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	Mitch Thomas
5 Minutes	HICP Overview	Mitch Thomas
10 Minutes	Using HICP and Supporting Resources	Mitch Thomas
40 Minutes	Threat 4 – Insider, Accidental or Intentional Data Loss and Mitigating Practices	William Welch/Mitch Thomas
5 Minutes	Looking Forward	William Welch
5 Minutes	Upcoming 5 Threats	William Welch
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

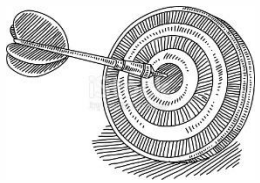
WHAT IS THE 405(d) EFFORT?

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

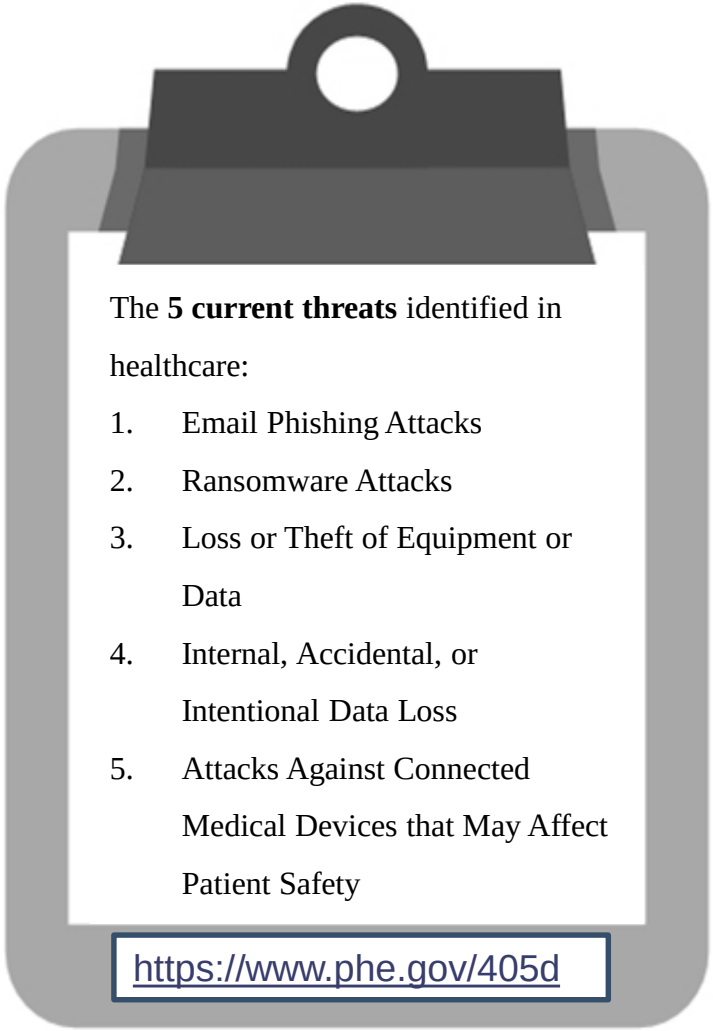
OFFICE OF THE CHIEF INFORMATION OFFICER

HICP Publication Overview

Document - Content Overview (1/2)

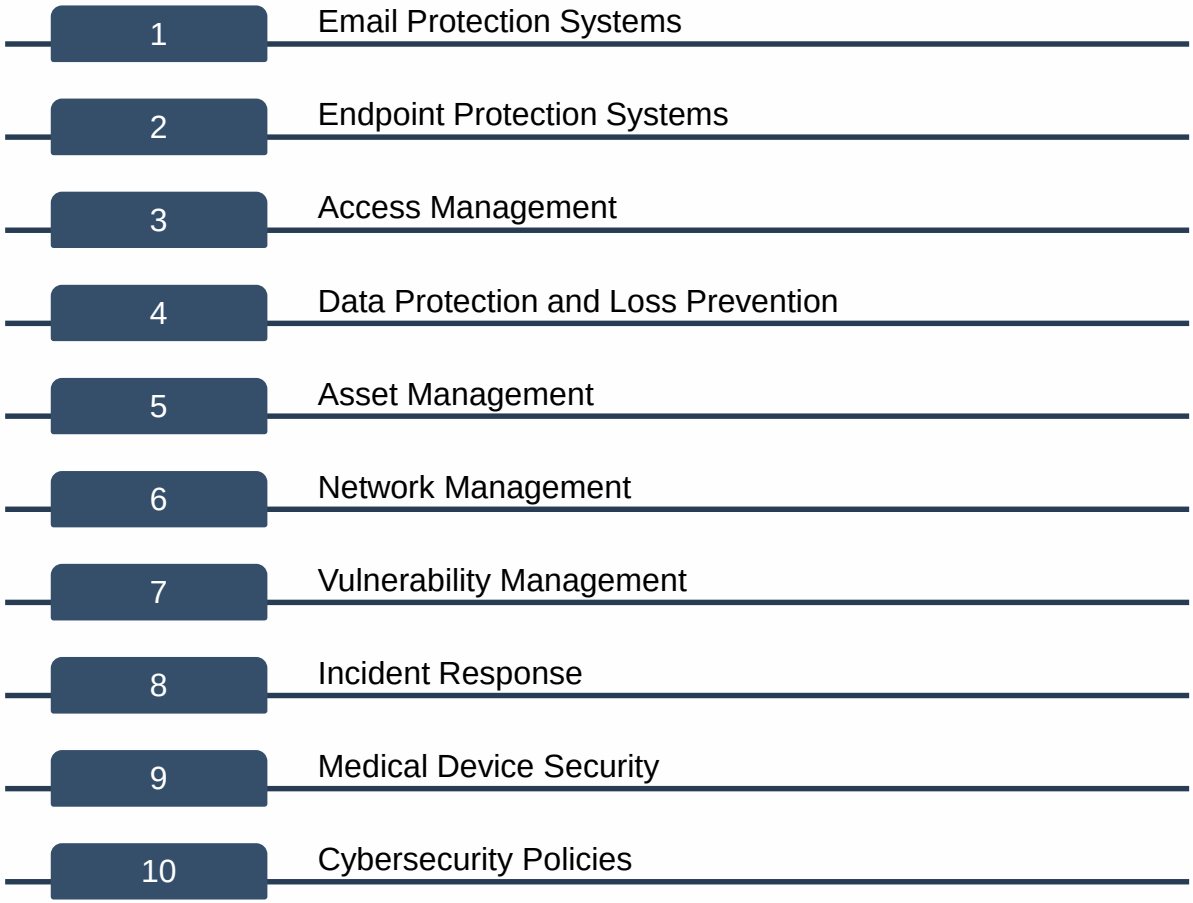
After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- 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

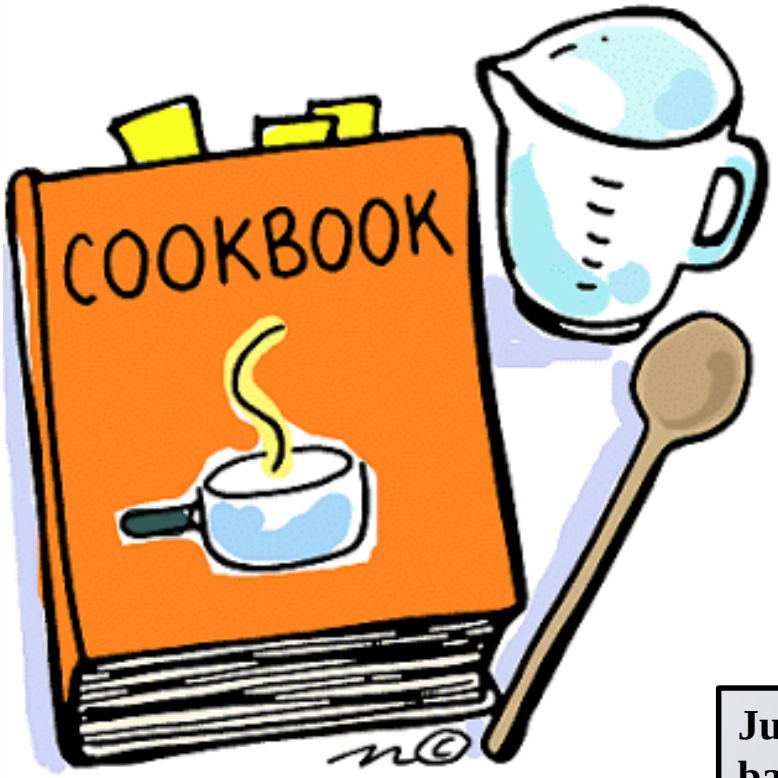
HICP is…

- 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 4 – Insider, Accidental or Intentional Data Loss

Cybersecurity Practice #4 Data Protection and Loss Prevention

What is Insider, Accidental or Intentional Data Loss?

Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases. There are two types of insider threats: accidental and intentional. An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. For example, mishandling data—sending it out to an unauthorized party by mistake is an accidental insider threat.

An intentional insider threat is malicious loss or theft caused by an employee, contractor, other user of the organization's technology infrastructure, network, or databases, with an objective of personal gain or inflicting harm to the organization or another individual.

Insider, Accidental or Intentional Data Loss Scenario

- **Real-World Scenario:** An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.
- **Impact**: The patient's PHI was compromised and used in an identity theft case.

Understanding Why Data Protection and Loss Prevention is Vital

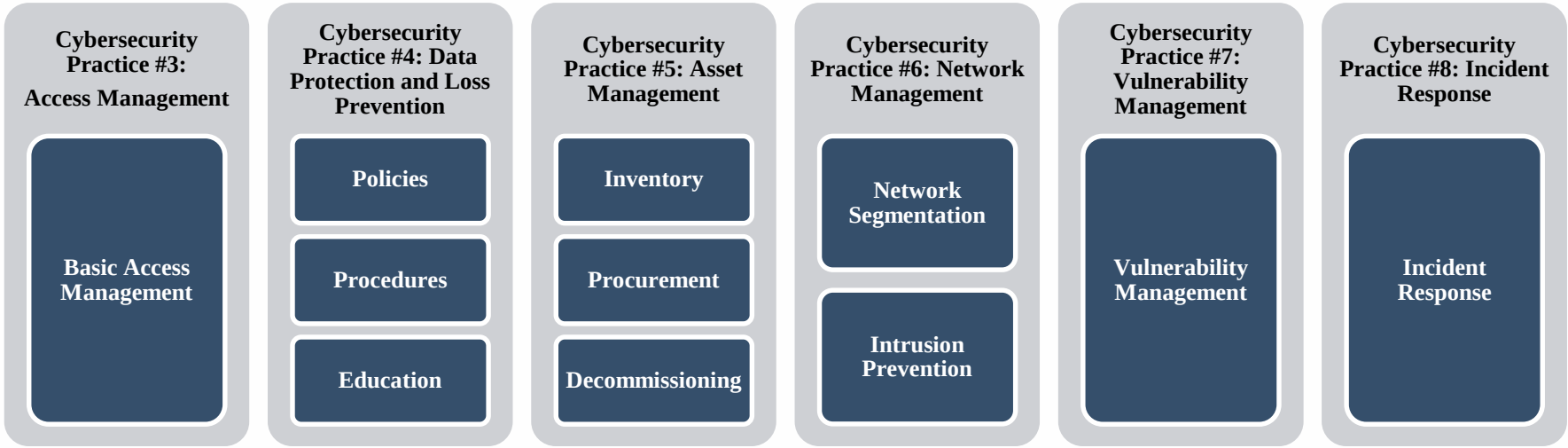
- All organizations within the health sector access, process, and transmit sensitive information, such as health information or PII. The fundamental data used in operations are highly sensitive, representing a unique challenge to the HPH sector. Most of the health care workforce must leverage these data to carry out their respective missions.
- In that context, healthcare faces a growing challenge of understanding where data assets exist, how they are used, and how they are transmitted. PHI is discussed, processed, and transmitted between information systems daily. Protecting these data requires robust policies, processes, and technologies.
- Impacts to the organization can be profound if data are corrupted, lost, or stolen. Security breaches may prevent users from completing work accurately or on time, and could result in potentially devastating consequences to patient treatment and well-being

Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, (NIST Special Publication 800-122, April, 2010, Gaithersburg, MD), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

Insider, Accidental or Intentional Data Loss 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.

The loss of sensitive data can be prevented in several ways. Data loss prevention is based on understanding where data resides, where it is accessed, and how it is shared. The Insider, Accidental or Intentional Data practices in Technical Volume 1 can be found in **Cybersecurity Practice #3, 4, 5, 6, 7, 8**



Insider, Accidental or Intentional Data Loss Mitigating Practices - Small Organizations

For each Sub-Practice, *Technical Volume 1* provides:

- Considerations your organization can take to enhance the security posture
- Implemental education and awareness activities that can assist your employees and partners in protecting your organization against Insider, Accidental or Intentional Data Loss

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #3, & #4.**

Policies

- Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost compromised data.
- Establish a data classification policy that categorizes data as, for example, Sensitives, Internal Use, or Public Use. Identify the types of records relevant to each category.

Procedures

- Procedures to manage sensitive data can ensure consistency, reduce errors, and provide clear and explicit instructions. Train your workforce to comply with organizational procedures and ONC guidance when transmitting PHI through e-mail. Encrypt PHI sent via e-mail or text, unless patients expressly authorize their PHI to be e-mailed or texted to them.
- When e-mailing PHI, use a secure messaging application such as Direct Secure Messaging (DSM), which is a nationally adopted secure e-mail protocol and network for transmitting PHI.

Education

- Train personnel to comply with organizational policies. At minimum, provide annual training on the most salient policy considerations, such as the use of encryption and PHI transmission restrictions.

Basic Access Management

- Basic user account configuration and provisioning procedures

Insider, Accidental or Intentional Data Loss Mitigating Practices - Small Organizations

Here are just a few more examples of what can be found within the sub-practices of **Cybersecurity Practice #6 & #7.**

Network Segmentation

- Segment devices into various networks, restricting access

Intrusion Prevention

- Implement and operate an IPS system to stop well known cyber attacks

Vulnerability Management

- Discover technical vulnerabilities (host and web) and remediate

Insider, Accidental or Intentional Data Loss Mitigating Practices - Small Organizations

Threat 4: Insider, Accidental or Intentional Data Loss | Sub-Practices for Small Organizations				
Cybersecurity Practice	Sub-Practice		Short Description	NIST Framework Ref
3	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7
4	4.S.A	Policies	Establishing a data classification policy	ID.GV-1, ID.AM-5
4	4.S.B	Procedures	Procedures for handling sensitive information, pursuant to Data Classification Policy	ID.GV-1, PR.AT-1, PR.DS-2, PR.DS-5, PR.DS-1, PR.IP-6, ID.GV-3
4	4.S.C	Education	Training workforce on how to handle sensitive data	PR.AT
5	5.S.A	Inventory	Conduct and manage an inventory of IT Assets	ID.AM-1
5	5.S.B	Procurement	Keep asset inventory up to date with procurement of new devices	ID.AM-6
5	5.S.C	Decommissioning	Securely remove devices from the circulation	PR.IP-6, PR.DS-3
6	6.S.A	Network Segmentation	Segment devices into various networks, restricting access	PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3
6	6.S.C	Intrusion Prevention	Implement and operate an IPS system to stop well known cyber attacks	PR.IP-1
7	7.S.A	Vulnerability Management	Discover technical vulnerabilities (host and web) and remediate	PR.IP-12
8	8.S.A	Incident Response	Establish procedures for managing cyber-attacks, especially malware and phishing	PR.IP-9

Insider, Accidental or Intentional Data Loss 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.

Insider, Accidental or Intentional Data Loss Mitigating Practices for Medium/Large Organizations

The Data Protection and Loss Prevention practices in *Technical Volume 2* can be found in **Cybersecurity Practice #1, #3, & #4.** 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: E-mail Protection Systems

- Workforce Education

Cybersecurity Practice #3: Access Management

- Provisioning, Transfers, and De-Provisioning Procedures
- Authentication

Cybersecurity Practice #4: Data Protection and Loss Prevention

- Data Loss Prevention
- Advanced Data Loss Prevention (Large)

Insider, Accidental or Intentional Data Loss Mitigating Practices for Medium/Large Organizations

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #3 & #4.**

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

- After you establish digital identities and user accounts, you must provision users with access to information systems prior to using them. It is important to ensure that provisioning processes follow organizational policies and principles, especially in the healthcare environment. 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.

Cybersecurity Practice #4 Sub Practice E: Data Loss Prevention

- Once standard data policies and procedures are established and the workforce is trained to use them, DLP systems should be implemented to ensure that sensitive data are used in compliance with these policies.

Cybersecurity Practice #4 Sub Practice A Large: Advanced Data Loss Prevention

- After implementing basic DLP controls, you should consider expanding your DLP capabilities to monitor other common data access channels. Recommends methods for your consideration include Ensure that cloud-based file storage and sharing systems do not expose sensitive data in an "open sharing" construct without authentication (i.e., do not permit the use of sharing data through a simple URL link).

Insider, Accidental or Intentional Data Loss Mitigating Practices for Medium Organizations

Threat 4: Insider, Accidental or Intentional Data Loss | Sub-Practices for Medium Organizations			
Cybersecurity Practice	Sub-Practice		NIST Framework Ref
1 – E-mail Protection Systems	1.M.D Workforce Education	Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors	PR.AT-1
3 – Access Management	3.M.B Provisioning, Transfers and De-Provisioning Procedures	Implement and use workforce access auditing of health record systems and sensitive data	PR.AC-4
	3.M.C Authentication	Implement and use privileged access management tools to report access to critical technology infrastructure and systems	PR.AC-7
4 – Data Protection and Loss Prevention	4.M.E Data Loss Prevention	Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads	PR.DS-5

Insider, Accidental or Intentional Data Loss Mitigating Practices for Large Organizations

Threat 4: Insider, Accidental or Intentional Data Loss | Sub-Practices for Large Organizations			
Cybersecurity Practice	Sub-Practice		NIST Framework Ref
4 – Data Protection and Loss Prevention	4.L.A Advanced Data Loss Prevention	Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads	PR.DS-5

Insider, Accidental or Intentional Data Loss 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 **Cybersecurity Practice #4 Data Protection and Loss Prevention** can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for Ransomware Attack:

Number of encrypted e-mail messages, trended by week	Number of blocked e-mail messages, trended by week	Number of files with excessive access on the file systems, trended by week	Number of unencrypted devices with access attempts, trended by week
• The goal is to establish a baseline of encrypted messages sent. Be on the lookout for spikes of encryption (which could indicate data exfiltration) and no encryption (which could indicate that encryption is not working properly).	• The goal is to detect large numbers of blocked messages, which could indicate potential malicious data exfiltration or user training.	• The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets, and deliver to access management.	• The goal is to use this information to educate the workforce on the risks of removable media..

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

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

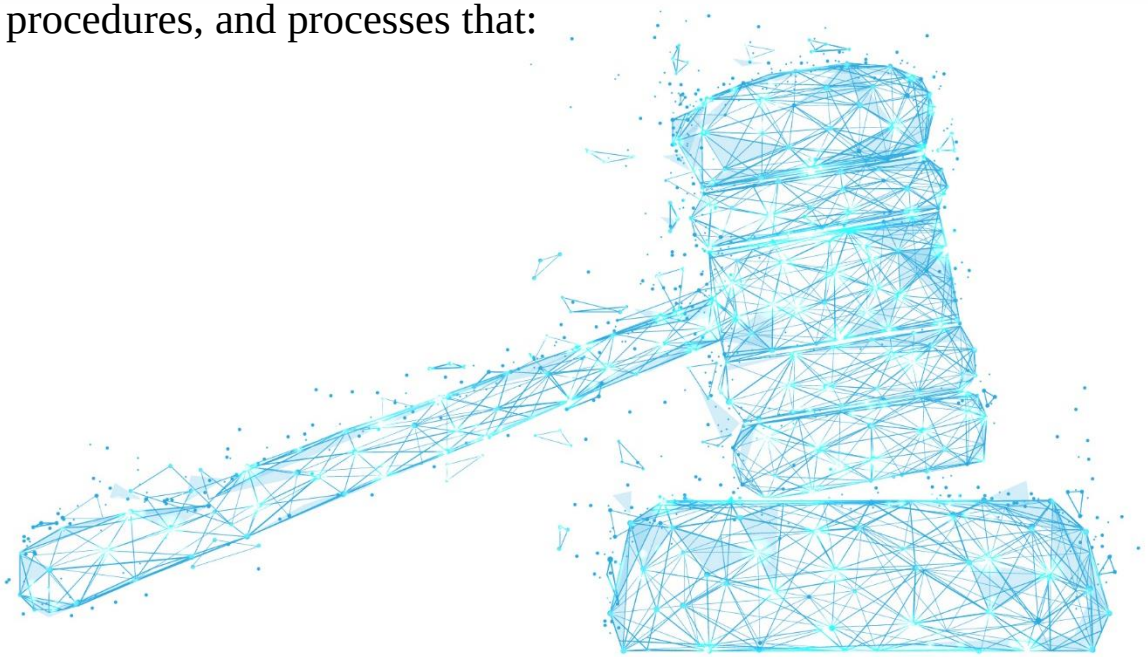
Contact Us at: CISA405d@hhs.gov

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:



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

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*.

Insider, Accidental or Intentional Data Loss: Direct Mitigating Sub-Practices (S)

The below table lists all of the **direct** Sub-Practices for small organizations to mitigate Threat 4: Internal, Accidental or Intentional Data Loss, 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.A	Policies	Establishing a data classification policy
4.S.B	Procedures	Procedures for handling sensitive information, pursuant to Data Classification Policy
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
5.S.C	Decommissioning	Securely remove devices from the circulation
6.S.A	Network Segmentation	Segment devices into various networks, restricting access
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

Insider, Accidental or Intentional Data Loss: Indirect Mitigating Sub-Practices (S)

The below table lists all of the **indirect** Sub-Practices for small organizations to mitigate Threat 4: Internal, Accidental or Intentional Data Loss, 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.B	Physical Security and Guest Access	Physically secure servers and network devices, and segment guest access from regular network
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

Insider, Accidental or Intentional Data Loss: Direct Mitigating Sub-Practices (M)

The below tables lists all of the **direct and indirect** Sub-Practices for medium organizations to mitigate Threat 4: Internal, Accidental or Intentional Data Loss, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

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

Insider, Accidental or Intentional Data Loss: Direct Mitigating Sub-Practices (M)

SP#	SP Title	Short Description
1.M.C	Email Encryption	Use of email encryption for sending sensitive information
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
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.A	Classification of Data	Classify data by sensitivity
4.M.B	Data Use Procedures	Implement data use procedures based upon data classification
4.M.C	Data Security	Implement data protections based upon data classification
4.M.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data
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.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones
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

Insider, Accidental or Intentional Data Loss: Indirect Mitigating Sub-Practices (M)

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.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
5.M.C	Secure Storage for Inactive Devices	Ensure unused devices are physically secure
6.M.A	Network Profiles and Firewalls	Deploy firewalls throughout the network
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.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

Insider, Accidental or Intentional Data Loss: Direct Mitigating Sub-Practices (L)

The below table lists all of the **direct and indirect** Sub-Practices for large organizations to mitigate Threat 4: Internal, Accidental or Intentional Data Loss, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

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

Insider, Accidental or Intentional Data Loss: Direct Mitigating Sub-Practices (L)

SP#	SP Title	Short Description
1.M.C	Email Encryption	Use of email encryption for sending sensitive information
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
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.A	Classification of Data	Classify data by sensitivity
4.M.B	Data Use Procedures	Implement data use procedures based upon data classification
4.M.C	Data Security	Implement data protections based upon data classification
4.M.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data
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.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones
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
4.L.A	Advanced Data Loss Prevention	Implement advanced technology and processes to automated security of data
4.L.B	Mapping of Data Flows	Identify and document data storage and data flows between systems
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.D	Network Based Sandboxing/Malware Execution	Monitor common transfer protocols to discover malicious attachments
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

Insider, Accidental or Intentional Data Loss: Indirect 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.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
5.M.C	Secure Storage for Inactive Devices	Ensure unused devices are physically secure
6.M.A	Network Profiles and Firewalls	Deploy firewalls throughout the network
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.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.A	Advanced and Next Generation Tooling	Advanced email security configurations to enable
1.L.C	Analytics Driven Education	Leverage data and analytics to determine high risk and targeted users, drive education
2.L.A	Automate the Provisioning of Endpoints	Leverage VARs to preconfigure and secure new endpoints
2.L.B	Mobile Device Management	Leverage MDM tools to secure mobile devices
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.A	Federated Identity Management	Leverage external org identity information for access
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
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.E	Network Access Control (NAC)	Ensure endpoints are secure on the network through automated tools
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