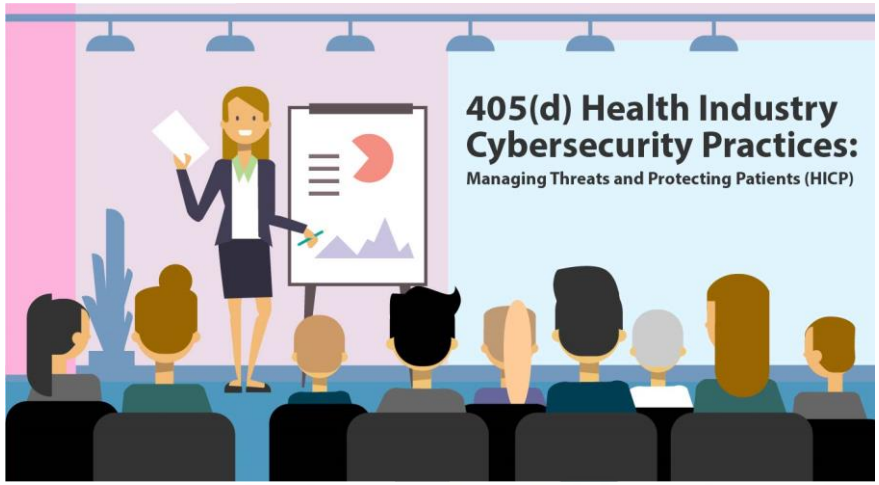
The Five Threats Series continues next week! Please join us for the upcoming Five Threat webinars to learn more about each of the Threats and the practices you can take to mitigate them.

- **Remaining Five Threats Webinars**
  - Week 3/Threat 3 – Loss or Theft of Equipment or Data: **April 2 & 4, 2019**
  - Week 4/Threat 4 – Insider, Accidental or Intentional Data Loss: **April 9 & 11, 2019**
  - Week 5/Threat 5 – Attacks Against Connected Medical Devices: **April 16 & 18, 2019**
- **Want to Receive Five Threats related Communication?**
  - Visit the 405(d) website and sign up to receive email notifications from us regarding the 5 Threat Weekly Series and other related information

Come Hear Us Speak

Throughout 2019 the 405(d) Team will be traveling around the country and speaking at different industry focused conferences to promote our collaborative initiative and deliver in-person awareness of the HICP publication. Here is a few of our upcoming conferences:

- H-ISAC Spring Summit – May 13-17 Jacksonville, FL
- Healthcare Innovation Health IT Summits – June 3-4 Philadelphia, PA & June 13-14 Nashville, TN
- American Hospital Association Leadership Conference - July 25-27 San Diego, CA



Questions

Thank you for Joining Us

Visit us at: www.phe.gov/405d

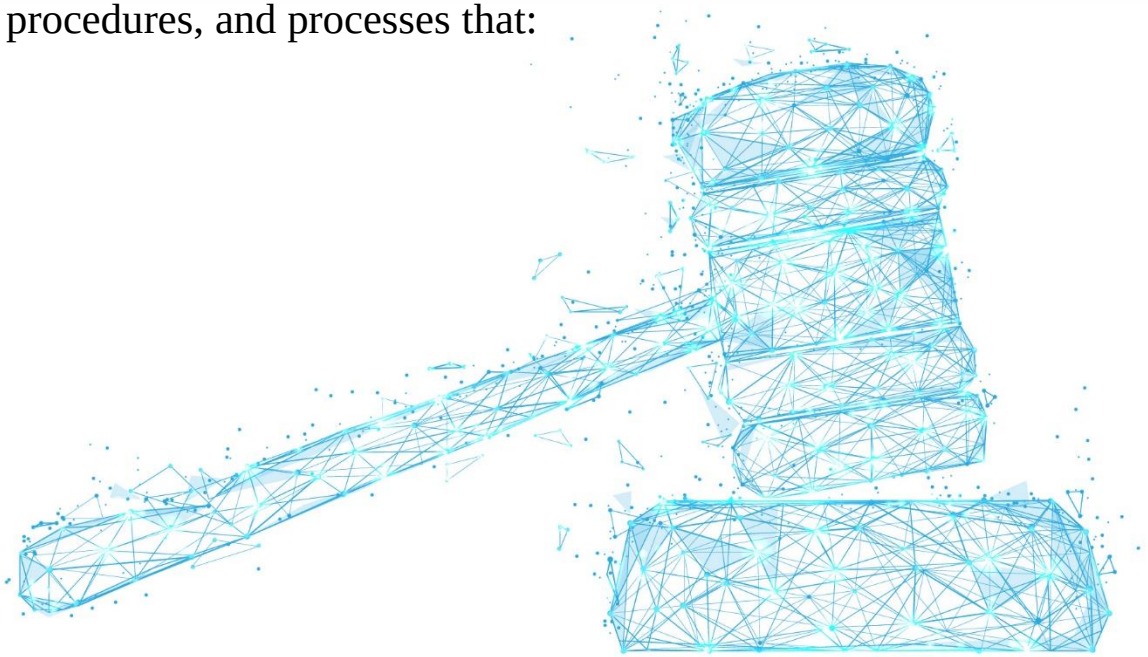
Contact Us at: CISA405d@hhs.gov

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 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

Ransomware Attacks: Direct Mitigating Sub-Practices (S)

The below table lists all of the **direct** Sub-Practices for small organizations to mitigate Threat 1: Ransomware Attacks, 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
1.S.A	Email System Configuration	Basic email security controls to enable
1.S.B	Education	Training of workforce on phishing attacks
1.S.C	Phishing Simulations	Conduct phishing campaigns to test and training users
2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
6.S.A	Network Segmentation	Segment devices into various networks, restricting access
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

Ransomware Attacks: Indirect Mitigating Sub-Practices (S)

The below table lists all of the **indirect** Sub-Practices for small organizations to mitigate Threat 1: Ransomware Attacks, 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.S.A	Basic Access Management	Basic user account configuration and provisioning procedures
4.S.C	Education	Training workforce on how to handle sensitive data
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
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
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

Ransomware Attacks: Direct Mitigating Sub-Practices (M)

The below table lists all of the **direct** Sub-Practices for medium organizations to mitigate Threat 1: Ransomware Attacks, 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
1.M.A	Basic Email Protection Controls	Basic email security controls to enable
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
1.M.D	Workforce Education	Educating workforce on spotting and reporting email based attacks
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources
4.M.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data
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
6.M.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies
7.M.A	Host/Server Based Scanning	Discover host based technical vulnerabilities
7.M.B	Web Application Scanning	Discover web 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

Ransomware Attacks: Indirect Mitigating Sub-Practices (M)

The below table lists all of the **indirect** Sub-Practices for medium organizations to mitigate Threat 1: Ransomware Attacks, 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.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
4.M.E	Data Loss Prevention (DLP)	Implement technology and processes to automate security of sensitive data
5.M.A	Inventory of Endpoints and Servers	Establish an asset management inventory database and roll out
5.M.B	Procurement	Keep asset inventory up to date with procurement of new devices
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
7.M.C	System Placement and Data Classification	Determine vulnerability risk based on system classification and location
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
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
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices

Ransomware Attacks: Indirect Mitigating Sub-Practices (L)

The below table lists all of the **direct** & **indirect** Sub-Practices for large organizations to mitigate Threat 1: Ransomware Attacks, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

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

Ransomware Attacks: Direct Mitigating Sub-Practices (L)

SP#	SP Title	Short Description
1.M.A	Basic Email Protection Controls	Basic email security controls to enable
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
1.M.D	Workforce Education	Educating workforce on spotting and reporting email based attacks
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources
4.M.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data
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
6.M.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies
7.M.A	Host/Server Based Scanning	Discover host based technical vulnerabilities
7.M.B	Web Application Scanning	Discover web 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
1.L.A	Advanced and Next Generation Tooling	Advanced email security configurations to enable
2.L.A	Automate the Provisioning of Endpoints	Leverage VARs to preconfigure and secure new endpoints
2.L.C	Host Based Intrusion Detection/Prevention Systems	Install host based protection systems to detect and prevent client-based attacks
2.L.D	Endpoint Detection Response	Detect malicious processes running on endpoints; respond at scale
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.D	Single-Sign On (SSO)	Authenticate against central credential repositories and ease access burdens
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.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.C	Incident Response Orchestration	Automate the manual response of IR playbooks through advanced tools
8.L.F	Deception Technologies	Establish 'tripwires' or honeypots on your network and alert when they are tripped

Ransomware Attacks: Indirect Mitigating Sub-Practices (L)

SP#	SP Title	Short Description
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
4.M.E	Data Loss Prevention (DLP)	Implement technology and processes to automate security of sensitive data
5.M.A	Inventory of Endpoints and Servers	Establish an asset management inventory database and roll out
5.M.B	Procurement	Keep asset inventory up to date with procurement of new devices
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
7.M.C	System Placement and Data Classification	Determine vulnerability risk based on system classification and location
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
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
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices
1.L.B	Digital Signatures	Leverage digital signatures to ensure sender authenticity
1.L.C	Analytics Driven Education	Leverage data and analytics to determine high risk and targeted users, drive education
2.L.B	Mobile Device Management	Leverage MDM tools to secure mobile devices
2.L.F	Micro-segmentation/virtualization strategies	Implement endpoint virtualization and prevent malcode from infecting OS
3.L.A	Federated Identity Management	Leverage external org identity information for access
3.L.C	Access Governance	Review access periodically to ensure user access still appropriate
4.L.A	Advanced Data Loss Prevention	Implement advanced technology and processes to automated security of data
5.L.A	Automated Discovery and Maintenance	Leverage automation to keep asset inventory details up to date
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
8.L.B	Advanced Information Sharing	Share and receive threat intelligence information from partner organizations
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
9.L.A	Vulnerability Management	Carefully identify vulnerabilities on medical devices, and remediate accordingly
9.L.C	Procurement and Security Evaluations	Conduct security evaluations for newly purchased medical devices