

Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients



Healthcare & Public Health
Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

This page intentionally left blank

Table of Contents

Disclaimer.....	2
Letter from the HHS Deputy Secretary	3
Foreword	4
Executive Summary	5
Call to Action: Cybersecurity a Priority for Patient Safety	5
Cybersecurity Act of 2015: Task Group Undertakes a Legislative Mandate.....	5
The Publication: Health Industry Cybersecurity Practices	6
Audience and Publication Components	6
Cybersecurity Threats and Mitigation Practices	6
Cybersecurity Attacks Continue to Affect the Health Care Industry	7
Why Should You Worry About Cybersecurity and Take Action Now?.....	9
How Does This Publication Help Me?	10
Can It Happen To Me?	10
Where Do I Fit?.....	11
Be Proactive: Hand Hygiene for Cybersecurity	12
Current Threat Scenarios Facing the Health Care Industry	13
Explaining Threats and Vulnerabilities	13
A Translation: Threats, Vulnerabilities, Impact, and Practices.....	14
Introducing Current Threats to the Health Care Industry.....	14
Threat: E-mail Phishing Attack.....	16
Threat: Ransomware Attack	18
Threat: Loss or Theft of Equipment or Data	20
Threat: Insider, Accidental or Intentional Data Loss	22
Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety	24
Cybersecurity Practices	26
Looking Ahead.....	27
Overview of Technical Volumes.....	28
Acknowledgements	31
Appendix A: Acronyms and Abbreviations	32
Appendix B: References.....	33

Tables

Table 1: Selecting the “Best Fit” For Your Organization.....	11
Table 2: Suggested Practices to Combat E-mail Phishing Attacks	17
Table 3: Suggested Practices to Combat Ransomware Attacks.....	19
Table 4: Suggested Practices to Combat Loss or Theft of Equipment or Data	21
Table 5: Suggested Practices to Combat Insider, Accidental or Intentional Data Loss.....	23
Table 6: Suggested Practices to Combat Attacks Against Medical Devices That May Affect Patient Safety	25
Table 7: Cybersecurity Practices and Sub-Practices for Small Organizations.....	28
Table 8: Cybersecurity Practices and Sub-Practices for Medium Organizations.....	29
Table 9: Cybersecurity Practices and Sub-Practices for Large Organizations.....	30

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 health care 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

Cyberattacks are an increasing threat across all critical infrastructure sectors. For the health sector, cyberattacks are especially concerning because these attacks can directly threaten not just the security of our systems and information but also the health and safety of American patients. We are under constant cyberattack in the health sector, and no organization can escape that reality. While innovation in health information technology is a cause for optimism and increasing sophistication in health IT holds the promise to help address some of 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.

HHS has a holistic view of the intersection between cybersecurity and healthcare, including data protection and response to cyber threats. Cybersecurity remains a top priority at HHS and is reflected in recent cybersecurity initiatives, including the development of this publication, titled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients."

This publication is the result of the collaborative work HHS and its industry partners embarked on more than a year ago—namely, the development of practical, understandable, implementable, industry-led, and consensus-based voluntary cybersecurity guidelines to cost-effectively reduce cybersecurity risks for health care organizations of varying sizes, ranging from local clinics, regional hospital systems, to large health care systems.

Many of the most influential industry organizations in healthcare came together as the 405(d)ⁱ Task Group in May 2017, to plan, develop and draft this publication. HHS engaged a diverse group of more than 150 healthcare and cybersecurity experts through the Health Sector Coordinating Council as well as our government partners. The Task Group focused on building a set of voluntary, consensus-based principles and practices to improve cybersecurity in the health sector. The group determined that it was not feasible to address every cybersecurity challenge across the large and complex U.S. healthcare industry. Therefore, it focused on the five most prevalent cybersecurity threats and the ten cybersecurity practices to significantly move the needle for a broad range of organizations within our sector.

Positive outcomes have come from a shared commitment to addressing this challenge. With each step, we will provide a safer and more secure environment for providers to deliver services, for manufacturers to develop products, and for patients to receive high-quality, uninterrupted care. Cybersecurity is a shared responsibility. HHS will continue to build partnerships with stakeholders to become a better, more coordinated team. Together, we can take on the cybersecurity challenges that lie ahead.

We have achieved great progress already but, as we know, in cybersecurity our work is never finished. I encourage anyone interested in cybersecurity and patient safety to get involved. If you are interested in joining the 405(d) Task Group, reach out to the [Task Group](mailto:CISA405d@hhs.gov) directly at CISA405d@hhs.gov.

/s/ Eric Hargan

Deputy Secretary of Health and Human Services

ⁱ Cybersecurity Act of 2015, Public Law 114-113, Section 405(d) "Aligning Health Care Industry Security Approaches" codified at 6 U.S.C. §1533 (d)

Foreword from Co-Leads

Over the past decade, the threat to the health care industry has increased dramatically along with the sophistication of cyber-attacks. Industry and government alike have recognized the dawning of this new era. For each gain delivered by automation, interoperability, and data analytics, the vulnerability to malicious cyber-attacks increases as well. To thwart these attacks before they occur, it is essential for health care organizations to establish, implement, and maintain current and effective cybersecurity practices.

The Cybersecurity Act of 2015 (CSA) (Public Law 114-113)¹ establishes a trusted platform and a tighter partnership between the United States (U.S.) government and the private sector, recognizing that our critical infrastructure, economic solvency, and personal safety have become intertwined with our digital technologies.

Section 405(d) of CSA calls for “Aligning Health Care Industry Security Approaches.” It is with this imperative that industry and government came together under the auspices of the 405(d) Task Group, starting in May 2017. The Task Group focused on building a set of voluntary, consensus-based principles and practices to ensure cybersecurity in the Health Care and Public Health (HPH) sector. This document reflects the Task Group’s current recommendations.

The Task Group determined that it was not feasible to address every cybersecurity challenge across the large and complex U.S. health care industry in a single document. The Task Group therefore made the decision to focus on the most impactful threats, with the goal of significantly moving the cybersecurity needle for a broad range of organizations within the industry.

The HPH sector comprises many different types of organizations, widely varying in size, complexity, capabilities, and available resources. The 405(d) Task Group determined that it is critical to tailor cybersecurity practices to a health care organization’s size, namely, small, medium-sized, or large. Each organization has specific cybersecurity-related attributes, strengths, and vulnerabilities, and, for the recommended cybersecurity practices to be optimally effective, organizations must tailor them to their unique needs.

Importantly, the Task Group recognized the complexity of cybersecurity threats. There is no simple method to combat them all. As a result, the Task Group provided a model, aligned with National Institute of Standards and Technology (NIST), and a method for assessment, which is discussed in *Appendix E* of this publication. This assessment will help organizations determine the implementation priority of the practices set forth by the Task Group based upon the threats with which they are most concerned.

We do not expect the practices provided in this publication to become a de facto set of requirements that all organizations must implement. Such a dogmatic approach is not effective given the dynamic nature of cybersecurity threats and the fast pace of technology evolution and adoption. Furthermore, we do not guarantee that these practices will aid organizations in meeting their compliance and reporting obligations.

This document does not create new frameworks, re-write specifications, or “reinvent the wheel.” We felt that the best approach to “moving the cybersecurity needle” was to leverage the NIST Cybersecurity Framework (*Appendix D*), introducing the Framework’s terms to start educating health sector professionals on an important and generally accepted language of cybersecurity and answering the prevailing question, “Where do I start and how do I adopt certain cybersecurity practices?”

We hope this document and its accompanying technical volumes and tools help answer that question.

/s/ Erik C. Decker

Health Sector Coordinating Council Co-Lead
Chief Security and Privacy Officer,
University of Chicago Medicine
Chairman of the Board, Association for Executives in
Health Care Information Security

/s/ Julie Chua

Health Sector Government Coordinating Council Co-Lead
Risk Management, Office of Information Security
Office of the Chief Information Officer
U.S. Department of Health and Human Services

Executive Summary

Call to Action: Cybersecurity a Priority for Patient Safety

Cybersecurity threats to health care organizations and patient safety are real. Health information technology, which provides critical life-saving functions, 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 and led to an inability to access patient records to continue care delivery. Such cyber-attacks 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 health care records, IT systems, and medical devices have infected even the most hardened systems.

Given the increasingly sophisticated and widespread nature of cyber-attacks, the health care industry 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, medical device manufacturers, and governments (state, local, tribal, territorial, and federal) to mitigate the risks and minimize the impacts of a cyber-attack. The U.S. Department of Health and Human Services (HHS) and the Health Care and Public Health (HPH, Health Sector, Health Care Industry) sector are working together to address these challenges.

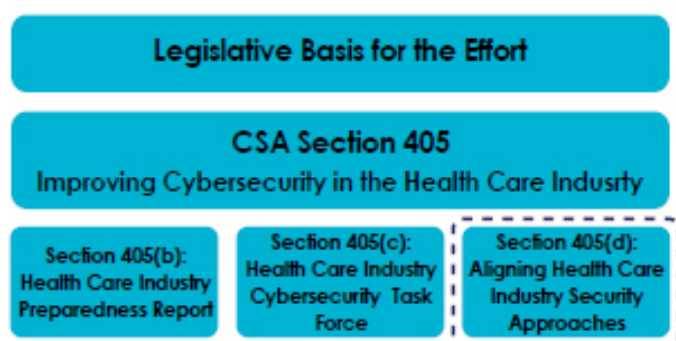


Figure 1. Section 405(d) is Part of CSA Section 405, Which Focuses on the U.S. Health Care Industry

Cybersecurity Act of 2015: Task Group Undertakes A Legislative Mandate

The Cybersecurity Act (CSA) became law in 2015. As illustrated in Figure 1, within this legislation is Section 405(d): Aligning Health Care Industry Security Approaches. In response to the CSA 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 <https://www.phe.gov/preparedness/planning/cip/Pages/default.aspx>.)*

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 health care and cybersecurity experts from the public and private sectors. Participation was open and voluntary. HHS collaborated with the HPH Sector Government Coordinating Council, the HPH Sector Coordinating Council, the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST).ⁱⁱ

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.

ⁱⁱ 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 health care practitioners

The Publication: Health Industry Cybersecurity Practices

In accordance with the CSA, this document 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 a range of health care organizations;
2. Support the voluntary adoption and implementation of its recommendations; and
3. Ensure, on an ongoing basis that content is actionable, practical, and relevant to health care stakeholders of every size and resource level.

Audience and Publication Components

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

The entire publication includes this main document, two technical volumes, and appendices:

- The **Main Document** discusses the current cybersecurity threats facing the health care industry. It sets forth a call to action for the health care industry, especially executive decision makers, with the goal of raising general awareness of the issue.
- **Technical Volume 1** discusses the ten Cybersecurity Practices (herein called Practices) and Sub-Practices for small health care organizations. It is intended for IT and/or IT security professionals and serves to guide organizations on what to ask their IT and/or IT security teams or vendors.
- **Technical Volume 2** discusses the ten Cybersecurity Practices (herein called Practices) and Sub-Practices for medium-sized and large health care organizations. It is intended for IT and/or IT security 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:

- E-mail phishing attacks
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices that may affect patient safety

The Technical Volumes detail ten Practices to mitigate these threats. The ten Practices are as follows:

- E-mail protection systems
- Endpoint protection systems
- Access management
- Data protection and loss prevention
- Asset management
- Network management
- Vulnerability management
- Incident response
- Medical device security
- Cybersecurity policies

The entire publication considers the recommendations made by HHS divisions including, but not limited to, the Assistant Secretary for Legislation, the Assistant Secretary for Public Affairs, the Assistant Secretary for Preparedness and Response, the Centers for Medicare and Medicaid Services, the Food and Drug Administration, the Office for Civil Rights, the Office of the Chief Information Officer, the Office of the General Counsel, the Office of the Inspector General, and the Office of the National Coordinator for Health Information Technology, as well as guidelines and practices from DHS and NIST.

Cybersecurity Attacks Continue to Affect the Health Care Industry

Medical professionals help patients identify probable health risks, for example based on family history of medical conditions. They also help patients protect themselves against those risks by making appropriate lifestyle changes and by implementing regimens to detect any health conditions that might arise. Additionally, medical professionals and patients respond to health conditions with appropriate medical protocols and recover as much of the patients' previous health as possible. Similarly, this document identifies current cybersecurity threats in the health care industry and provides cybersecurity practice recommendations. These practice recommendations are consistent with the NIST Cybersecurity Framework (NIST Framework), discussed in *Appendix D*. The NIST Framework consists of five concurrent and continuous functions that constitute the cybersecurity lifecycle for any organization: **Identify, Protect, Detect, Respond, and Recover**.

The health care industry 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. In addition to the benefits derived from health care technology, health care organizations have 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 health care organizations, their business partners, and particularly, their patients.

"I entered into the health care field with a mission to protect and care for patients. This mission now includes cybersecurity."

Hackers of all types (nation-state actors, cyber criminals, hacktivists) have found numerous ways to make money from illegally obtained health care data. Examples include selling these data on the black market to facilitate Medicare fraud and identity theft, and the malicious gathering of foreign intelligence.

In 2016, a bold new threat arrived on the scene: **ransomware**, a type of malicious software that attempts to deny access to data, usually by encrypting the data with a key known only to the hacker, until the data's owners pay a ransom.

In ransomware schemes, attackers hold a hospital's or a physician's data hostage until money is paid, interrupting services and putting patients' lives at risk.

Ransomware attacks that occurred at hospitals in 2016 and 2017, distributed denial of service attacks, and theft of protected health information (PHI), all demonstrate that cyber threats are capable of triggering emergencies that impact patient care and public health. Furthermore, in 2016, a private hospital suffered a ransomware attack resulting in the freeze of all computer systems. The attack forced the hospital to revert to pen and paper during the downtime to maintain patient and data records. With the systems down, schedules, documents, and patient data were unavailable, requiring the transfer of some patients to nearby health care institutions for more complete care. The attacker demanded compensation before restoring access to the hospital's systems and network. Although authorities became involved, after a week, **the hospital conceded and paid the \$17,000 ransom to regain full operational control.**² Although the hospital regained control following the ransom payment in this instance, the FBI does not recommend paying ransoms to criminal actors. Furthermore, paying a ransom does not guarantee an organization will regain control of its data.

Addressing these threats requires a broad, collaborative approach across a multitude of organizations within government and the private sector. HHS is working with a wide-ranging coalition of partners to enhance cybersecurity within HHS and across the HPH sector. Cybersecurity is a challenge of technology and tactics, and organizations can meet the challenge through increased training and awareness, transparency, and coordination across the sector.

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

News headlines report major cyber-attacks on health care organizations. Following are two recently reported stories, with details removed to protect the privacy of those involved:

- **Orthopedics' Data Breach Put Patients**

Identities at Risk: A popular orthopedic practice announced that its computer system was hacked via breach of a software vendor's log-in credentials. This breach put just under a half-million people at risk of identity theft. Of those, 500 patient profiles appeared for sale on the dark web. The information for sale included names, addresses, social security numbers, and other personally identifiable information (PII). Although not posted for sale, pertinent PHI such as X-ray results and medical diagnoses were also stolen.

- **Entire Hospital Computer System Scrapped Due to Cyber-attack:** A rural hospital had to replace its entire computer network after a ransomware cyber-attack froze the hospital's electronic health record (EHR) system. Doctors were unable to review their patients' medical histories or transmit laboratory and pharmacy orders. Officials were unable to restore essential services and could not pay the ransom for the return of their system. After consultations with the Federal Bureau of Investigation and cybersecurity experts, hospital officials made the difficult decision to replace the entire system.



4 in 5

U.S. physicians have experienced some form of a cybersecurity attack

3



If either of these cyber-attacks happened to your organization, what would be your first response? Do you know what steps to take or who to contact? If you are a small physician practice, do you believe that this could happen to you, or do you dismiss the idea as something that only happens to large hospital systems? Just imagine for a moment that one of these news reports was about your practice.

Small Business Impacts:

- 58% of malware attack victims are small businesses.⁴
- In 2017, cyber-attacks cost small and medium-sized businesses an average of \$2.2 million.⁵
- 60% of small businesses go out of business within six months of an attack.⁶
- 90% of small businesses do not use any data protection at all for company and customer information.⁷

Why Should You Worry About Cybersecurity and Take Action Now?

Health care organizations are committed to providing the very best care to their patients. While the thought of risking patient safety to a cyber-attack is terrifying for any health care professional, 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.

According to a study from IBM Security and the Ponemon Institute, the cost of a data breach for health care organizations rose from \$380 per breached record in 2017 to \$408 per record in 2018.⁸ Across all industries, health care has the highest cost for data breaches.

Most health care personnel are experts at identifying and eradicating viruses in patients, not computers. 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 data and training personnel to be cyber-vigilant.

Cyber-attacks disrupt health care personnel’s ability to provide life-changing and life-saving capabilities.

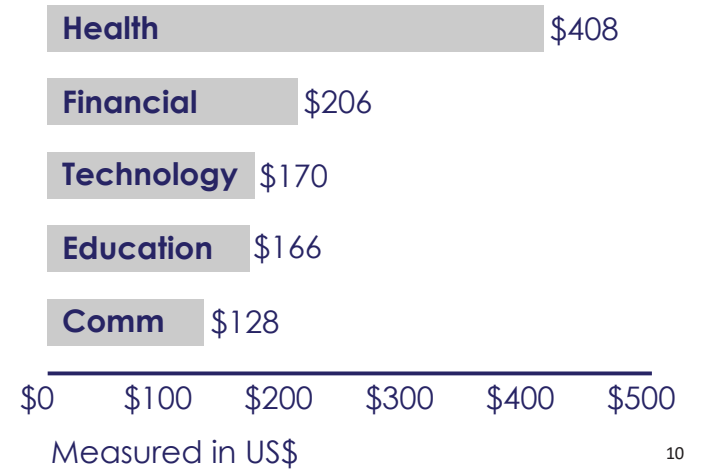
Cyber-attacks disrupt health care personnel’s ability to provide life-changing and life-saving capabilities. They impede the ability to disseminate patient data appropriately to other health care entities, which is a key benefit of digitization. For example, a Missouri health care organization was victim to a ransomware attack, leading the organization to redirect ambulances as a safety measure. This was a small clinic of under 50 beds that specialized in treating trauma and stroke patients.⁹ The attack compromised the entire EHR system, prompting the facility to take precautions in an effort to guarantee quality of care.

Health care organizations require current and resilient cybersecurity that is compatible across organizations **without restricting innovative efforts around population health, precision medicine, and transparency.**

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 continual battle, because hackers constantly find creative ways to defeat cyber threat defense initiatives. Health care organizations increasingly transmit data electronically, through mobile devices, cloud-based applications, medical devices, and technology infrastructures.

Data Breach Cost Per Record

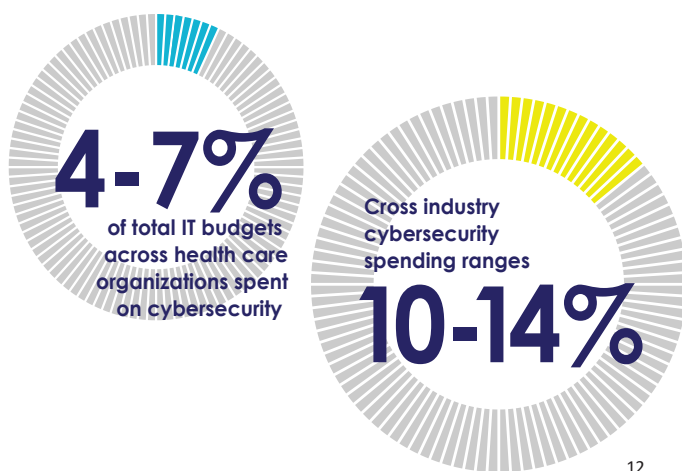


Often, organizations deploy technologies without cybersecurity safeguards or use them (intentionally or unintentionally) without proper protections, making them an appealing target for hackers. For example, a Montana hospital had over 7,000 patient records stolen from an employee’s e-mail while the employee was on business travel outside of the country.¹¹ The cyber-attack occurred while the individual was using an unsecure internet connection, making the device susceptible to the hacker. The e-mails and attachments were exposed, prompting the employer to put in place efforts to safeguard patient data.

How Does this Publication Help Me?

This publication provides a starting point of basic cybersecurity practices to implement in your health care organization. It does not prioritize the ten Practices in any order, but rather provides the flexibility for an organization to determine its unique security posture, through a risk assessment or other assessment, and to determine how to prioritize and allocate resources. All three components of the publication have the purpose of informing stakeholders in the health care community about current cybersecurity threats, what makes these effective attack methods for hackers, and what cybersecurity practices organizations can implement to thwart them.

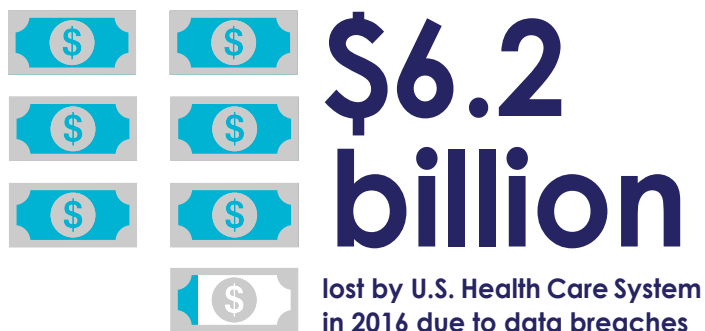
Cybersecurity incidents affect patient care and may represent serious threats to patient safety. Failing to address cyber issues can also negatively impact an organization's bottom line or result in loss of credibility and patient trust. It is this publication's intention to help the reader understand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



12

Can It Happen to Me?

It is tempting for those who own a health care practice or are part of a small-to-medium-sized health care organization to think that cyber-attacks only affect large hospitals and health care organizations. The reality is that cyber-attacks are indiscriminate and adversely affect healthcare practices of every size and specialization. The *IBM X-Force Threat Intelligence Index 2017*, a recent study designed to track cybersecurity incidents around the globe, identified the top-targeted cyber-attack industries, stating: *"It is worth noting that the health care industry, which fell just outside the top five in terms of records breached, continued to be beleaguered by a high number of incidents. However, attackers focused on smaller targets, resulting in a lower number of leaked records in that industry."*¹³



14

The "smaller targets" mentioned in the report may include small or medium-sized organizations. Hackers 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 health care entity, your job is to make it difficult for these attackers to succeed.

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.

Identifying your organization's size can be more complicated than it seems. It may be clear, for example, if you are a small practice with one or two providers and no affiliations or exchanges with other care systems. However, this configuration is not as common as it used to be. Even the smallest health care 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 in deciding which size tier is your “best fit.”

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

Table 1. Selecting the “Best Fit” For Your Organization

The Technical Volumes divide cybersecurity practices by organization size, so you can implement the Practices specific to the type of organization with which you most identify. *Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations* presents Practices intended specifically for small organizations.

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.

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 other than those within your “best fit” size category as you continuously build and improve your cybersecurity strategy.

Cyber Incident Reporting

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

- Please contact your [FBI Field Office Cyber Task Force](http://www.fbi.gov/contact-us/field/field-offices) www.fbi.gov/contact-us/field/field-offices 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.
- Please report cyber incidents to the [US-CERT](http://www.us-cert.gov/ncas) www.us-cert.gov/ncas and [FBI's Internet Crime Complaint Center](http://www.ic3.gov) www.ic3.gov
- For further analysis and healthcare-specific indicator sharing, please contact [HHS' Health Sector Cybersecurity Coordination Center](mailto:HC3@hhs.gov) (HC3) at HC3@hhs.gov

Be Proactive: Hand Hygiene for Cybersecurity

Doctors and nurses know that hand sanitizing is critical to prevent the spread of germs. That does not mean health care 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 are able to protect our patients from infection, we should all work towards protecting patient data to allow physicians and caregivers to trust the data and systems that enable quality health care.

Just as health care professionals must wash their hands before caring for patients, health care 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 hand-washing, a culture of cyber-awareness does not have to be complicated or expensive for a small organization. It must simply be effective at enabling organization members to protect information that is critical to the organization’s patients and operations.

Your organization’s vigilance against cyber-attacks will increase concurrently with your and your workforce’s knowledge of cybersecurity. This knowledge will enable you to advance to the next series of cybersecurity Practices, expanding your organization’s awareness of and ability to thwart cyber threats.

1,309 records
were inappropriately accessed by a
single
employee between 2016 and 2017



16

Current Threat Scenarios Facing the Health Care Industry

In this section, we introduce cybersecurity threats and some of the associated vulnerabilities that currently affect the health sector. Threats and vulnerabilities are two different types of exposure to cyber-attacks. Why is it important to understand the difference between the two? The ability to distinguish between the two helps determine which cybersecurity practices and tools are necessary and appropriate for your organization to mitigate the harm that may come from an attacker or from a mistaken or uninformed but authorized individual.

\$2.2 million

**is the average cost of a data
breach for health care organizations**



17

Explaining Threats and Vulnerabilities

Threats and vulnerabilities go hand in hand, but they are not interchangeable. Threats are internal or external 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, intentional or accidental. Think of hurricanes and floods causing power outages. These are examples of external, natural, accidental 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. Take an example that most health care practitioners are familiar with: 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 often exploits a vulnerability. Using the above example, most people would assume that an elderly person is more vulnerable than a college athlete to harm from the flu. This increased vulnerability is due to the diminished function of an aged immune system, reduced physical strength, and even compromised mental capabilities that 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 above discussion of threats and vulnerabilities applies similarly to cybersecurity. Threats to your organization may include phishing attacks, malware (e.g., ransomware), insider threats, lost equipment, hackers, and many others. These threats exist at some level for all health care 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 Health Care Industry

This next section describes five of the most current and common cybersecurity threats to health care organizations. As depicted in the hospital graphic on the next page, the five current cybersecurity threats are:

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

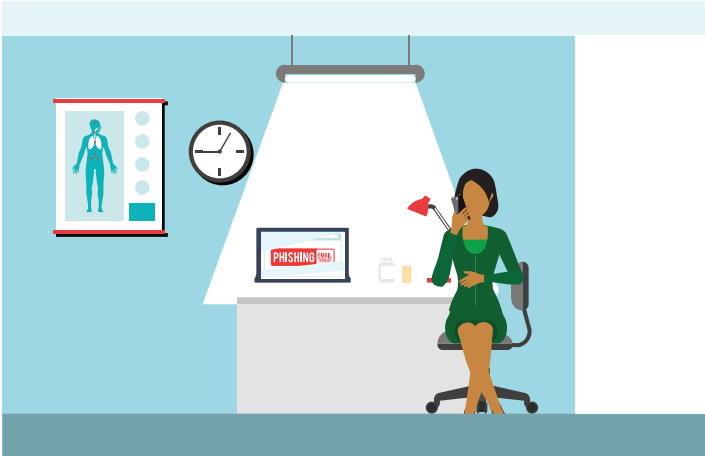
Each threat portrayed in the graphic is meant to show that these threats can affect organizations in various parts of a hospital and in different health care settings. Cyber-attacks can happen anywhere, any time. The following sections discuss these threats in detail, with additional quick tips for *What to Ask*, *When to Ask*, and *Who to Ask*.

Additionally, vulnerabilities that may determine the impact of each threat are listed in a table at the end of each threat section. The tables also include “Practices to Consider” for each threat to help you 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 7–9* serve as key references for this mapping (e.g. 1.S.B.) Sub-Practices labeled with “S” can be found in Technical Volume 1, and those labeled with “M” or “L” can be found in Technical Volume 2.



Threat: E-mail Phishing Attack



Description:
E-mail phishing is an attempt to trick you, a colleague, or someone else in the workplace into giving out information using e-mail. An inbound phishing e-mail includes an active link or file (often a picture or graphic). The e-mail appears to come from a legitimate source, such as a friend, coworker, manager, company, or even the user’s own e-mail 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.¹⁸

Real-World Scenario:
Your employees receive a fraudulent e-mail from a cyber-attacker disguised as an IT support person from your patient billing company. The e-mail 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:
A pediatrician learns that an attacker stole patient data using a phishing attack and used it in an identity theft crime.

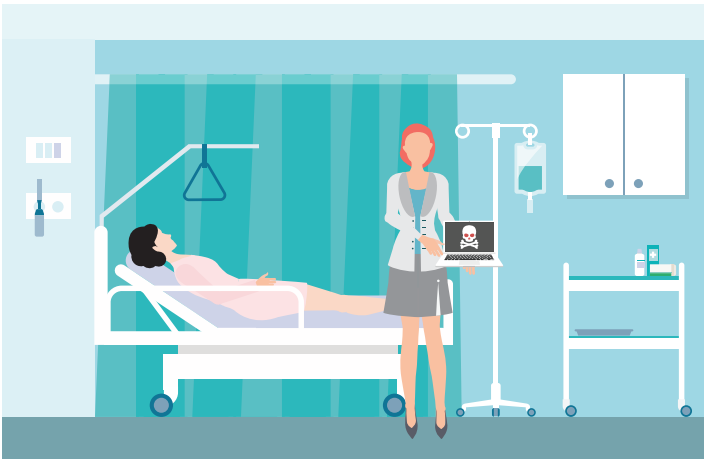
Table 2 identifies vulnerabilities, impacts, and Practices to consider for e-mail phishing attacks.

Threat Quick Tips	
What to Ask? 	On average, a person will receive about 80 e-mails 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? • Are there any spelling or grammatical errors, or any other indicators that the tone or style of the e-mail is off? • Before clicking on a link, did you hover over it to see the URL destination? • Do you know the sender, or are you suspicious of the e-mail? If in doubt, do NOT open any attachments. • What are my organization’s processes for reporting suspicious e-mails?
When to Ask? 	The best time to familiarize yourself with your organization’s policies for reporting a suspicious e-mail is when you begin employment. Whenever you receive an e-mail that sounds too good to be true or that you were not expecting, verify it before opening it!
Who to Ask? 	Check with colleagues to find out whether they received the same phishy e-mail. 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.

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

Table 2. Suggested Practices to Combat E-mail Phishing Attacks

Threat: Ransomware Attack



Description:

The [HHS Ransomware Factsheet](https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf), available at <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>, defines ransomware as follows: “Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user’s data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

However, hackers may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so.” Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats. For example, successful phishing attacks may lead to the installation of ransomware.

Real-World Scenario:

Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called security update is actually a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data.

Impact:

A practitioner cannot view patient charts because of a ransomware attack that has made the EHR system inaccessible.

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

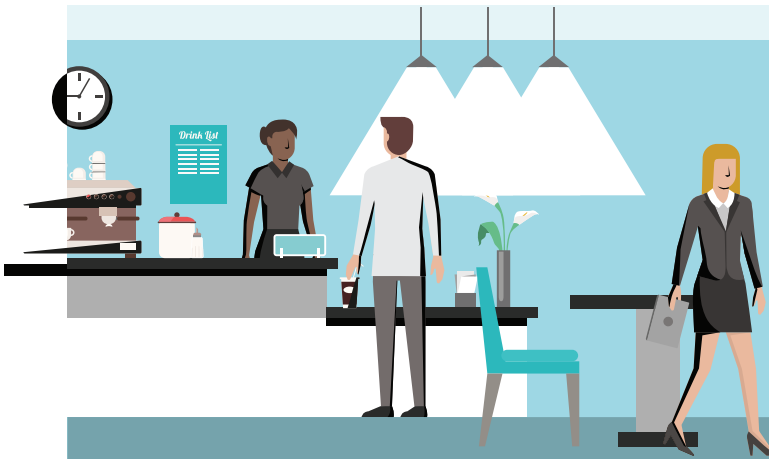
Threat Quick Tips	
What to Ask? 	Most ransomware attacks are sent in phishing campaign e-mails asking you to either open an attachment or click on an embedded link. Be sure you know how to identify these phishing e-mails! Stay alert when any e-mail asks you to enter your credentials. As a proactive measure, check to see whether the computer and network to which you are connected have the proper intrusion prevention system or software in place. 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?
When to Ask? 	Provide user awareness and compliance training during the onboarding process or when purchasing a new laptop or desktop equipment. If you discover that your computer has been infected, immediately disconnect from the network and notify your IT security team. Do not power off or shut down the computer or server, in case a volatile (RAM) memory image needs to be collected for forensics and incident response investigations.
Who to 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.

Threat: Ransomware Attack		
Vulnerabilities	Impact	Practices to Consider
Lack of system backup	Partial or complete clinical and service disruption Patient care and safety concerns Expenses for recovery The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	Ensure that users understand authorized patching procedures (7.S.A)
Lack of anti-phishing capabilities		Patch software according to authorized procedures (7.S.A)
Unpatched software		Be clear which computers may access and store sensitive or patient data (4.M.C)
Lack of anti-malware detection and remediation tools		Use strong/unique username and passwords with MFA (1.S.A, 3.S.A, 3.M.C)
Lack of testing and proven data back-up and restoration		Limit users who can log in from remote desktops (3.S.A, 3.M.B)
Lack of network security controls such as segmentation and access control		Limit the rate of allowed authentication attempts to thwart brute-force attacks (3.M.C)
		Deploy anti-malware detection and remediation tools (2.S.A, 2.M.A, 3.L.D)
		Separate critical or vulnerable systems from threats (6.S.A, 6.M.B, 6.L.A)
		Maintain a complete and updated inventory of assets (5.S.A, 5.M.A)
		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)
		Implement proven and tested incident response procedures (8.S.A, 8.M.B)
		Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C)
		Develop a ransomware recovery playbook and test it regularly (8.M.B)
		Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures (HHS Ransomware Fact Sheet)

Table 3. Suggested Practices to Combat Ransomware Attacks

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](https://csrc.nist.gov/publications/detail/sp/800-184/final) at <https://csrc.nist.gov/publications/detail/sp/800-184/final>

Threat: Loss or Theft of Equipment or Data



Description:

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 hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations. From January 1, 2018, to August 31, 2018, the Office for Civil Rights received reports of 192 theft cases affecting 2,041,668 individuals. Although the value of the device represents one loss, far greater are the consequences of losing a device that contains sensitive data. In cases where the lost device was not appropriately safeguarded or password protected, 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.

Real-World Scenario:

A physician stops at a coffee shop for a coffee and to use the public Wi-Fi to review radiology reports. As the physician leaves the table momentarily to pick up his coffee, 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, and, with thousands of records potentially stolen, the physician’s reputation could be at stake if all the patient records make it to the dark web for sale.

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

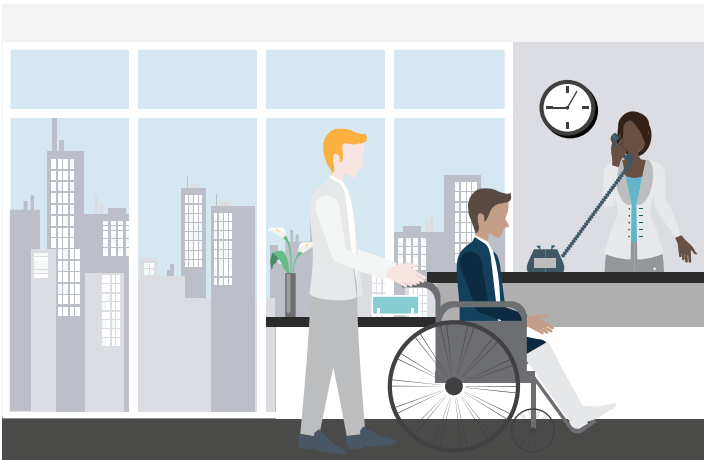
Threat Quick Tips	
What to Ask? 	Heading out on a business trip or a personal holiday? You need to follow the same, and maybe greater, security procedures as you do in the office. Make sure you know your organization’s policy on removing equipment from the workplace by asking: • Can I travel with my equipment? • Can I take my equipment offsite to work remotely? • Are USB or other portable storage devices allowed? • Is the information on my computer or storage device 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 to Ask? 	As soon as you realize that your device or equipment has been stolen or misplaced, your supervisor and IT security professional should be notified immediately so appropriate measures can be taken to safeguard the data saved on your device or equipment.
Who to 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 them 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.

Threat: Loss or Theft of Equipment or Data		
Vulnerabilities	Impact	Practices to Consider
Lack of asset inventory and control	Inappropriate access to or loss of sensitive patient information occurs; may involve proprietary or confidential company information or intellectual property	Encrypt sensitive data, especially when transmitting data to other devices or organizations (4.S.B, 4.M.C)
Lack of encryption; Data at rest is data stored on a hard drive at any location.		Implement proven and tested data backups, with proven and tested restoration of data (4.M.D)
Lack of physical security practices; open offices and poor physical access management, giving attackers opportunities		Acquire and use data loss prevention tools (4.M.E, 4.L.A)
Lack of simple safeguards such as computer cable locks to secure devices within office environments	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	Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices (9.M.A)
Lack of awareness that theft of IT assets from the office accounts for nearly as much as from cars	Lost productivity	Promptly report loss/theft to designated company individuals to terminate access to the device and/or network (3.S.A)
Lack of effective vendor security management, including controls to protect equipment or sensitive data	Damage to reputation	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)
Lack of “End-of-Service” process to clear sensitive data before IT assets, including medical devices, are discarded or transferred to other users or other organizations		Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device (4.M.C)
		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)

Table 4. Suggested Practices to Combat Loss or Theft of Equipment or Data

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](https://csrc.nist.gov/publications/detail/sp/800-184/final) at <https://csrc.nist.gov/publications/detail/sp/800-184/final>

Threat: Insider, Accidental or Intentional Data Loss



Description:

Insider threats exist within every organization where employees, contractors, or other users access the organization’s technology infrastructure, network, or databases. There are two types of insider threats: accidental and intentional.

An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. For example, being the victim of an e-mail phishing attack is an accidental insider threat.

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

Real-World Scenario:

An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.

Impact:

The patient’s PHI was compromised and used in an identity theft case.

Table 5 identifies vulnerabilities, impacts, and Practices to consider for accidental or intentional data loss.

Threat Quick Tips	
What to Ask? 	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 to 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 attack. By doing so, you can lower the probability of such attacks happening in your organization.
Who to Ask? 	Always consult your IT security professionals when exposed to a situation of stolen data or employee misconduct. Every situation will vary so your IT security professionals will be able to guide you best because a cyber-threat is not limited to hacking.

Threat: Insider, Accidental or Intentional Data Loss		
Vulnerabilities Files	Impact	Practices to Consider
containing sensitive data accidentally e-mailed to incorrect or unauthorized addressees 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 e-mail and file storage Lack of technical controls to monitor the e-mailing and uploading of sensitive data outside the organization's network Lack of physical access controls Lack of training about social engineering and phishing attacks	Accidental loss of PHI or PII through e-mail 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 because the attacker used a phishing e-mail disguised as originating from the bank Patients given the wrong medicines or treatment because of incorrect data in the EHR	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) 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 e-mail and web uploads (4.M.E, 4.L.A)

Table 5. Suggested Practices to Combat Insider, Accidental or Intentional Data Loss

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety



Description:

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

Real-World Scenario:

A cyber attacker gains access to a care provider’s computer network through an e-mail phishing attack and takes command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.

Impact:

Patients are at great risk because an attack has shut down heart monitors, potentially during surgery and other procedures.

Table 6 identifies vulnerabilities, impacts, and Practices to consider for attacks against connected medical devices.

Threat Quick Tips	
What to Ask? 	Know your organization’s protocols in case of a potential shutdown or attack against medical devices. Help patients and staff by understanding the processes and procedures; this can help mitigate the impacts. That means asking • How do we notify patients if their medical devices are compromised? • How do patients notify us if they suspect their medical devices are compromised?
When to Ask? 	Knowledge of your organization’s protocols for potential attacks on 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 medical devices.
Who to Ask? 	Each organization should have IT security professionals to help answer any questions on the policy and governance associated with 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 medical devices may need to be engaged to understand vulnerabilities, risks, and appropriate protection and response measures.

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety		
Vulnerabilities	Impact	Practices to Consider
Patches not implemented promptly; includes regular and routine commercial system patches to maintain medical devices Equipment not current, or legacy equipment that is outdated and lacks current functionality Most 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 medical devices that augments the risk of threats compared with managed IT products For medical devices, the cybersecurity profile information is not readily available at health care 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 Heterogeneity of 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	Broad hospital operational impact due to unavailable medical devices and systems Medical devices do not function as required for patient treatment and recovery Patient safety compromised due to breach	Establish and maintain communication with medical device manufacturer's product security teams (9.L.A) Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested (9.M.B) Assess current security controls on networked medical devices (9.M.B, 9.M.E) Assess inventory traits such as IT components that may include the Media Access Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks (9.M.D) Implement pre-procurement security requirements for vendors (9.L.C) Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities (1.L.A) Engage information security as a stakeholder in clinical procurements (9.L.C) Use a template for contract language with medical device manufacturers and others (9.L.C) 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 security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities (9.L.B) Develop and implement network security applications and practices for device networks (9.M.E)

Table 6. Suggested Practices to Combat Attacks Against Medical Devices That May Affect Patient Safety

Cybersecurity Practices

Health care organizations must implement safeguards to mitigate the impact of the threats discussed in the previous section. The breadth and complexity of these threats complicates mitigation. **This is not simply an IT problem.** When threats and vulnerabilities are identified and assessed for potential impact, the most effective combination of safeguards and cybersecurity practices must be determined based on the organization's particular needs, exposures, resources, and capabilities.

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, but are rather meant to be considered as part of an organization's overall cybersecurity program. Further, 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 health care 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, but rather to introduce guidance that will help raise the cybersecurity floor across the health care industry regarding our 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 is described in Appendix E.**

The Practices discussed in the two Technical Volumes align with the outcomes listed in the NIST Framework. The NIST Framework is organized around five steps to manage cyber threats: Identify, Protect, Detect, Respond, and Recover. **The ten Practices in the Technical Volumes help answer the question of “how” to achieve the outcomes identified in the NIST Framework and are tailored to the health sector.**

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 with a 360-degree view of the intersection between cybersecurity and health care. We constantly share practices with federal and private-sector stakeholders and partners, and we are committed to improving the security and resiliency of the health care community.

HHS and its health care industry partners provide valuable information on critical threats related to the health sector. 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 emphasizes transparency and a partnership mentality by collaborating with health sector organizations.** We develop and maintain cybersecurity guidelines, like this publication, that can be used across health care organizations. These partnerships enable HHS to expand its ability to ingest, create, and share threat information, general cybersecurity practices, and mitigation strategies. As data become 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 health care 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 health care 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 health care systems and, ultimately, to providing safe, accurate, and uninterrupted treatment.

“...there must be a culture 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.**

Overview of Technical Volumes

Two technical volumes are provided with this document.

- 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 CSA 405(d) Task Group to mitigate the current threats identified:

1. E-mail 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. Incident response
9. Medical device security
10. Cybersecurity policies

Each Technical Volume presents these ten Practices, followed by a total of 88 Sub-Practices, with implementation recommendations. *Tables 7, 8, and 9* below 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.

Small Organization	
Cybersecurity Practice	Sub-Practice
1— E-mail Protection Systems	1.S.A E-mail System Configuration
	1.S.B Education
	1.S.C Phishing Simulation
2 – Endpoint Protection Systems	2.S.A Basic Endpoint Protection
3 – Access Management	3.S.A Basic Access Management
4 – Data Protection and Loss Prevention	4.S.A Policy
	4.S.B Procedures
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 – Incident Response	8.S.A Incident Response
	8.S.B ISAC/ISAO Participation
9 – Medical Device Security	9.S.A Medical Device Security
10 – Cybersecurity Policies	10.S.A Policies

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

Medium Organization	
Cybersecurity Practice	Sub-Practice
1 – E-mail Protection Systems	1.M.A Basic E-mail Protection Controls
	1.M.B Multifactor Authentication for Remote E-mail Access
	1.M.C E-mail 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 De-Provisioning Procedures
	3.M.C Authentication
	3.M.D Multifactor 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, and Change Management
8 – Incident Response	8.M.A Security Operations Center
	8.M.B Incident Response
	8.M.C Information Sharing/ISACs/ISAOs
9 – Medical Device Security	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 Network Management
10 – Cybersecurity Policies	10.M.A Policies

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

Large Organization	
Cybersecurity Practice	Sub-Practice
1 – E-mail 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 and 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 Remediation Planning
8 – Incident Response	8.L.A Advanced Security Operations Centers
	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 – Medical Device Security	9.L.A Vulnerability Management
	9.L.B Security Operations and Incident Response
	9.L.C Procurement and Security Evaluations
	9.L.D Contacting the FDA
10 – Cybersecurity Policies	N/A

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

Acknowledgements

More than 150 members from the private and public sectors of the U.S. health care industry have participated in the CSA 405(d) Task Group. These members bring experience and knowledge from diverse backgrounds and roles, including cybersecurity, privacy, health care, 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). A list of the current task group members is provided as *Appendix C*. We extend special thanks to the following authors and members of the Writing Committee for their contributions to this document.

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

- **Main Document:** Julie Chua (lead), Daniel Bowden, Allana Cummings, Erik Decker, David Finn, Dale Nordenberg, and Erika Riethmiller
- **Technical Volume 1: Practices for Small Organizations:** Erik Decker (lead), Matthew Barrett, Kendra Siler, and Philip A. Smith, M.D.
- **Technical Volume 2: Practices for Medium and Large Organizations:** Erik Decker (lead), Matthew Barrett, Leonard Levy, Wayne Lee, Mitch Thomas, Stephen Dunkle, and Dale Nordenberg
- **Resources and Templates:** Lee Barret, Erik Decker, and Erika Riethmiller
- **Toolkit:** Erik Decker (lead), Daniel Bowden, William Cai, Emery Csulak, Allana Cummings, Mark Jarrett, M.D., Gabriel Portillo, and Philip A. Smith, M.D.

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; 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.

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

Appendix A: Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
CISO	Chief Information Security Officer
CSA	Cybersecurity Act of 2015
DHS	Department of Homeland Security
EHR	Electronic Health Record
FDA	Food and Drug Administration
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HPH	Health Care and Public Health
IBM	International Business Machines Corporation
ICU	Intensive Care Unit
IP	Intellectual Property or Internet Protocol
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
OCR	Office for Civil Rights
PHI	Personal Health Information
PII	Personal Identifiable Information
RAM	Random Access Memory
URL	Uniform Resource Locator
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network

Appendix B: References

1. “Division N—Cybersecurity Act of 2015” (Pub. L. No. 114-113, Div. N, 129 STAT. 2242, 2015) 1728. <https://www.epic.org/privacy/cybersecurity/Cybersecruity-Act-of-2015.pdf>
2. Ragan, Steve. “Ransomware Takes Hollywood Hospital Offline, \$3.6M Demanded by Attackers.” CSO. Last modified February 14, 2016. <https://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html>.
3. Ragan, Steve. “Ransomware Takes Hollywood Hospital Offline, \$3.6M Demanded by Attackers.” CSO. Last modified February 14, 2016. <https://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html>.
4. 2018 Data Breach Investigations Report. Verizon Enterprise. April 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf.
5. 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB). Ponemon Institute. September 2017. <https://csrps.com/Media/Default/2017%20Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf>.
6. Strauss, Steve. “Cyber Threat is Huge for Small Businesses.” USA Today. Last modified October 20, 2017. <https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/>.
7. Strauss, Steve. “Cyber Threat is Huge for Small Businesses.” USA Today. Last modified October 20, 2017. <https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/>.
8. Landi, Heather. “Healthcare Data Breach Costs Remain Highest at \$408 Per Record.” Healthcare Informatics. Last modified July 13, 2018. <https://www.healthcare-informatics.com/news-item/cybersecurity/healthcare-data-breach-costs-remain-highest-408-record>.
9. Security Intelligence Staff. “IBM X-Force Threat Intelligence Index 2017.” SecurityIntelligence. Last modified March 29, 2017. <https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/>.
10. “Healthcare Breaches Cost \$6.2B Annually.” Becker’s Health IT & CIO Report. Last modified January 19, 2017. <https://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html>
11. Spitzer, Julie. “Montana Hospital Employee’s Email Hacked While Traveling, 8.4K Patients’ Data Stolen.” Becker’s Health IT & CIO Report. Last modified July 17, 2018. <https://www.beckershospitalreview.com/cybersecurity/montana-hospital-employee-s-email-hacked-while-traveling-8-4k-patients-data-stolen.html>
12. Collins, Delano. “How Much Should I Spend on Cyber Security?” EDTs. Last modified January 16, 2016. <https://www.edts.com/edts-blog/how-much-should-i-spend-on-cyber-security>.
13. Kolbasuk McGee, Marianne. “Hospital Diverts Ambulances Due to Ransomware Attack.” Last modified July 11, 2018. <https://www.careersinfosecurity.com/hospital-diverts-ambulances-due-to-ransomware-attack-a-11193>.
14. Donovan, Fred. “Healthcare Data Breach Costs Remain Highest Among Industries.” Health IT Security. Last modified July 12, 2018. <https://healthitsecurity.com/news/healthcare-data-breach-costs-remain-highest-among-industries>.
15. Lopez-Gonzalez, Lorena, Gary T. Pickens, Raynard Washington, and Audrey J. Weiss. *Characteristics of Medicaid and Uninsured Hospitalizations*, 2012. HCUP Statistical Brief #182. Rockville, MD: Agency for

Healthcare Research and Quality, 2014. <https://www.hcup-us.ahrq.gov/reports/statbriefs/sb182-Medicaid-Uninsured-Hospitalizations-2012.pdf>.

16. “[Hacking Responsible for 83% of Breached Healthcare Records in January](#).” HIPAA Journal. Last modified March 1, 2018. <https://www.hipaajournal.com/hacking-responsible-83-breached-healthcare-records-january/>.
17. Snell, Elizabeth. “[How Expensive are Cybersecurity Attacks, Data Breaches?](#)” Health IT Security. Last modified September 20, 2016. <https://healthitsecurity.com/news/how-expensive-are-cybersecurity-attacks-data-breaches>.
18. For an extended description of phishing, see Rose, Scott, Stephen Nightingale, Simson Garfinkel, and Ramaswamy Chandramouli. Trustworthy Email ([NIST Special Publication](#) 800-177 Revision 1, Gaithersburg, MD, 2017). <https://csrc.nist.gov/CSRC/media/Publications/sp/800-177/rev-1/draft/documents/sp800-177r1-draft2.pdf>.