Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

2023 Edition

Healthcare & Public Health Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

This page intentionally left blank.

Table of Contents

Disclaimer 1

Letter from the HHS Deputy Secretary 2

Executive Summary 3
Call to Action: Cybersecurity, a Priority for Patient Safety 3
Why Cyber Safety is Patient Safety 3
In The News 5
Can It Happen to Me? 6

Cybersecurity in the Workplace 7
Effective Cybersecurity is a Shared Responsibility 7
The Human Element 8
Be Proactive: Hand Hygiene for Cybersecurity 9

How to Use this Publication 10
The Publication: Health Industry Cybersecurity Practices (HICP) 10
Audience and Publication Components 10
Cybersecurity Threats and Mitigation Practices 11
How Does this Publication Help Me? 12
Where Do I Fit? 12
HICP & Cybersecurity Strategy Approaches 14
The Zero Trust Strategy 14
Defense-in-Depth 15

Current Threat Scenarios Facing the HPH Sector 16
Explaining Threats and Vulnerabilities 16
A Translation: Threats, Vulnerabilities, Impact, and Practices 16
Introducing Current Threats to the HPH Sector 17

Threat: Social Engineering 18

Threat: Ransomware Attack 21

Threat: Loss or Theft of Equipment or Data 24

Threat: Insider, Accidental or Malicious Data Loss 27

Threat: Attacks Against Network Connected Medical Devices 29

Looking Ahead 32

Acknowledgements 33
Original Publication 33
2023 Edition 33

Appendix A: Overview of Technical Volumes and Practices 34

Appendix B: 405(d) Program and History 39
Cybersecurity Act of 2015: Task Group Undertakes a Legislative Mandate 39
405(d) and the Health Sector Coordinating Council 39
Aligning Healthcare Industry Security Approaches 40

Appendix C: Acronyms and Abbreviations 41

Appendix D: References 43

List of Tables

Table 1. Selecting the "Best Fit" For Your Organization 13
Table 2. Threat Profile: Social Engineering 20
Table 3. Threat Profile: Ransomware Attack 23
Table 4. Threat Profile: Loss or Theft of Equipment or Data 26
Table 5. Threat Profile: Insider, Accidental or Malicious Data Loss 28
Table 6. Threat Profile: Attacks Against Network Connected Medical Devices That May Affect Patient Safety 30
Table 7. Cybersecurity Practices and Sub-Practices for Small Organizations 35
Table 8. Cybersecurity Practices and Sub-Practices for Medium-Sized Organizations 36
Table 9. Cybersecurity Practices and Sub-Practices for Large Organizations 37

Disclaimer

This document is provided for informational purposes only. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all healthcare providers and organizations. This document is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.

Letter from the HHS Deputy Secretary

Cyber-attacks are an increasing threat across all critical infrastructure sectors. For the health sector, cyber-attacks are especially concerning as they can directly threaten not just the security of our systems and information, but also the health and safety of the American public. While innovation and increasing sophistication in health information technology is a cause for optimism and holds the promise to help address some our most intractable problems, whether in clinical care, fundamental research, population health or health system design, our technology will work for us only if it is secure. Information systems are crucial to today and tomorrow's healthcare system, so we must take every step possible to protect them.

The U.S. Department of Health and Human Services (HHS) maintains a holistic view of the intersection between cybersecurity and healthcare, including data protection and response to cyber threats. Cybersecurity is no longer a one-step solution. Rather, it is vital that the entire Healthcare and Public Health Sector (HPH) sector has a cybersecurity strategy, including a zero trust approach. Healthcare Delivery Organizations (HDOs) need to make bold changes and significant investments to defend the institutions that make up the HPH sector. Cybersecurity remains a top priority at HHS. We are committed to partnering with the health sector to make sure they are prepared and have the tools they need to develop these strategies, protecting us from evolving cyber threats. This is reflected in our dedication to the 405(d) Program and the 405(d) Task Group efforts, including the release of this update to our cornerstone publication, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP).

HHS' commitment began in 2017 with the establishment of the 405(d) Task Group. The 405(d) Task Group includes thought leaders from across the HPH sector. This group collaborated to provide the sector with practical, understandable, implementable, industry-led, voluntary, and consensus-based cybersecurity guidelines to cost-effectively reduce cybersecurity risks for healthcare organizations of varying sizes. Since the first publication was released in 2018, HHS has witnessed its impact on the sector as entities implement HICP best practices (and help their staff remain aware of threats) by using the 405(d) Program's vast collection of cyber awareness materials. HHS is dedicated to assisting the sector with their cybersecurity needs and will continue this public-private partnership not only to deliver in-depth technical publications, but also build cybersecurity awareness and offer training to the sector. Cybersecurity is not simply an IT issue; it is an enterprise-wide issue that must be addressed by everyone in an organization, from healthcare professionals to administrators and executives.

Due to the outstanding work of the 405(d) Program and Task Group, Congress passed H.R. 7898 (public law PL 116-321), which includes "approaches promulgated under Section 405(d) of the Cybersecurity Act of 2015" as types of "recognized security practices." HHS would like to acknowledge the public-private partnership of the 405(d) Task Group for their hard work, dedication, and willingness to collaborate with HHS to develop cybersecurity resources, products, and tools. The enactment of this bill not only highlights the work of the 405(d) Task Group and all its efforts, it is also another step forward in encouraging HPH entities to continue to focus on cybersecurity practices that will help protect their organizations and their patients.

We have seen progress since the 405(d) Program's inception in 2017. However, in cybersecurity, our work is never finished. I encourage anyone interested in cybersecurity and patient safety to get involved. Through the 405(d) Program, HHS will continue to build partnerships with stakeholders, becoming a better, more synchronized team. Together, we can take on the cybersecurity challenges that lie ahead.

/s/ Andrea Palm
Deputy Secretary of Health and Human Services

Executive Summary

Call to Action: Cybersecurity, a Priority for Patient Safety

Cybersecurity threats to healthcare organizations and patient safety are real. Health IT provides critical life-saving functions. It consists of connected, networked systems and leverages wireless technologies, leaving such systems more vulnerable to cyber-attack. Recent highly publicized ransomware attacks on hospitals, for example, necessitated diverting patients to other hospitals. This led to an inability to access patient records to continue care delivery. Such cyber-attacks can delay critical care, expose sensitive patient information, and lead to substantial financial costs to regain control of hospital systems and patient data. From small, independent practitioners to large, university hospital environments, cyber-attacks on healthcare records, IT systems, and network connected medical devices have impacted even the most hardened systems. It is for these reasons we consider Cyber Safety to be a part of Patient Safety.

Given the increasingly sophisticated and widespread nature of cyber-attacks, the HPH sector must make cybersecurity a priority and make the investments needed to protect its patients. Like combatting a deadly virus, cybersecurity requires mobilization and coordination of resources across myriad public and private stakeholders [including hospitals, IT vendors, connected medical device manufacturers, and governments (state, local, tribal, territorial, and federal)] to mitigate the risks and minimize the impacts of a cyber-attack. HHS and the HPH sector are working together to address these challenges.

Why Cyber Safety is Patient Safety

The HPH sector has become reliant on the digitization of data and automation of processes to maintain and share patient information and to deliver patient care more efficiently and effectively. Along with the benefits derived from healthcare technology, healthcare organizations have also become vulnerable to cyber-attacks on their computer systems and on the data contained therein. These vulnerabilities create significant risks with potential high-impact consequences for healthcare organizations, their business partners, and, particularly, their patients.

Most healthcare personnel are experts at identifying and eradicating viruses in patients, not computers. Cybersecurity is a problem that must be addressed by everyone in an organization, not just the IT or cybersecurity departments. Just as providing safe care to a patient requires a multidisciplinary team, so does ensuring safety of healthcare's digital ecosystem. Cybersecurity has expanded the scope of patient wellness to include protecting the technology, networks, and databases that enable uninterrupted

and accurate patient care. This includes securing computer systems, protecting patients' information, including PHI, and training personnel to be cyber-vigilant.

> Cyber-attacks disrupt healthcare personnel's ability to securely provide life-changing and life-saving capabilities.

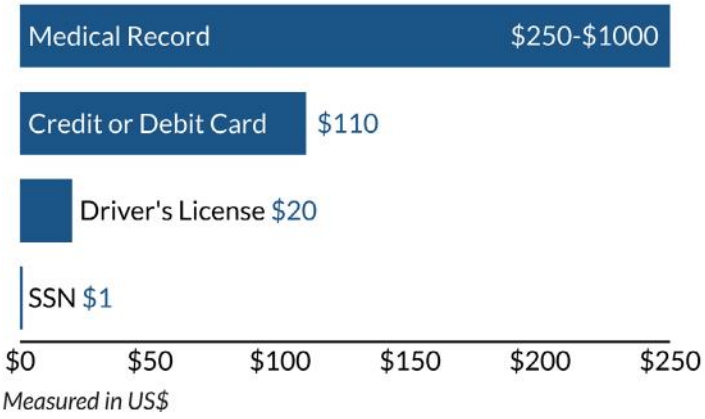
Cyber-attacks impede the ability to safely and appropriately disseminate patient data to other healthcare entities, which directly affects the delivery of accurate care. For example, a healthcare organization was victim to a ransomware attack, leading the organization to redirect ambulances as a safety measure. The attack compromised the entire Electronic Health Record (EHR) system (which supports the delivery of accurate care), and prompted the facility to take extra precautions just to guarantee quality care.

> Cybersecurity is an investment in patient safety.

Healthcare organizations are committed to providing the very best care to their patients. The thought of a cyber-attack risking patient safety is terrifying for any healthcare professional. However, it can be difficult to justify investments in cybersecurity when there are pressing opportunities to invest in equipment, materials, training, and personnel, which more visibly relate to patient care.

Healthcare records continue to be one of the most lucrative items on the underground market, ranging from $250 to $1,000 compared to other items like

Figure 1. Cost per piece of personal information on the Dark Web.[1]



credit cards only selling for an average $100.[1]

This demonstrates the value of data like Protected Health Information (PHI) to cyber-attackers and their motivation for attacking healthcare institutions.

Therefore, protecting a patient's health information and PHI is paramount at every level of an organization, from practitioners to executives. In the next section, you will read firsthand stories of how devastating a cyber-attack can be to patient care. The main take-away from this is that investing properly in cybersecurity protects your patients and organizations from the damaging effects even one cyber-attack can have.

> HHS wants to do everything it can to help the sector do what it does best—care for and protect patients.

In The News

News headlines continue to report major cyber-attacks on healthcare organizations. Following are three recently reported stories. *Details have been removed to protect the privacy of those involved.*

Ransomware Attack Affects Cancer Care During COVID-19 Pandemic

A ransomware attack on a major hospital system in 2021 resulted in the freeze of all computer systems, including all communication networks for patients and staff. The attack forced the hospital to disable internet access and prevented regular, large, and in-person meetings. During the downtime, the hospital had to revert to pen and paper operations to maintain patient and data records. The cyber-attack resulted in a 41% decrease in total outpatient volume which included a 39% decrease in new patient visits during the attack timeline. Federal and local law enforcement had to be notified and disaster recovery processes were implemented to bring the network back on-line. After five months of cyber response activities, the hospital was finally able to return to normal operations and could focus primarily on patient care.

FTA Hack—At Least 3.51 Million Records Stolen

In 2021, one of the largest healthcare data breaches was a hacking incident involving a firewall vendor. Four vulnerabilities in the legacy File Transfer Appliance (FTA) – used to transfer files too large to be sent via email- were exploited and more than 100 companies were affected, including at least 11 U.S. healthcare organizations. The attack was conducted by a threat actor linked to the Clop ransomware gang. Ransomware was not used in the attack, but sensitive data were stolen, ransom demands issued, and stolen data were leaked on the Clop ransomware gang's leak site.

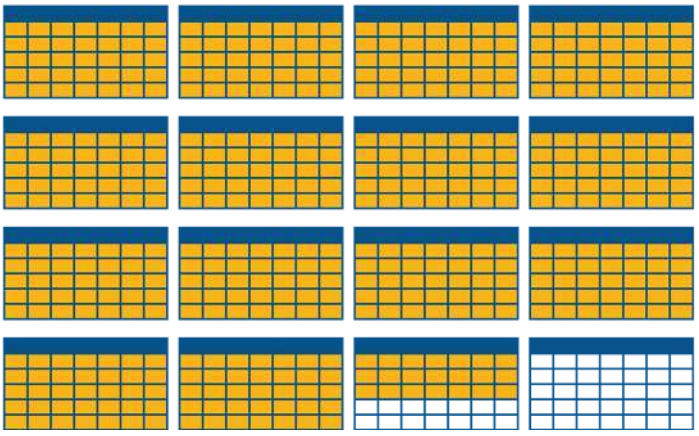
This FTA hack does not appear as a single incident on the HHS' Office for Civil Rights breach portal as each affected healthcare organization reported the breach separately. In total, the PHI of at least 3.51 million individuals is believed to have been stolen.

PHI Breach, Data Exfiltration Impacts 1.3 Million

A health system provided notice of an October 2021 healthcare data breach that exposed PHI and resulted in data exfiltration. A submission to the office of the attorney general revealed that the breach impacted 1,357,879 individuals. An unauthorized bad actor gained access to the health network through the office of a third-party medical provider. The exposed information included Social Security numbers, phone numbers, birth dates, addresses, email addresses, financial account information, insurance information and account numbers, medical record numbers, and driver's license numbers.

Just imagine for a moment that one of these news reports was about your organization. Cybersecurity is a challenge of technology and tactics. Organizations can meet this challenge by engaging their workforce with increased training and awareness, transparency, and coordination across the sector.

Figure 2. Healthcare had the **highest average time** to identify and contain a breach, at **329 days.**[2] This was the highest amount of time across all industry sectors.



Can It Happen to Me?

For those who own a healthcare practice or are part of a small to medium-sized healthcare organization, it is tempting to think that cyber-attacks only affect large hospitals and healthcare organizations. The reality is that cyber-attacks are indiscriminate and adversely affect healthcare practices of every size and specialization. The key risks are patient safety and care delivery. Cyber-attacks touch every level of an organization from the nurse floor to the board room, affecting many organizational roles:

- ***Executives:*** Impacting the organization's revenue and reputation.
- ***IT Professionals:*** Limiting the ability to maintain operations, critical infrastructure, and critical systems.
- ***Healthcare Professionals:*** Limiting access to data such as treatment regimens, medical history, prescriptions, and even making medical devices and equipment unavailable.

In 2021, compared to organizations in other industries, healthcare organizations experienced the highest average cost of a data breach for the eleventh year in a row. Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase.[3] The HPH sector is particularly susceptible, as criminals target valuable personal data that healthcare providers store and process.

Figure 3. Average loss per data breach.[3]

Attackers typically look for targets that require the least time, effort, and money to exploit. Do not make the mistake of thinking that your practice, no matter how small, is not a target for indiscriminate cyber-attacks.

Malicious actors will always exist. Whether you are a small-practice physician or the Chief Information Security Officer (CISO) of a large healthcare entity, your job is to make it difficult for these attackers to succeed.

Know your role. Utilize these resources (based on your role) to help navigate organizational cybersecurity:

- IT Professionals Leave Behind
- Practitioners Leave Behind

Use these quick start guides (based on your organization size) to help you get started with HICP:

- Quick Start Guide for Small Organizations
- Quick Start Guide for Medium/Large Organizations

Quick Start Guides

Cybersecurity in the Workplace

Effective Cybersecurity is a Shared Responsibility

Effective cybersecurity is a shared responsibility involving the people, processes, and technologies that protect digital data and technology investments. It is a constant battle, as attackers constantly find creative ways to defeat cyber threat defense initiatives. Healthcare organizations increasingly transmit data electronically—through mobile devices, cloud- based applications, network connected medical devices, and technology infrastructures.

Often, organizations deploy technologies without cybersecurity safeguards, or use them (maliciously or not) without proper protections, making them an appealing target for attackers. For example, the theft of a laptop (owned by a state healthcare transportation vendor) demonstrated that physical security controls and vendor management need adequate attention as cybersecurity priorities. As a result, the state's largest Medicaid coordinated care organization notified 654,000 patients their information could have been stolen.[4] The stolen device contained patient names, contact details, dates of birth, and Medicaid ID numbers, which put patients at risk for identity theft and further cybercrimes. Cybersecurity, physical security, and vendor management are all part of a robust cybersecurity program.

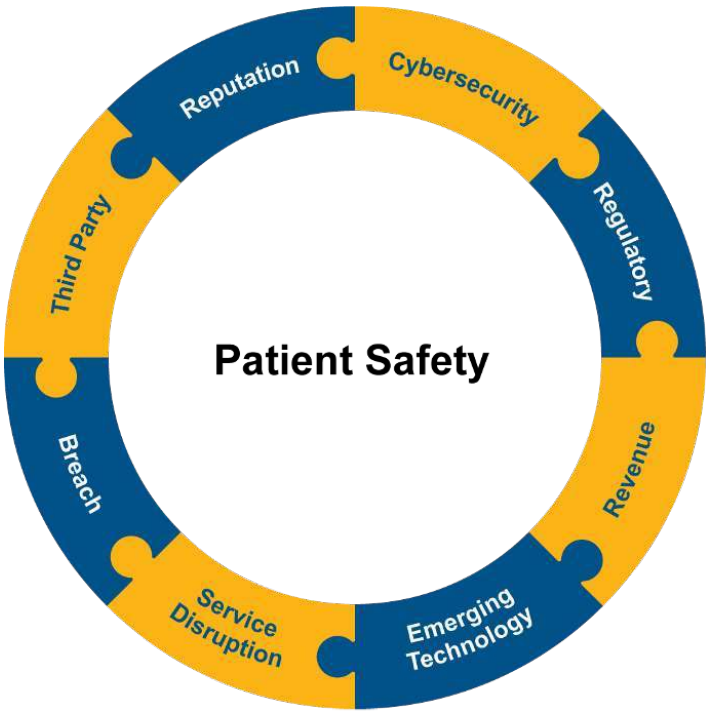
> When looking at the average total cost of a data breach, detection and escalation costs accounted for **29% of the total cost,** which is an average of **$1.24 million.**[5]

Management Imperative

Cybersecurity requires a top-down approach. Management, C-suite, or practice owners must set the tone that cybersecurity is a top priority. Cybersecurity risks are one of many enterprise risks. These risks can affect every aspect of your organization including care delivery, financial, and reputation. Patient safety is the cornerstone of every health organization and is, therefore, the most crucial risk. It is important that health organizations incorporate cybersecurity risks into its overall Enterprise Risk Management (ERM) strategy. This allows entities to manage significant cyber risks alongside other enterprise risks that have potential mission and patient safety impacts. Leadership must play a large part in executing cyber initiatives by sharing the vision to their staff. Initiation of a non-technical cybersecurity training and awareness campaign (one that constantly communicates cyber updates, knowledge, training, and stories), requires collaboration from IT, leadership, operational staff and human resources. Empowering staff to champion the cause can bring immeasurable value to an organization and strengthen its culture.

For additional resources on Enterprise Risk Management visit NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM).

Figure 4. Components of patient safety



The Human Element

When we consider cybersecurity protections and best practices beyond technology, one commonality stands out—the human element. This element is now understood to be a major component to your cybersecurity posture and resilience. A simple mistake on the human side can be the greatest vulnerability to a breach.

To protect your organization, regardless of your role or department, it is imperative that you stay informed and aware of the latest cybersecurity tactics being used. This issue can no longer be delegated to an IT department. It is up to every individual in an organization, from doctors and nurse practitioners to administration professionals and executives, to have a working knowledge of how to protect patients. A great way to begin this endeavor is cyber hygiene.

> "People are the problem and people are the solution."
>
> *—Peter Pritchard, Hero of the Planet*

Be Proactive: Hand Hygiene for Cybersecurity

Doctors and nurses know that hand sanitization is critical to prevent the spread of germs, but that does not mean healthcare workers wash up as often as they should. Similarly, we know that cybersecurity practices reduce the risk of cyber-attacks and data breaches. Just as we can protect our patients from infection, we should all aim to protect patient data and the resiliency of our systems. This will allow physicians and caregivers to trust the data (and systems) that enable quality healthcare.

Healthcare professionals must wash their hands before caring for patients, and healthcare organizations must practice good cyber hygiene in today's digital world, including it as a part of daily universal precautions. Like the simple act of handwashing, a culture of cyber-awareness does not have to be complicated or expensive for organizations of any size. It must simply be effective at enabling organization members to protect information critical to the organization's patients and operations.

Your organization's vigilance against cyber-attacks will increase concurrently with the entire workforce's knowledge of cybersecurity. This knowledge enables advancement to the next series of cybersecurity practices, expanding your organization's awareness of and ability to thwart cyber threats. This will be discussed in the **"How to Use this Publication"** section of this document.

We also recommended proactively partnering with your organization's privacy program. Privacy and cybersecurity are related but are different disciplines. Your privacy professionals can help guide you to understand what appropriate levels of access look like, how data disclosures can occur, and what general acceptable use of data is permitted. Cybersecurity professionals are well positioned to help implement these requirements.

Cyber Incident Reporting

If you are the victim of a serious cyber incident, HHS recommends the following steps:

- Contact your Federal Bureau of Investigation (FBI) Field Office Cyber Task Force immediately to report a cyber incident and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
- Report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) US-CERT Incident Reporting System and FBI's Internet Crime Complaint Center (IC3).
- For further analysis and healthcare-specific indicator sharing, please contact HHS' Health Sector Cybersecurity Coordination Center (HC3) at HC3@hhs.gov.
- Inform your Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs), such as Health-ISAC Inc. (H-ISAC, Health Information Sharing and Analysis Center). H-ISAC is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other.

How to Use this Publication

The Publication: Health Industry Cybersecurity Practices (HICP)

In accordance with the Cybersecurity Act of 2015 (CSA), this publication sets forth a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to achieve three core goals:

1. Cost-effectively reduce cybersecurity risks for the HPH sector;
2. Support the voluntary adoption and implementation of its recommendations; and
3. Ensure that content is actionable, practical, and relevant to healthcare stakeholders of every size and resource level on an ongoing basis.

Audience and Publication Components

Recognizing that cybersecurity recommendations are rarely one-size-fits-all solutions, the publication compiles practices specific to healthcare organizations of varying sizes, ranging from small physician practices to large university hospital systems. It can be leveraged by various audiences to raise awareness for executives, healthcare practitioners, providers, and health delivery organizations, such as hospitals. The publication is applicable to health organizations of all types and sizes across the sector. It also provides technical implementation recommendations for IT and cybersecurity professionals.

The entire publication includes this Main Document, two Technical Volumes, and additional Resources and Templates:

- The **Main Document** (this document) discusses the current cybersecurity threats facing the HPH sector. It sets forth a call to action for the HPH sector, especially executive decision makers, with the goal of raising general awareness.
- **Technical Volume 1** outlines the ten cybersecurity practices (herein called practices) and sub-practices for small healthcare organizations. While it is intended for use by IT and/or cybersecurity professionals, it also serves to guide organizations on what to ask their IT and/or cybersecurity teams or vendors.
- **Technical Volume 2** outlines the ten cybersecurity practices and sub-practices for medium-sized and large healthcare organizations. It is intended for IT and/or cybersecurity professionals.
- The **Resources and Templates** volume provides additional resources and references to supplement the Main Document and Technical Volumes.

Cybersecurity Threats and Mitigation Practices

The goal of the publication is to foster awareness, provide practices, and move towards consistency within the HPH sector in mitigating the current most impactful cybersecurity threats. The five threats explored in this document are as follows:

- Social engineering
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that may affect patient safety

The Technical Volumes detail ten Cybersecurity Practices (CSPs) to mitigate these threats. The ten practices are as follows:

CSP 1. Email Protection Systems
CSP 2. Endpoint Protection Systems
CSP 3. Access Management
CSP 4. Data Protection and Loss Prevention
CSP 5. Asset Management
CSP 6. Network Management
CSP 7. Vulnerability Management
CSP 8. Security Operation Centers and Incident Response
CSP 9. Network Connected Medical Devices
CSP 10. Cybersecurity Oversight and Governance

This document is *not* intended to be used as a list of controls that all organizations must implement. Rather, it is a series of recommended practices to consider as risk mitigation techniques. We recommended beginning with a risk assessment and tailoring your mitigations accordingly.

> The Threat-to-Practice Matrix located at 405d.hhs.gov outlines the relationship between the five threats and ten practices. This can be the start of your risk assessment.

The entire publication considers the recommendations made by HHS divisions including, but not limited to, the Assistant Secretary for Legislation (ASL), the Assistant Secretary for Public Affairs (ASPA), the Administration for Strategic Preparedness and Response (ASPR), the Centers for Medicare and Medicaid Services (CMS), the Food and Drug Administration (FDA), the Office for Civil Rights (OCR), the Office of the Chief Information Officer (OCIO), the Office of the General Counsel (OGC), the Office of the Inspector General (OIG), and the Office of the National Coordinator for Health Information Technology (ONC), as well as guidelines and practices from the Department of Homeland Security (DHS) and National Institute of Standards and Technology (NIST).

Social engineering

Ransomware attacks

Loss or theft of equipment or data

Insider, accidental or malicious data loss

Attacks against network connected medical devices that may affect patient safety

How Does this Publication Help Me?

This publication provides a starting point for implementing basic cybersecurity practices in your healthcare organization. The ten practices are not prioritized in any specific order, providing flexibility for an organization to determine its unique security posture (through a risk assessment or other assessment) and how to prioritize and allocate resources. All three components of the publication serve to inform HPH sector stakeholders on current cybersecurity threats, what makes these effective attack methods for attackers, and what cybersecurity practices organizations can implement to thwart them.

> Across the **686** 2021 healthcare data breaches, **44,993,618 healthcare records** have been exposed or stolen, which makes 2021 the second-worst year in terms of breached healthcare records.[6]

Cybersecurity incidents affect patient care and may represent serious threats to patient safety. Failing to address cyber issues can also negatively impact an organization's bottom line or result in loss of credibility and patient trust. It is this publication's intention to promote the importance of cybersecurity and to provide information in a distilled, useable format.

Where Do I Fit?

The process of implementing cybersecurity practices will vary by organization size, complexity, and type. For example, the development and implementation of an incident response plan will differ significantly between a large, integrated delivery network and a small two-physician practice. To emphasize this variation, the Technical Volumes present cybersecurity practice implementations separately for small, medium-sized, and large organizations. These volumes are intended for your IT staff, cybersecurity staff, or managed service providers (MSPs).

Categorizing your organization's size can be more complicated than it seems. It may seem simple if you are a small practice, however even the smallest healthcare organizations may be tightly coupled with one another, sharing information between common patients, establishing health exchanges, and affiliating with larger health systems. Table 1 provides guidance for deciding which size is your "best fit." To determine the best fit, review the attributes on the left and highlight those that best align to your organization. It's possible your organization might have elements of multiple sizes; that is ok. Your selected size should be based on the one that best represents you.

The two Technical Volumes cover small, medium, and large sized organizations.

Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations presents practices intended specifically for small organizations. If you have an MSP, it is recommended to hand them this publication and Technical Volume 1. If you do not have an MSP, then it is recommended to designate an individual within your organization to evaluate how best to apply this publication. Ask them for an assessment of your existing practices and have them build a plan to mitigate any gaps that have been identified.

Technical Volume 2: Cybersecurity Practices for Medium and Large Organizations presents the practices differently. For each practice, the volume provides a series of sub-practices for medium-sized organizations and sub-practices for large organizations. Medium-sized organizations are advised to start with the sub-practices for medium-sized organizations. Large organizations are advised to review the sub-practices for both medium-sized and large organizations. Medium-sized organizations are encouraged to consider and implement the sub-practices for large organizations as applicable to their needs.

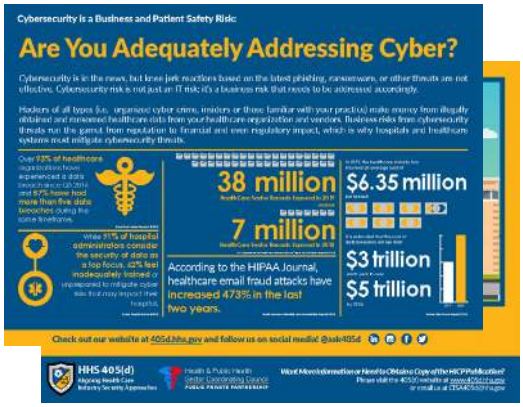
Table 1. Selecting the "Best Fit" For Your Organization

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, or IT is outsourced	Dedicated IT resources are on staff, co-managed with outsourcing, or fully outsourced IT	Dedicated IT resources with dedicated budget
			IT is responsible for security	CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Non-existent or limited funding	Funding allocated for specific initiatives (projects)	Dedicated budget with strategic roadmap specific to cybersecurity
			Potentially limited future funding allocations	
			Cybersecurity budgets are blended with IT	
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)	1-50 beds	51-299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated Delivery Networks (IDNs)
				Participate in Accountable Care Organizations (ACOs) or Clinically Integrated Networks (CINs)
Other org types			Practice management organization	Health plan
			Managed service organization	Large device manufacturer
			Smaller device manufacturers	Large pharmaceutical organization
			Smaller pharmaceutical companies	
			Smaller payor organizations	

Characteristics of your organization and the nature of the products and/or services you provide may decrease or increase the complexity of your cybersecurity needs. You may consider practices outside of your "best fit" size category as you continuously build and improve your cybersecurity strategy.

Use these executive cards (based on organization size) to help you communicate the importance of cybersecurity for your organization and patients:

- Executive Card for Small Organizations
- Executive Card for Medium/Large Organizations



Executive Cards

HICP & Cybersecurity Strategy Approaches

Cybersecurity is no longer a one-step solution. Rather, it is crucial that all healthcare organizations have a cybersecurity strategy. While incremental improvements are better than no action; cybersecurity can no longer be reactive. Healthcare organizations need to be forward leaning, strategic, and prepared for the future. A cybersecurity strategy should be living, breathing, and adaptable to the current threat landscape and organization structure.

Setting a cybersecurity strategy is a fundamental step in helping your organization proactively secure its environment and protect patients. While a cybersecurity strategy should be unique to an organization, there are two general approaches that organizations should consider: *zero trust* and *defense-in-depth*. HICP and the mitigation practices covered in the technical volumes assist organizations in implementing the concepts and controls that both these strategies focus on.

The Zero Trust Strategy

The HPH sector is increasingly targeted by ransomware attacks due to its valuable PHI. To safeguard this critical infrastructure, a security posture focused on identity management, access control, and data security should become part of daily operations. One proposed solution is the *zero trust* security strategy. The strategy provides guidance for organizations to protect their resources by creating processes and workflows focused on protecting assets and securing sensitive data. Building a zero trust architecture that encompasses multi-layer protections strengthens your security posture. This means all device and user identities, both internal and external, are validated prior to being granted access to network resources. This approach can be used to mitigate vulnerabilities created by network trends, including bring your own device (BYOD), cloud-based services and users working remotely. Your organization can enable the zero trust strategy at all network levels to ensure a strong security posture. This includes firewalls, physical security, and all IT systems and their users. Employees should also be trained on email security and how to recognize phishing attempts.

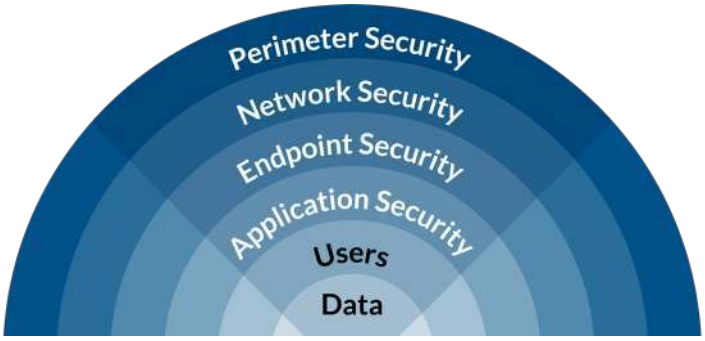
One way to begin implementing zero trust into your healthcare organization includes applying an access and identity management solution. (This practice can be found in Cybersecurity Practice #3: Access Management located in Technical Volumes 1 and 2.) Applying a least privilege access process creates additional security controls by only allowing users access to applications they need to do their work. For example, a front desk receptionist should not be able to view/edit the same level of PHI a physician can. This process can be automated to grant file and data access applicable to each job function. It also ensures that when an employee changes jobs or leaves the organization, their access is revoked. This prevents any additional vulnerabilities that might arise when access control is not continuously monitored. This is just one way of implementing zero trust in your organization; one that the practices covered in HICP can help your organization achieve.

Defense-in-Depth

Today's cyber threats are continuously evolving and expanding in sophistication. While the goal is to stop cyber threats before they happen, the reality is that organizations can't prevent attacks 100 percent of the time. A holistic cybersecurity approach, such as *defense-in-depth*, could slow attacks and minimize the damage taking place. Defense-in-depth is a strategy that layers multiple security safeguards, rather than relying on a single layer. This means if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach. It is a best practice strategy that can be implemented in different ways (for different entity sizes) due to its ability to be implemented across the entire infrastructure. HICP Technical Volumes 1 and 2 outline industry-proven practices that organizations of different sizes and capabilities can use to develop their defense-in-depth strategy. The approach should include a wide range of security elements, such as:

- **Identity and access security controls,** such as multi-factor authentication (MFA) or condition-based access, to control access to infrastructure and enable proper change control management. (See Cybersecurity Practice #3: Access Management located in Technical Volumes 1 and 2.)
- **Perimeter security** including distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial-of-service for users. (See Cybersecurity Practice #9: Network Connected Medical Devices located in Technical Volumes 1 and 2.)
- **Network security,** such as network segmentation and network access controls, limit communication between resources. (See Cybersecurity Practice #6: Network Management located in Technical Volumes 1 and 2.)
- **Patch Management** removes vulnerabilities that can be exploited by attackers. (See Cybersecurity Practice #7: Vulnerability Management located in Technical Volumes 1 and 2.)

Figure 5. Defense-in-depth model



- **Intrusion Prevention,** implemented with intrusion prevention systems (IPS) and configured to update automatically, reduces your organization's vulnerability to known types of cyber-attacks. (See Cybersecurity Practice #7: Vulnerability Management located in Technical Volumes 1 and 2.)
- **Endpoint Solutions,** such as endpoint detection and antivirus software, to control access to privileged endpoint accounts. (See Cybersecurity Practice #2: Endpoint Protection Systems located in Technical Volumes 1 and 2.)

Defense-in-depth may appear to slow down productivity due to its increased security controls and may seem redundant at first glance. However, a defense-in-depth strategy prevents threats (i.e., ransomware and zero-day attacks, which take place when hackers exploit a flaw before developers have a chance to address it—meaning they have "zero days" to fix it) by utilizing a combination of detection tools and preventative controls. These will stop attackers from reaching your organization's internal network, which houses valuable health information. Having defense-in-depth will help organizations ensure they have a comprehensive cybersecurity strategy.

Current Threat Scenarios Facing the HPH Sector

In this section, we introduce cybersecurity threats and some of the associated vulnerabilities that currently affect the HPH sector. A vulnerability requires a threat to be actioned before it can have any impact. A vulnerability on its own will not induce cyber risks. Why is it important to understand the difference between a threat and a vulnerability? The ability to distinguish between the two helps determine which cybersecurity practices and tools are necessary and appropriate for your organization. The correct practices and tools will mitigate the harm that may come from an attacker or from a mistaken or uninformed, but authorized, individual.

> **Threats** are anyone or anything, internal or external, natural or manmade, malicious or accidental, with the potential to negatively impact the quality, efficiency, and profitability of your organization.
>
> **Vulnerabilities** are weaknesses that, if exposed to a threat, may result in harm and, ultimately, some form of loss.
>
> **A threat exploits a vulnerability.**

Explaining Threats and Vulnerabilities

Threats and vulnerabilities go hand in hand, but they are *not* interchangeable. Threats are activities or events that have the potential to negatively impact the quality, efficiency, and profitability of your organization. Threats may be internal or external, natural or manmade, malicious or accidental. Think of hurricanes and floods causing power outages. These are examples of external natural threats. A threat may also be a person, including an existing employee, who decides to steal data or do harm to your practice.

A threat is anything, or anyone, with the potential to harm something of value. An example most healthcare practitioners are familiar with is the influenza virus. The flu can infect nearly anyone exposed to the virus. The extent of harm caused by the virus depends on that person's vulnerability. Comparing an elderly person with a college athlete, most would say that the elderly person is more vulnerable to harm caused by the flu. What is it that makes the elderly person more vulnerable?

Vulnerabilities are weaknesses that, if exposed to a threat, may result in harm and, ultimately, some form of loss. *A threat exploits a vulnerability.* Using the flu example, most people would assume that an elderly person is more vulnerable to harm than a college athlete. This increased vulnerability is due to the diminished function of an aged immune system, reduced physical strength, and even compromised mental capabilities that could result in an inability to adhere to a prescribed treatment plan. In addition to these factors, the failure to get a flu shot may increase an elderly person's vulnerability to harm even further.

A Translation: Threats, Vulnerabilities, Impact, and Practices

The discussion above on threats and vulnerabilities applies similarly to cybersecurity. Threats to your organization may include phishing attacks, malware (e.g., ransomware), insider threats, lost equipment, attackers, and many others. These threats exist at some level for all healthcare organizations. As in our flu scenario with the college athlete and the elderly person, the impact of these threats to your organization depends on the ability of the threat to exploit existing vulnerabilities.

Threat: Influenza		
Vulnerabilities	**Impact**	**Practices**
Weak immune system; no flu shot; lack of hand washing	Patient is stricken with a case of the flu	Receive a flu shot; wash hands or use hand sanitizer frequently

Introducing Current Threats to the HPH Sector

This section describes five of the most current and common cybersecurity threats to the HPH sector. As depicted below, the five current cybersecurity threats are:

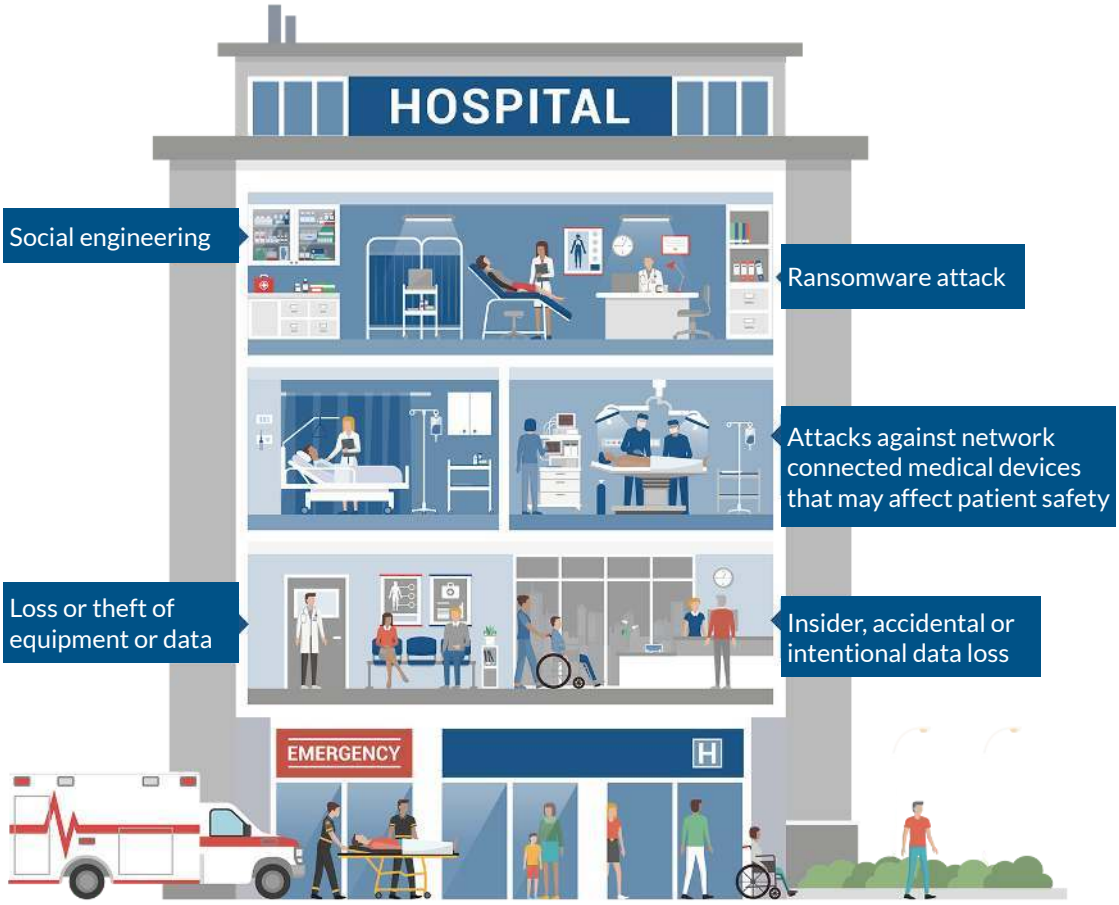
1. Social engineering attack
2. Ransomware attack
3. Loss or theft of equipment or data
4. Insider, accidental or intentional data loss
5. Attacks against network connected medical devices that may affect patient safety

Figure 6 portrays how these five threats can affect organizations in various parts of a hospital and in different healthcare settings. Cyber-attacks can happen anywhere, any time. The following sections discuss these threats in detail, with additional quick tips for *What to Ask*, *When to Ask*, *and Who to Ask*.

Vulnerabilities that may determine the impact of each threat are also listed in a table at the end of each threat section. The tables also include "Practices to Consider" for each threat to help determine effective ways to address your vulnerabilities and limit the damage.

Cybersecurity sub-practices from the Technical Volumes are mapped to each of the "Practices to Consider." Tables 7, 8, and 9 serve as key references for this mapping (e.g., 1.S.B.) Sub-practices labeled with "S" (small) can be found in Technical Volume 1, and those labeled with "M" (medium) or "L" (large) can be found in Technical Volume 2.

Figure 6. Top 5 threats facing the HPH sector



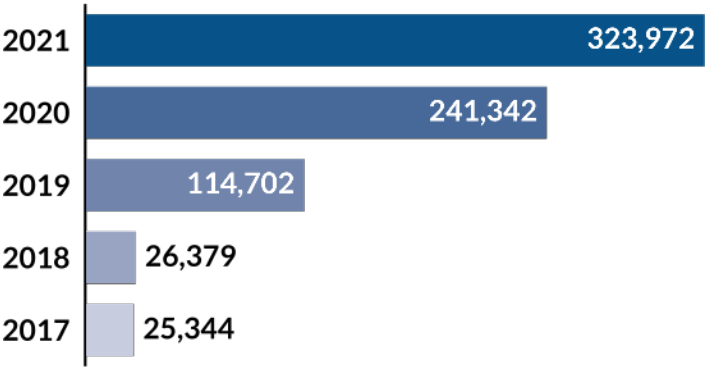
The threats portrayed in this graphic are meant to show that these threats can affect organizations in various parts of a hospital and in different healthcare settings. Cyber-attacks can happen anywhere, any time.

Threat: Social Engineering

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks or taking an action (e.g., clicking a link, opening a document).

Social engineering attacks begin as tricks to fool people into providing sensitive details, such as passwords, banking numbers, Social Security numbers, or other sensitive data by claiming to be someone they are not. Attackers might send a spoofed email pretending to be your supervisor or send a message that appears to be from your IT department. One common type of social engineering attack is called "phishing," which is typically delivered through email. Email phishing is an attempt to trick you, a colleague, or someone else in the workplace into providing information using email. An inbound phishing email includes an active link or file (often a picture or graphic). The email appears to come from a legitimate source, such as a friend, coworker, manager, company, or even the user's own email address. Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on your computer (or other computers within your network). Social engineering attacks also appear as fraudulent text messages or phone calls claiming to be an important facility. In the past several years, these attacks have become much more sophisticated and personal.

Figure 7. Number of phishing/vishing/smishing/pharming victims reported to the FBI Internet Crime Complaint (IC3), 2017-2021[7]



Other social engineering techniques include an attacker leveraging trending events (e.g., the COVID-19 pandemic) or a high-profile social or political event (e.g., a local election). Another trick attackers use is sending emails, calls, or flyers to claim free tickets or other giveaways items, such as free healthcare IT services. The attacker may send several emails to establish a level of trust, convincing the victim to reveal personal data, such as their personal email or place of employment. The attacker may even impersonate the user, call an IT help desk, and attempt to reset their password.

The attacker can then use information to reset passwords by using easily discoverable personal information available through various data sources. For instance, the question "What high school did you attend?" can often be found in public data records, social media posts, or a blog.

Over the last five years, there has been a substantial rise in Business Email Compromise (BEC) reported to the FBI.[7] In these attacks, the relationship with an organization is exploited for financial gain (e.g., creation of a fake invoice). The attacker will attempt to impersonate a high-level figure and ask them to conduct wire transfers, or even purchase gift cards to send back to them through email. Payment is often through wire transfer and may not be recoverable. In 2020, individual businesses lost between $1,240 to $44,000 in these BEC attacks.[8]

Some BEC attacks are launched within an organization when one person is tricked into providing the login to their email account. The attacker can then use this person's email account to send out more emails to all their contacts. Attackers are even known to use email conversations you were already having with a contact to send a new email with infected links or attachments.

Real-World Scenario:
Your employees receive a fraudulent email from a cyber-attacker disguised as an IT support person from your patient billing company. The email instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data.

Impact:
The cyber-attacker now has full access to your organization's system and can install malware, which can affect all your organization's IT systems and delay patient care.

Table 2 identifies vulnerabilities, impacts, and practices to consider for email phishing attacks.

405(d) Resources:

- Email Phishing Flyer
- Email Phishing Threat Series Slides
- Email Phishing Poster

Quick Tips to Prevent Social Engineering	
What should I ask?	On average, a person will receive about 80 emails per day. Knowing which are safe to open can get tricky if you are not asking yourself the following questions: • Do you know the sender? If so, were you expecting the email? • Are there any spelling or grammatical errors, or any other indicators that the tone or style of the email is off? • Does the email have a sense of urgency or deadline to take an action? • Before clicking on a link, did you hover over it to see the URL destination? • If the link is to access the site of an account you have, did you go directly to the site instead of using the link to see if the information can be found directly on their site? • Do you know the sender, or are you suspicious of the email? If in doubt, do NOT open any attachments. • What are my organization's processes for reporting suspicious emails?
When should I ask?	The best time to familiarize yourself with your organization's policies for reporting a suspicious email is when you begin employment. Whenever you receive an email that sounds too good to be true or that you were not expecting, verify it before opening it!
Who should I ask?	Check with colleagues to find out whether they received the same suspicious email. You can always seek the guidance of your IT security support team or similar point of contact. Talk to them to find out whether your account is protected with the proper security filters to ward off unwanted junk mail.

Table 2. Threat Profile: Social Engineering

Threat: Email Phishing Attack, an Example of Social Engineering		
Vulnerabilities	**Impact**	**Practices to Consider**
• Lack of awareness training • Lack of email detection software testing for malicious content • Lack of software scanning emails for malicious content or bad links • Lack of email sender and domain validation tools • Lack of IT resource for managing suspicious emails	• Stolen access credentials used for access to sensitive data • Potential negative impact to the ability to provide timely and quality patient care • Patient safety concerns • Erosion of trust or brand reputation • Loss of reputation in the community (referrals dry up, patients leave the practice)	• Implement MFA (1.S.A, 3.M.D) • Tag external emails to make them recognizable to staff (1.S.A) • Implement advanced technologies for detecting and testing email for malicious content or links (1.L.A) • Be suspicious of emails from unknown senders, emails that request sensitive information such as PHI or personal information, or emails that include a call to action that stresses urgency or importance (1.S.B) • Train staff to recognize suspicious emails and to know where to forward them (1.S.B) • Never open email attachments from unknown senders (1.S.B) • Implement proven and tested response procedures when employees click on phishing emails (1.S.C) • Implement incident response plays to manage successful phishing attacks (8.M.A) • Establish cyber threat information sharing with other healthcare organizations and/or ISACs and ISAOs (8.S.B, 8.M.C)

Cybersecurity sub-practices from the Technical Volumes are mapped to each of the "Practices to Consider." Tables 7, 8, and 9 serve as key references for this mapping (e.g., 1.S.B.) Sub-practices labeled with "S" (small) can be found in Technical Volume 1, and those labeled with "M" (medium) or "L" (large) can be found in Technical Volume 2.

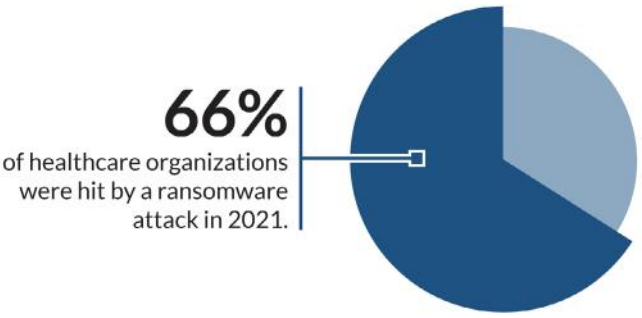
Threat: Ransomware Attack

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 attacker 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 attacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key."

Over time, ransomware attacks have evolved to include targeted attacks. These attacks are adapted for specific groups or organizations to make them more effective. Once attackers access your network, they use ransomware to restrict access to your devices and data until a ransom is paid. Generally, these attacks are "human-operated," meaning there is an actor directing the deployment of ransomware once they have made an initial compromise of the network. It's common for attackers to first leverage social engineering to get access to credentials, then use those credentials to access the network and deploy ransomware. HHS issued supplemental materials to the original Factsheet with additional details about the evolution of ransomware.

Ransomware threats may incorporate tactics or techniques that begin as one type of threat and provide opportunities for other threats to render your systems defenseless. For example, successful phishing attacks may lead to the installation of ransomware. Ransomware often begins by running in the background to avoid detection. This way, attackers can monitor their victim and design the attack plan. One step could be to interfere with the routine backup schedule, rendering all backups unusable. When the hackers are ready to launch their attack, the victim is surprised, unprepared, and defenseless. Using these tactics, some ransomware attackers have even stolen data *prior* to encrypting the data on the systems. If the victim refuses to pay, they threaten to release the information publicly or sell it to other third parties. **Paying a ransom does not guarantee that the attacker will unencrypt or unlock the stolen or locked data, even if the attacker guarantees that it will work.** It is also common for attackers to tailor the size of the ransom based on the ability of an organization to pay. In some cases, they will review any cyber insurance policies in place and set the ransom to be the limit covered under insurance. Defense against ransomware requires a multi-faceted strategic approach.

Figure 8. Organizations affected by ransomware in 2021.[9]



Real-World Scenario:

A small town's family medical practice went from treating its patients, to being locked out of patient records, appointment schedules, and payment information after attackers encrypted the data. The attackers demanded $7,000 for the key to decrypt the files, or they would delete all the data. The practice owners made the tough decision to not pay the ransom, as the key was not guaranteed, and thus the attackers could just demand more money.

Impact:

These attacks have serious monetary repercussions that can lead to permanent closures, especially for small healthcare organizations. In instances where no backups are in place, attackers delete the files, and owners are forced to close their practice. These threats are on the rise and becoming more advanced. In healthcare, our business is caring for people. In many cases this care must be timely for the health and safety of the patient. Ransomware operators know this, which is one reason why healthcare is often targeted and considered a data-rich industry. Because of this, we should expect attacks to steadily spike in the years to come.

405(d) Resources:

- Ransomware Flyer
- Ransomware Threat Series Slides
- Ransomware Poster
- Ransomware One-Pager: Prepare, React, Recover
- Have You Heard - Ransomware

Table 3 identifies vulnerabilities, impacts, and practices to consider for ransomware attacks.

Quick Tips to Prevent Ransomware Attacks	
What should I ask?	It is common for attackers to first break into an organization using a phishing attack, getting access to sensitive credentials, then deploy the ransomware itself. Be sure you know how to identify these phishing emails! Stay alert when any email asks you to enter your credentials. Defenses against ransomware are multifaceted. That means asking: • Do I have a high-performance firewall? • Do I have my firewall configured to only allow certain ports to be open? • Is there training I should be aware of to understand my organization's security policies? • Do I have validated isolated backups of key systems and data? • Is remote access to Remote Desktop Protocol (RDP) secured with MFA? • Do we have an incident response plan in the event we are impacted? • When was the last time we conducted a tabletop exercise to confirm our readiness? • Do we know how to contact the Local FBI Cyber Branch Office?
When should I ask?	Employers should implement user awareness and compliance training during the onboarding process or when issuing a new laptop or desktop equipment. As an employee, if you discover that your computer has been infected, immediately notify your IT security team. Do not power off or shut down the computer or server, in case a volatile random-access memory (RAM) image needs to be collected for forensics and incident response investigations.
Who should I ask?	Due to the severity and time sensitivity of ransomware attacks, it is in your best interest (and that of your organization) to always seek out professional IT security or a similar point of contact help when you think your computer is infected with ransomware. As these attackers become more aggressive with their tactics and demands, it is essential that you have all the information possible to make necessary business decisions effectively during an attack.

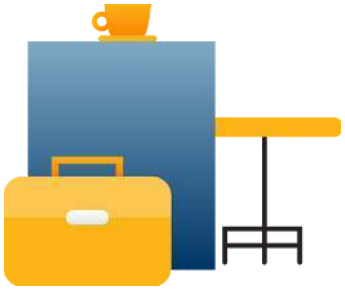
Table 3. Threat Profile: Ransomware Attack

Threat: Ransomware Attack		
Vulnerabilities	**Impact**	**Practices to Consider**
• Lack of anti-phishing capabilities • Lack of anti-malware detection and remediation tools • Lack of network security controls like segmentation and access control • Unpatched software • Lack of isolated system backup • Lack of testing and proven data back-up and restoration	• Potential data breach of PHI or Personally Identifiable Information (PII) • Partial or complete clinical and service disruption which can cause a delay in care • Loss of revenue of key services while under disruption • Patient care and safety concerns • Expenses for recovery	• Use strong/unique username and passwords with MFA (1.S.A, 3.S.A, 3.M.C) • Deploy anti-malware detection and remediation tools (2.S.A, 2.M.A, 3.L.D) • Limit users who can log in from remote desktops (3.S.A, 3.M.B) • Limit the rate of allowed authentication attempts to thwart brute-force attacks (3.M.C) • Be clear about which computers may access and store sensitive or patient data (4.M.C) • Implement a proven and tested data backup and restoration test (4.M.D) • Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up (4.M.D) • Maintain a complete and updated inventory of assets (5.S.A, 5.M.A) • Implement network segmentation and establish network zones to limit access from threats (6.S.A, 6.M.B, 6.L.A) • Ensure that users understand authorized patching procedures (7.S.A) • Patch software according to authorized procedures (7.S.A) • Implement proven and tested incident response procedures (8.S.A, 8.M.B) • Establish cyber threat information sharing with other healthcare organizations (8.S.B, 8.M.C) • Develop a ransomware recovery playbook and test it regularly (8.M.B) • Secure a cyber insurance policy that provides ransomware protections (10.S.D) • Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures (HHS Ransomware Factsheet)

Cybersecurity sub-practices from the Technical Volumes are mapped to each of the "Practices to Consider." Tables 7, 8, and 9 serve as key references for this mapping (e.g., 1.S.B.) Sub-practices labeled with "S" (small) can be found in Technical Volume 1, and those labeled with "M" (medium) or "L" (large) can be found in Technical Volume 2.

For additional information on activities to prepare for and respond to a ransomware attack, please see NIST Special Publication 800-184 – Guide to Cybersecurity Event Recovery at https://csrc.nist.gov/publications/detail/sp/800-184/final

Threat: Loss or Theft of Equipment or Data



Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen, and they end up in the hands of attackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations.

In 2021, 713 major health data breaches (affecting more than 45.7 million individuals) were reported to the HHS OCR.[10] Although the value of the device represents one loss, the consequences of losing a device that contains sensitive data are far greater. In cases where the lost device was not appropriately safeguarded with practices such as MFA or other encryptions, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

Even if the device is recovered, the data may have been erased and completely lost. Loss or malicious use of data may result in business disruption and compromised patient safety, and may require notification to patients, applicable regulatory agencies, and/or the media.

Figure 9. Impact of data breaches in December 2021[11]

Across December 2021's **56 data breaches, 2,951,901 records were exposed or impermissibly disclosed**—a **24.52% increase** from the previous month. At the time of posting, the OCR breach portal shows **45,706,882 healthcare records** were breached in 2021.

Real-World Scenario:
A physician stops at a coffee shop to review radiology reports. As he leaves his table momentarily to pick up his order, a thief steals the laptop. The doctor returns to the table to find the laptop is gone.

Impact:
Loss of sensitive data may lead to a clear case of patient identity theft. With thousands of records potentially stolen, the physician's and practice's reputations could be at stake if all the patient records make it to the dark web for sale.

Table 4 outlines vulnerabilities, impacts, and practices to consider for loss or theft of equipment or data.

405(d) Resources:

- Loss or Theft of Equipment or Data Flyer
- Loss or Theft of Equipment or Data Threat Series Slides
- Loss or Theft of Equipment or Data Poster

Loss or Theft of Equipment or Data Flyer

Quick Tips to Prevent Loss or Theft of Equipment or Data	
What should I ask?	If headed on business trip or a personal holiday, you must follow the same (and maybe greater) security procedures as you do in the office. Make sure you know your organization's policy on removing equipment from the workplace by asking: • Is my device encrypted? • Can I travel with my equipment? • Have we made sure there are no written copies of login information or encryption keys being carried with the equipment? • Can I take my equipment offsite to work remotely? • Is there a cable lock or similar mechanism for securing equipment? • Are USB or other portable storage devices allowed and are they encrypted? • Is there a secure virtual private network (VPN) that I can use, along with secure, password-protected Wi-Fi, to log into the network and work?
When should I ask?	When you are provided your equipment, ask if it is encrypted. If you realize that your device or equipment has been stolen or misplaced, notify your supervisor and IT security professional immediately so appropriate measures can be taken to safeguard the data saved on your device or equipment.
Who should I ask?	Your IT security support staff or similar point of contact should be notified when a work device or equipment has been misplaced, lost, or stolen. The data saved on the device/equipment are now compromised and susceptible to unauthorized access, dissemination, and use. This is a serious cyber breach and should be handled by trained IT security professionals.

Table 4. Threat Profile: Loss or Theft of Equipment or Data

Threat: Loss or Theft of Equipment or Data		
Vulnerabilities	**Impact**	**Practices to Consider**
• Lack of awareness that theft of IT assets is nearly as common as car theft • Lack of physical security practices; open offices and poor physical access management • Lack of simple safeguards such as computer cable locks to secure devices within office environments • Lack of asset inventory and control • Lack of encryption; data at rest is data stored on a hard drive at any location • Lack of effective vendor security management including controls to protect equipment or sensitive data • Lack of "End of Service" process to clear sensitive data before IT assets (including network connected medical devices) are discarded or transferred to other users or other organizations • Lack of authentication to prove user identity	• Inappropriate access to or loss of sensitive patient information; may involve proprietary or confidential company information or intellectual property (IP) • Theft or loss of unencrypted PHI or PII; may result in a data breach requiring notification to affected patients, relevant regulatory bodies, and the media • Lost productivity • Damage to reputation	• Promptly report loss/theft to designated company individuals to terminate access to the device and/or network (3.S.A) • Encrypt sensitive data, especially when transmitting data to other devices or organizations (4.S.B, 4.M.C) • Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device (4.M.C) • Implement proven and tested data backups, with proven and tested restoration of data (4.M.D) • Acquire and use data loss prevention tools (4.M.E, 4.L.A) • Maintain a complete, accurate, and current asset inventory to mitigate threats, especially the loss and theft of mobile devices such as laptops and USB/ thumb drives (5.S.A) • Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold (5.S.C, 5.M.D) • Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices (9.M.A)

Cybersecurity sub-practices from the Technical Volumes are mapped to each of the "Practices to Consider." Tables 7, 8, and 9 serve as key references for this mapping (e.g., 1.S.B.) Sub-practices labeled with "S" (small) can be found in Technical Volume 1, and those labeled with "M" (medium) or "L" (large) can be found in Technical Volume 2.

For additional information on activities to prepare and respond to a data loss scenario, please see NIST Special Publication 800-184 – Guide to Cybersecurity Event Recovery at https://csrc.nist.gov/publications/detail/sp/800-184/final

Threat: Insider, Accidental or Malicious 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 malicious.

An accidental insider threat is not malicious and can be caused by honest mistakes, such as being tricked, procedural errors, or a degree of negligence. For example, an employee accidentally emailing large volumes of PHI to an incorrect recipient would be an accidental insider threat.

A malicious 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, extortion, or inflicting harm to the organization or another individual.

Real-World Scenario:
An employee with access to patient records begins to print extra copies of patient records that include a significant amount of sensitive information such as PHI. They then take the copies and sell them on the dark web.

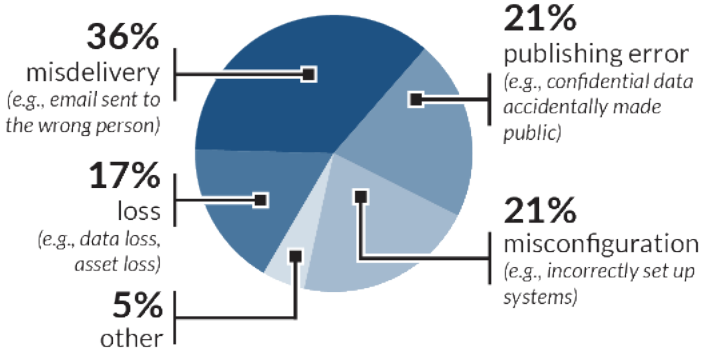
Impact:
Insider threats involve people who typically have legitimate access to your computer systems and network. Whether through negligence or malice, insiders can compromise your patient and enterprise data over short or extended periods of time. This has serious repercussions for the patients, their security, and overall quality of care delivery.

Table 5 identifies vulnerabilities, impacts, and practices to consider for accidental or malicious data loss.

405(d) Resources:

- Insider, Accidental or Intentional Data Loss Flyer
- Insider, Accidental or Intentional Data Loss Threat Series Slides
- Insider, Accidental or Intentional Data Loss Poster

Figure 10. Error varieties in healthcare breaches[12]



Quick Tips to Prevent Insider, Accidental or Malicious Data Loss	
What should I ask?	Do you see something? Say something! Follow your instinct, and always report what does not look or feel right to you. Beware of social engineering techniques. Check to see whether your organization conducts enhanced employee and vendor screening to make sure that those gaining access to company data are who they say they are and that they truly require access to the information. Are you limiting access to information to those who require it based on roles and responsibilities?
When should I ask?	Conduct regular security training sessions to further employees' education and awareness. Train and test your staff to make sure they understand the security risks and the consequences of falling victim to insider attacks. By doing so, you can lower the probability of such attacks happening in your organization. If staff members are under an abnormal amount of stress (for either internal or external reasons), they are more likely to make mistakes or get caught up in insider issues. Ask them how you can help with the workload or monitor the work they are doing more closely.

Quick Tips to Prevent Insider, Accidental or Malicious Data Loss	
Who should I ask?	Always consult HR when exposed to a situation of stolen data or employee misconduct. Human resource departments should establish a relationship with the IT security professionals so they can run appropriate legal and forensic activities. A cyber incident is not limited to hacking. Every situation will vary, so your IT security professionals will be able to best guide you.

Table 5. Threat Profile: Insider, Accidental or Malicious Data Loss

Threat: Insider, Accidental or Malicious Data Loss		
Vulnerabilities	**Impact**	**Practices to Consider**
• Lack of training on social engineering and phishing attacks • Lack of physical access controls • Lack of adequate monitoring, tracking, and auditing of access to patient information on EHR systems • Lack of adequate logging and auditing of access to critical technology assets, such as email and file storage • Lack of adequate logging and audit of third-party/business associate support • Excessive access provided to employees or third-party affiliates • Lack of technical controls to monitor the emailing and uploading of sensitive data outside the organization's network • Files containing sensitive data accidentally emailed to incorrect or unauthorized addressees • Server or other storage device not encrypted or configured securely	• Inability to perform vital patient services, financial loss, access to critical data and systems, etc. • Patients given the wrong medicines or treatment due to incorrect data in the EHR • Accidental loss of PHI or PII via email and unencrypted mobile storage, resulting in reportable data breaches • Reportable incidents involving patients who are victims of employees who inappropriately view patient information • Financial loss from insiders being socially engineered into not following proper procedures • Financial loss due to an employee inadvertently giving an attacker access to banking and routing numbers in response to a phishing email disguised as originating from the bank	• Update Business Associate Agreements (BAA) to include legal safeguards, BAA security review and implement enhanced security processes, BAA contingency plans (Technical Volume 1 Introduction) • Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors (1.S.B, 1.M.D) • Promptly terminate access when an employee or affiliate no longer requires it (3.S.A, 3.M.A, 3.M.B) • Limit access to "need to know" (3.S.A, 3.M.C, 3.L.B, 3.L.C) • Implement and use workforce access auditing of health record systems and sensitive data (3.M.B) • Implement and use privileged access management tools to report access to critical technology infrastructure and systems (3.M.C) • Implement and use data loss prevention tools to detect and block leakage of PHI and PII via email and web uploads (4.M.E, 4.L.A)

Cybersecurity sub-practices from the Technical Volumes are mapped to each of the "Practices to Consider." Tables 7, 8, and 9 serve as key references for this mapping (e.g., 1.S.B.) Sub-practices labeled with "S" (small) can be found in Technical Volume 1, and those labeled with "M" (medium) or "L" (large) can be found in Technical Volume 2.

Threat: Attacks Against Network Connected Medical Devices

Network connected medical devices are network-based devices that leverage networking protocols to communicate and transmit clinical information, such as Bluetooth, TCP/IP and other networks-based technology. According to the Food and Drug Administration (FDA), "medical devices range from simple tongue depressors and bedpans to complex programmable pacemakers and closed loop artificial pancreas systems. Additionally, medical devices include in vitro diagnostic (IVD) products, such as reagents, test kits, and blood glucose meters. Certain radiation-emitting electronic products that have a medical use or make medical claims are also considered medical devices. Examples of these include diagnostic ultrasound products, x-ray machines and medical lasers."

Real-World Scenario:

A cyber-attacker gains access to a care provider's computer network and takes command of a file server. While scanning the network for devices, the attacker takes control (e.g., powers off, continuously reboots) of all heart monitors in the intensive care unit (ICU), putting multiple patients at risk. They could even implement a new malware proof of concept that can change image data to the point where doctors, even when alerted that the image indicates a change, could not detect it.

Impact:

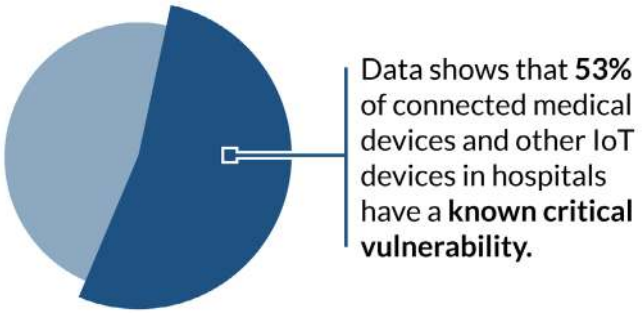
Patients are at great risk because an attack has shut down heart monitors, including ones being used in surgery and other procedures. Doctors are now distracted, quality of patient care has suffered, and patients' health is at risk.

Table 6 outlines vulnerabilities, impacts, and practices to consider for attacks against network connected medical devices.

405(d) Resources:

- Attacks Against Network Connected Medical Devices Flyer
- Attacks Against Network Connected Medical Devices Threat Series Slides
- Attacks Against Network Connected Medical Devices Poster

Figure 11. Internet of Things (IoT) vulnerabilities.[13]



Quick Tips to Prevent Attacks Against Network Connected Medical Devices

What should I ask?

Know your organization's protocols in case of a potential shutdown or attack against network connected medical devices. Help patients and staff by understanding the processes and procedures; this can help mitigate the impacts. Be sure to ask:

- How do we notify patients if their network connected medical devices are compromised?
- How do patients notify us if they suspect their network connected medical devices are compromised?
- Are network connected medical devices kept up to date and protected against compromise?

Quick Tips to Prevent Attacks Against Network Connected Medical Devices	
What should I ask?	• Is the IT staff aware of new devices connecting to the network to ensure the proper security is in place? • Ask the vendor for any configuration options that will make the device more secure than the default settings provide. • Are security reviews being conducted while the devices are being purchased?
When should I ask?	Knowledge of your organization's protocols for potential attacks on network connected medical devices should be shared during new hire orientation or at security training. These protocols need to be communicated to patients when they are given network connected medical devices.
Who should I ask?	Each organization should have IT security professionals to help answer any questions on the policy and governance associated with network connected medical devices. If your organization does not, ask your supervisor for information and/or resources allowing you to learn more about the threat. Vendors or manufacturers of network connected medical devices may need to be engaged to understand vulnerabilities, risks, and appropriate protection and response measures.

Table 6. Threat Profile: Attacks Against Network Connected Medical Devices That May Affect Patient Safety

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety		
Vulnerabilities	**Impact**	**Practices to Consider**
• Default passwords are not changed on network connected medical devices • Equipment not current, or legacy equipment that is outdated and lacks current functionality • Patches not implemented promptly; includes regular and routine commercial system patches to maintain network connected medical devices • Heterogeneity of network connected medical devices means that the vulnerability identification and remediation process is complex and resource intensive; increases the likelihood that devices will not be assessed or patched, leading to missed opportunities to close vulnerabilities	• Medical devices will lose connection and may not function as intended for patient diagnosis treatment. • Patient safety compromised due to breach • Broad hospital operational impact due to unavailable network connected medical devices and systems connected	• Implement cybersecurity assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities (1.L.A) • Establish and maintain communication with network connected medical device manufacturer's product security teams (9.L.A) • Patch devices after patches have been validated, distributed by the network connected medical device manufacturer, and properly tested (9.M.B) • Assess current security controls on network connected medical devices (9.M.B, 9.M.E) • Implement security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities (9.L.B)

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety		
Vulnerabilities	**Impact**	**Practices to Consider**
• Devices are not segmented off the regular general access network onto their own secure network • Most network connected medical devices, unlike IT equipment, cannot be monitored by an organization's intrusion detection system (IDS); safety of patients and protection of data integrity are dependent on identifying and understanding the threats and threat scenarios. However, it is the challenge of identifying and addressing vulnerabilities in network connected medical devices that augment the risk of threats compared with managed IT products • For network connected medical devices, the cybersecurity profile information is not readily available at healthcare organizations, making cybersecurity optimization more challenging; this may translate into missed opportunities to identify and address vulnerabilities, increasing the likelihood for threats to result in adverse effects		• Implement access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, MFA, and minimum necessary or least privilege (9.M.C) • Implement pre-procurement security requirements for vendors (9.L.B) • Engage cybersecurity as a stakeholder in clinical procurements (9.L.B) • Use a template for contract language with network connected medical device manufacturers and others (9.L.B) • 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 cybersecurity risks (9.M.D) • Develop and implement network security applications and practices for device networks (9.M.E)

Cybersecurity sub-practices from the Technical Volumes are mapped to each of the "Practices to Consider." Tables 7, 8, and 9 serve as key references for this mapping (e.g., 1.S.B.) Sub-practices labeled with "S" (small) can be found in Technical Volume 1, and those labeled with "M" (medium) or "L" (large) can be found in Technical Volume 2.

Looking Ahead

The HHS mission is to enhance the health and well-being of all Americans by providing effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. In support of this mission, we are positioned at the forefront of identifying, testing, and piloting new technologies and methodologies with a 360-degree view of the intersection between cybersecurity and healthcare. We constantly share practices with federal and private-sector stakeholders and partners, and we are committed to improving the security and resiliency of the healthcare community.

HHS and its healthcare industry partners provide valuable information on critical threats related to the HPH sector. Many publications have been created by the Health Sector Coordinating Council (HSCC), including the following:

- Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)
- Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)
- Health Industry Cybersecurity Workforce Guide
- Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)
- Medical Device and Health IT Joint Security Plan (JSP)
- Health Industry Cybersecurity Managing Legacy Technology Security (HIC-MaLTS)

The serious nature of cyber-attacks makes it essential to continually compile and disseminate relevant, actionable information that mitigates the risk of cyber-attacks. HHS promotes transparency and a partnership mentality by collaborating with HPH sector organizations. We develop and maintain cybersecurity guidelines, like this publication, that can be used across healthcare organizations. These partnerships enable HHS to expand its ability to ingest, create, and share threat information, general cybersecurity practices, and mitigation strategies. As data becomes more complex and technology becomes more sophisticated, we must continue to work together to maintain cybersecurity vigilance.

The drive towards a consistent, resilient, and robust cybersecurity strategy starts with HHS and each public- and private-sector healthcare organization. It continues by building strong working relationships with associations, vendors, and other user communities in the patient care continuum. Cybersecurity must be the responsibility of every healthcare professional, from data entry specialists to physicians to board members. Importantly, patients also have cybersecurity responsibilities to safeguard their personal information and be vigilant when providing information electronically. Effective cybersecurity goes beyond privacy and reputation to control of patient data and healthcare systems and, ultimately, to providing safe, accurate, and uninterrupted treatment.

> There must be a cultural change and an acceptance of the importance and necessity of cybersecurity as an integrated part of patient care.

To adequately maintain patient safety and protect our sector's information and data, there must be a culture change and an acceptance of the importance and necessity of cybersecurity as an integrated part of patient care. The changes and the resulting effort required will not abate, but will rather change with the times, technologies, threats, and events. Now is the time to start, and, together, we can achieve real results.

Since 2017, this 405(d) public-private partnership has achieved tangible results and increased the HPH sector's cybersecurity awareness. HHS is committed to continue this work with our health sector partners to move closer towards a common understanding that Cyber Safety is Patient Safety.

Acknowledgements

Original Publication

More than 150 members from the private and public Sectors of the HPH sector have participated in the HHS 405(d) Task Group. These members bring experience and knowledge from diverse backgrounds and roles, including cybersecurity, privacy, healthcare, health IT, and other areas. The Task Group convened in May 2017.

We thank all Task Group members who collectively dedicated thousands of hours of their valuable time and expertise to fulfill the directives of CSA 405(d). We extend special thanks to the following authors and members of the original publication for their contributions to this document.

The following participants provided leadership to develop the documents that constitute this publication:

Lee Barrett
Matthew Barrett
Daniel Bowden
William Cai
Emery Csulak
Allana Cummings
Erik Decker—lead
Stephen Dunkle
David Finn
Mark Jarrett, M.D.
Wayne Lee
Lenny Levy
Dane Nordenberg
Gabriel Portillo
Erika Riethmiller
Kendra Siler
Philip A. Smith, M.D.
Mitch Thomas

The following members of the Writing Committee contributed, reviewed, and edited content for the documents that constitute this publication: Kenneth Adams; Daniel Bowden; Julie Chua; Allana Cummings; Erik Decker; Stephen Dunkle; Ken Durbin; Anna Etherton; Ty Greenhalgh; David Finn; David Holtzman; Mark Jarrett, M.D.; Wayne Lee; Leonard Levy; Dale Nordenberg; Erika Riethmiller; Philip A. Smith, M.D.; Mitch Thomas; and David Willis, M.D.

2023 Edition

Additionally, we would like to provide thanks to those individuals who contributed to this updated version of the HICP document. It is through their efforts that this document will remain timely and useful for the current healthcare cybersecurity environment. This edition is the result of the leadership and the collaboration of the following groups and professionals: the HPH Joint Cybersecurity Working Group, the Health Sector Coordinating Council, the Population Health Information Sharing and Analysis Center (PH-ISAC), the 405(d) Steering Committee, and the 405(d) Task Group.

We would like to mention the leadership and collaboration of the following professionals: Michael Alicea, Lee Barrett, Lee Barrett, Cindi Bassford, Karen Blanchette, Hazel Chappell, Phil Curran, Erik Decker, Ed Gaudet, Donna Grindle, Navar Holmes, David Holtzman, Steven Hughes, Jaz King, Lenny Levy, Bruce McDonald, Brady Miller, Andy Price, Pye Reddy, Kendra Siler, David Sims, Dallas Smith, Mitch Thomas, Amy Wood.

We would also like to express gratitude to HHS, DHS, and NIST for their input, collaboration, and efforts to establish and support the 405(d) Task Group and the updated edition.

Appendix A: Overview of Technical Volumes and Practices

As presented in Technical Volumes 1 and 2, the ten Cybersecurity Practices range from personnel training and awareness to the development and implementation of new processes, the acquisition and customization of new technology, and, ultimately, to fostering a consistent, robust, and continually updated approach to cybersecurity. The Practices are not intended to be comprehensive; they are meant to be considered as part of an organization's overall cybersecurity program. Furthermore, the Practices are intended to be recommendations and are not presented as the only solution.

The Practices introduced in this publication strengthen cybersecurity capabilities in healthcare organizations by:

- enabling organizations to evaluate and benchmark cybersecurity capabilities effectively and reliably;
- sharing knowledge, common practices, and appropriate references across organizations to improve cybersecurity competencies; and
- enabling organizations to prioritize actions and investments—knowing what to ask—to improve cybersecurity.

This Main Document and the accompanying Technical Volumes are intended to be descriptive, rather than prescriptive. All the practices presented can be reviewed for applicability within your organization to reduce the potential impacts of the five current threats discussed in the previous sections. The intent of these cybersecurity practices is not to introduce a new framework, new methodology, or new regulatory requirement into the cybersecurity space. Rather, to introduce practices relevant to the HPH sector—helping raise the cybersecurity floor across the healthcare industry regarding defensive and responsive cybersecurity practices. They may be implemented in whole or in part. Additionally, the practices are not prioritized. An organization should assess its current security and risk posture to determine how to prioritize the practices and should allocate resources accordingly. A method and toolkit for determining and prioritizing the practices to implement are described in the Cybersecurity Practices Assessments Toolkit (also known as Appendix E-1).

The practices discussed in the two Technical Volumes align with the outcomes listed in the NIST Framework. The NIST Framework is organized by the five steps to manage cyber threats: Identify, Protect, Detect, Respond, and Recover.

Two Technical Volumes can be accessed here:

- Technical Volume 1: Cybersecurity Practices for Small Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Organizations

The Technical Volumes are organized according to the following ten most effective Cybersecurity Practices, selected by the 405(d) Task Group to mitigate the current threats identified:

1. Email protection systems
2. Endpoint protection systems
3. Access management
4. Data protection and loss prevention
5. Asset management
6. Network management
7. Vulnerability management
8. Security operation centers and incident response
9. Network connected medical devices
10. Cybersecurity oversight and governance

Each Technical Volume presents these ten Practices, followed by a total of 88 sub-practices, with implementation recommendations. Tables 7, 8, and 9 on the following pages serve as an at-a-glance reference to the practices and sub-practices. Not all sub-practices will be effective for every organization.

To help assess each sub-practice and its application to your organization, an evaluation methodology and toolkit is provided in Appendix E: Practices Assessment, Roadmap and Toolkit. This methodology and toolkit offer guidance to select and prioritize the sub-practices that are most relevant to you.

Table 7. Cybersecurity Practices and Sub-Practices for Small Organizations

Small Organization	
Cybersecurity Practice	Sub-Practice
1: Email Protection Systems	**1.S.A** Email System Configuration **1.S.B** Education **1.S.C** Phishing Simulation
2: Endpoint Protection Systems	**2.S.A** Basic Endpoint Protection Controls
3: Access Management	**3.S.A.** Basic Access Management
4: Data Protection and Loss Prevention	**4.S.A** Policies **4.S.B** Procedures **4.S.C** Education
5: Asset Management	**5.S.A** Inventory **5.S.B** Procurement **5.S.C** Decommissioning
6: Network Management	**6.S.A** Network Segmentation **6.S.B** Physical Security and Guest Access **6.S.C** Intrusion Prevention
7: Vulnerability Management	**7.S.A** Vulnerability Management
8: Security Operation Centers and Incident Response	**8.S.A** Incident Response **8.S.B** ISAC/ISAO Participation
9: Network Connected Medical Devices	**9.S.A** Medical Device Security
10: Cybersecurity Oversight and Governance	**10.S.A** Policies **10.S.B** Cybersecurity Risk Assessment and Management **10.S.C** Security Awareness and Training **10.S.D** Cyber Insurance

Table 8. Cybersecurity Practices and Sub-Practices for Medium-Sized Organizations

Medium Organization	
Cybersecurity Practice	Sub-Practice
1: Email Protection Systems	**1.M.A** Basic Email Protection Controls **1.M.B** Multifactor Authentication for Remote Access **1.M.C** Email Encryption **1.M.D** Workforce Education
2: Endpoint Protection Systems	**2.M.A** Basic Endpoint Protection Controls
3: Access Management	**3.M.A** Identity **3.M.B** Provisioning, Transfers, and Deprovisioning Procedures **3.M.C** Authentication **3.M.D** Multi-Factor Authentication for Remote Access
4: Data Protection and Loss Prevention	**4.M.A** Classification of Data **4.M.B** Data Use Procedures **4.M.C** Data Security **4.M.D** Backup Strategies **4.M.E** Data Loss Prevention
5: Asset Management	**5.M.A** Inventory of Endpoints and Servers **5.M.B** Procurement **5.M.C** Secure Storage for Inactive Devices **5.M.D** Decommissioning Assets
6: Network Management	**6.M.A** Network Profiles and Firewalls **6.M.B** Network Segmentation **6.M.C** Intrusion Prevention Systems **6.M.D** Web Proxy Protection **6.M.E** Physical Security of Network Devices
7: Vulnerability Management	**7.M.A** Host/Server Based Scanning **7.M.B** Web Application Scanning **7.M.C** System Placement and Data Classification **7.M.D** Patch Management, Configuration Management **7.M.E** Change Management
8: Security Operation Centers and Incident Response	**8.M.A** Security Operations Center **8.M.B** Incident Response **8.M.C** Information Sharing and ISACs/ISAOs
9: Network Connected Medical Devices	**9.M.A** Medical Device Management **9.M.B** Endpoint Protections **9.M.C** Identity and Access Management **9.M.D** Asset Management **9.M.E** Vulnerability Management **9.M.F** Contacting the FDA

Medium Organization	
Cybersecurity Practice	Sub-Practice
10: Cybersecurity Oversight and Governance	**10.M.A** Policies **10.M.B** Cybersecurity Risk Assessment and Management **10.M.C** Security Awareness and Training

Table 9. Cybersecurity Practices and Sub-Practices for Large Organizations

Large Organization	
Cybersecurity Practice	Sub-Practice
1: Email Protection Systems	**1.L.A** Advanced and Next-Generation Tooling **1.L.B** Digital Signatures **1.L.C** Analytics Driven Education
2: Endpoint Protection Systems	**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
3: Access Management	**3.L.A** Federated Identity Management **3.L.B** Authorization **3.L.C** Access Governance **3.L.D** Single Sign-On
4: Data Protection and Loss Prevention	**4.L.A** Advanced Data Loss Prevention **4.L.B** Mapping of Data Flows
5: Asset Management	**5.L.A** Automated Discovery and Maintenance **5.L.B** Integration with Network Access Control
6: Network Management	**6.L.A** Additional Network Segmentation **6.L.B** Command and Control Monitoring of Perimeter **6.L.C** Anomalous Network Monitoring and Analytics **6.L.D** Network Based Sandboxing/Malware Execution **6.L.E** Network Access Control
7: Vulnerability Management	**7.L.A** Penetration Testing **7.L.B** Vulnerability Remediation Planning **7.L.C** Attack Simulation

Large Organization	
Cybersecurity Practice	Sub-Practice
8: Security Operation Centers and Incident Response	**8.L.A** Advanced Security Operations Center **8.L.B** Advanced Information Sharing **8.L.C** Incident Response Orchestration **8.L.D** Baseline Network Traffic **8.L.E** User Behavior Analytics **8.L.F** Deception Technologies
9: Network Connected Medical Devices	**9.L.A** Security Operations and Incident Response **9.L.B** Procurement and Security Evaluations
10: Cybersecurity Oversight and Governance	**10.L.A** Cyber Insurance

Appendix B: 405(d) Program and History

Cybersecurity Act of 2015: Task Group Undertakes a Legislative Mandate

The CSA became law in 2015. As illustrated in **Figure 12**, within this legislation is Section 405(d): Aligning Healthcare Industry Security Approaches. In response to the CSA Section 405(d) requirement, HHS leveraged the HPH sector's Critical Infrastructure Security and Resilience Partnership to establish the 405(d) Task Group. To learn more about this important partnership, please visit ASPR's Division of Critical Infrastructure Protection.

HHS convened the Task Group in May 2017 to plan, develop, and draft this guidance document. To ensure a successful outcome and a collaborative public-private development process, HHS engaged a diverse group of healthcare and cybersecurity experts from the public and private sectors. In 2019, the Task Group began working on an update to HICP. Participation was open and voluntary.

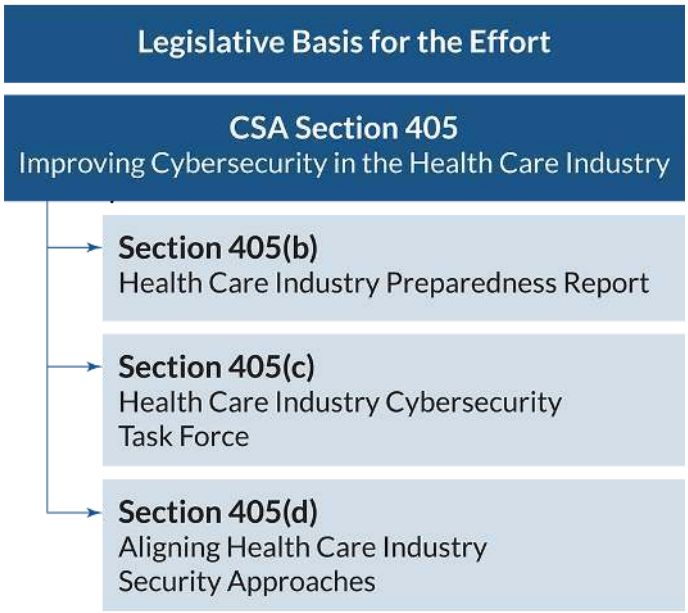
HHS collaborated with the HPH Sector Government Coordinating Council, the HPH Sector Coordinating Council, DHS, and NIST.*

The Task Group's approach to the guidance document:

1. Examines current cybersecurity threats affecting the HPH sector;
2. Identifies specific weaknesses that make organizations more vulnerable to the threats; and
3. Provides selected practices that cybersecurity experts rank as the most effective to mitigate the threats.

* Participants included subject matter experts with backgrounds and experience in the following roles: Chief Executive Officer; Chief Information Security Officer (CISO) and/or IT security professional; chief information officer; chief risk officer or other risk manager; office of technology leader or hospital administrator; doctor, nurse, and other healthcare practitioners.

Figure 12. Section 405(d) is Part of CSA Section 405, Which Focuses on the HPH Sector



405(d) and the Health Sector Coordinating Council

The 405(d) Task Group is a standing task group within the larger HSCC Joint Cybersecurity Working Group (CWG). The HSCC is a private-sector organized and managed council created within the framework set forth in Executive Order 13636 (2013) and Presidential Policy Directive 21 (PPD-21). The 405(d) Task Group Members are by association members of the HSCC; thus membership is defined by the HSCC Charter CWG Charter. The Task Group utilizes their connection to HSCC to meet the strategic goal of industry collaboration by reviewing other HSCC products that could be turned into 405(d) products, such as the HICP publication.

Aligning Healthcare Industry Security Approaches

The HHS 405(d) website, 405d.hhs.gov, is the home for all 405(d) publications and resources. In addition to the HICP publication, the website also features healthcare-focused resources such as:

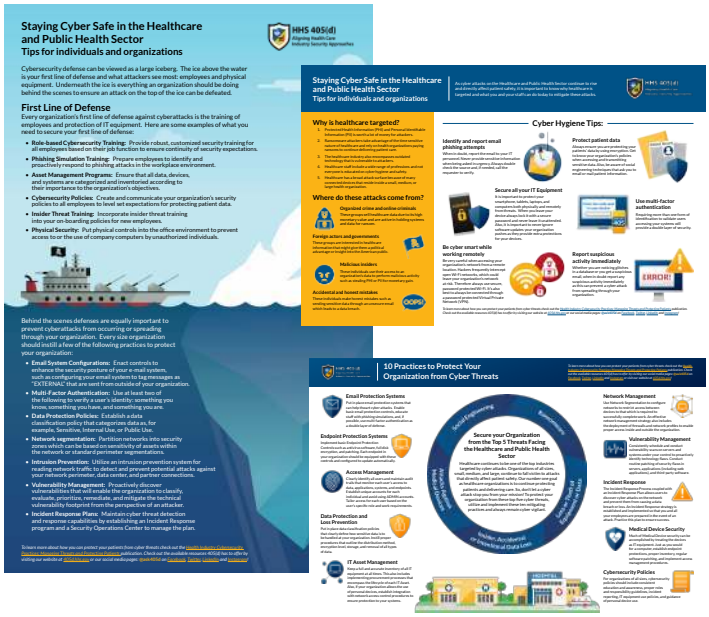
- Tips on how to get started with your cybersecurity protection
- 5 Threat resources
- 10 Practice resources
- Infographics
- SBARs
- 405(d) Post editions
- 405(d) Spotlight webinars
- General cybersecurity awareness resources for your organization!

The 405(d) website establishes a single 405(d) Program platform for the entire HPH sector to reference for HPH-focused cybersecurity resources provided by this public-private partnership initiative.

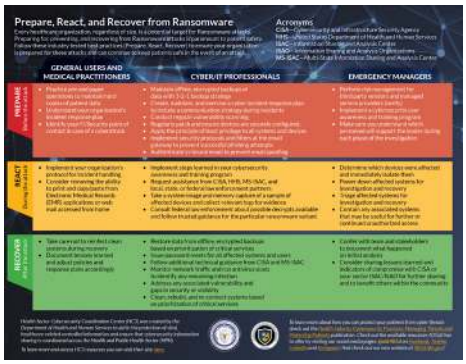
You can also stay up to date with the latest 405(d) product releases by subscribing to our mailing list on the homepage of the 405(d) website, as well as by following **@ask405d** on Facebook, LinkedIn, Twitter, and Instagram.

How-To Products

Infographics



Prepare, React, and Recover from Ransomware



SBARs

The 405(d) Post

Appendix C: Acronyms and Abbreviations

Acronym/Abbreviation	Definition
ACO	Accountable Care Organization
ASL	Assistant Secretary for Legislation
ASPA	Assistant Secretary for Public Affairs
ASPR	Administration for Strategic Preparedness and Response
BAA	Business Associate Agreement
BEC	Business Email Compromise
BYOD	Bring Your Own Device
CIN	Clinically Integrated Network
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CSA	Cybersecurity Act of 2015
CSP	Cybersecurity Practice
CWG	Cyber Working Group
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
EHR	Electronic Health Record
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FTA	File Transfer Appliance
HC3	Health Sector Cybersecurity Coordination Center
HDO	Healthcare Delivery Organization
HHS	Department of Health and Human Services
HICP	Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
HIPAA	Health Insurance Portability and Accountability Act
H-ISAC	Health Information Sharing and Analysis Center
HPH	Healthcare and Public Health
HSCC	Health Sector Coordinating Council
IBM	International Business Machines Corporation
IC3	Internet Crime Complaint Center
ICU	Intensive Care Unit
IDN	Integrated Delivery Network
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Intellectual Property or Internet Protocol

Acronym/Abbreviation	Definition
IPS	Intrusion Prevention Systems
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
MAC	Media Access Control
MD	Medicinae Doctor (Doctor of Medicine)
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCR	Office for Civil Rights
OGC	Office of the General Counsel
OIG	Office of the Inspector General
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
PH-ISAC	Population Health Information Sharing and Analysis Center (PH-ISAC)
PII	Personal Identifiable Information
RAM	Random Access Memory
RDP	Remote Desktop Protocol
URL	Uniform Resource Locator
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network

Appendix D: References

1. Stack, Brian. "Here's How Much Your Personal Information Is Selling for on the Dark Web." Experian. December 6, 2017. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
2. IBM Security. "Cost of a Data Breach Report 2020." 2021. https://www.ibm.com/reports/data-breach.
3. IBM. "Cost of a Data Breach Report 2021." 2022. https://www.ibm.com/reports/data-breach.
4. Davis, Jessica. "Computer Theft Exposes Personal, Health Data of 654K Oregon Patients." Health IT Security. February 2, 2020. https://healthitsecurity.com/news/computer-theft-exposes-personal-health-data-of-654k-oregon-patients.
5. IBM. "Cost of a Data Breach Report 2021." 2022. https://www.ibm.com/reports/data-breach.
6. "Largest Healthcare Data Breaches of 2021." HIPAA Journal. December 30, 2021. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/.
7. Federal Bureau of Investigation: Internet Crime Report 2021 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
8. Verizon. 2020 Data Breach Investigation Report. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
9. Sophos. "The State of Ransomware 2022." April 2022. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf.
10. McGee, Marianne Kolbasuk. "Record Number of Major Health Data Breaches in 2021." Gov Info Security. Last updated January 17, 2022. https://www.govinfosecurity.com/record-number-major-health-data-breaches-in-2021-a-18327.
11. "December 2021 Healthcare Data Breach Report." HIPAA Journal. January 18, 2022. https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/.
12. Verizon. "DBIR: 2021 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.
13. Hahn, Willa. "Medical Device Risks Continue to Threaten Hospital Security and Patient Safety." Cynerio. January 19, 2022. https://www.cynerio.com/blog/cynerio-research-finds-critical-medical-device-risks-continue-to-threaten-hospital-security-and-patient-safety.