Form Approved
OMB No. 0990-0379
Exp. Date 09/30/2020

Table of Contents

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.

Foreword from Co-Leads

Over the past decade, the threat to the Healthcare 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 healthcare organizations to establish, implement and maintain current and effective cybersecurity practices.

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

Section 405 (d) of CSA also calls for "Aligning Health Care Industry Security Approaches." It is with this imperative that industry and government came together under the auspice of the 405(d) Task Group, starting in May 2017. The Task Group focused on building a set of voluntary, consensus-based principles and best practices to ensure cybersecurity in the Health Sector. The current recommendations of this Task Group are reflected in this document.

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

The U.S. health care sector is comprised of 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 best practices to a health care organization's size and resources — namely, small, medium and large. Each organization has specific cybersecurity-related attributes, strengths and vulnerabilities, and must tailor the recommended cybersecurity best practices for their unique needs to be optimally effective.

Importantly, the Task Group recognized the complexity of cybersecurity threats. There is no simple method to combat all of them. As a result, the Task Group provided a model, discussed in *Appendix F* of this document, which enables an organization to evaluate which best practices will be most effective.

We do not expect the best practices provided in this publication to become a de facto set of requirements that all organizations must implement. The dynamic nature of cybersecurity threats, and the fast pace of technology evolution and adoption, are not managed effectively by a dogmatic approach. Furthermore, these best practices are not intended to aid organizations with the Health Insurance Portability and Accountability Act (HIPAA) or Advancing Care Information compliance 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 National Institute of Standards and Technology (NIST) Cybersecurity Framework (*Appendix E*), introduce Framework terms to start educating health sector professionals on an important and generally-accepted language of cybersecurity, and answer the prevailing question of "How can I adopt certain cybersecurity best practices?"

We hope this document, and its accompanying technical volumes, helps answer that question.

/s/ Erik C. Decker
Industry Co-Lead
Chief Security and Privacy Officer, University of Chicago Medicine
Chairman of the Board, Association for Executives in Healthcare Information Security

/s/ Julie Chua
Government Co-Lead
Risk Management, Office of Information Security
Office of the Chief Information Officer
U.S. Department of Health and Human Services

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, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts. The Task Group convened in May 2017.

We thank all Task Group members who collectively have dedicated thousands of hours of their valuable time and expertise to fulfill the directives of CSA 405(d). A list of the current task force members is provided as *Appendix D*. 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 comprise this publication:

- *Main Document:* Julie Chua (lead), Daniel Bowden, Allana Cummings, Erik Decker, David Finn, Dale Nordenberg, and Erika Riethmiller
- *Technical Volume 1, Best Practices for Small Organizations:* Kendra Siler (lead) and Erik Decker
- *Technical Volume 2, Best Practices for Medium and Large Organizations:* Erik Decker (lead) and Dale Nordenberg
- *Appendices:* Lee Barrett

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

We would like to express gratitude to the Department of Health and Human Services (HHS), the Department of Homeland Security (DHS), and NIST for their collaboration and efforts to establish and support the CSA Section 405(d) Task Group.

Executive Summary

Private healthcare and public health organizations along with the people who rely on their products and services are vulnerable to the impacts of cybersecurity threats. From small, independent practitioners to large, university hospital systems, cyber-attacks on healthcare records, systems, and medical devices have infected the most hardened systems. Like a deadly virus, cyber-attacks on healthcare organizations require mobilization and coordination of resources to mitigate the risks and minimize the impacts. The U.S. Department of Health and Human Services (HHS) and the U.S. Healthcare and Public Health (HPH) Sector are working together to address these challenges.

The Cybersecurity Act became law in 2015. As illustrated in Figure 1, within this legislation is Section 405(d): Aligning Health Care Industry Security Approaches. As an approach to the CSA 405(d) requirement, HHS leveraged the HPH Sector Critical Infrastructure Security and Resilience Partnership to establish the 405(d) Task Group.[1]

The Task Group's initiative was to develop a guidance document that is available to everyone at no cost. It includes a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to achieve three core goals:

- Cost-effectively reduce cybersecurity risks for a range of health care organizations;
- Support the voluntary adoption and implementation of its recommendations; and,
- Ensure, on an ongoing basis, that content is actionable, practical, and relevant to healthcare stakeholders of every size and resource level.

HHS convened the Task Group in May 2017, scheduling working sessions to plan, develop, and write this guidance document. To ensure a successful outcome and a collaborative public-private development process, HHS reached out to 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 and Sector Coordinating Council, the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST).

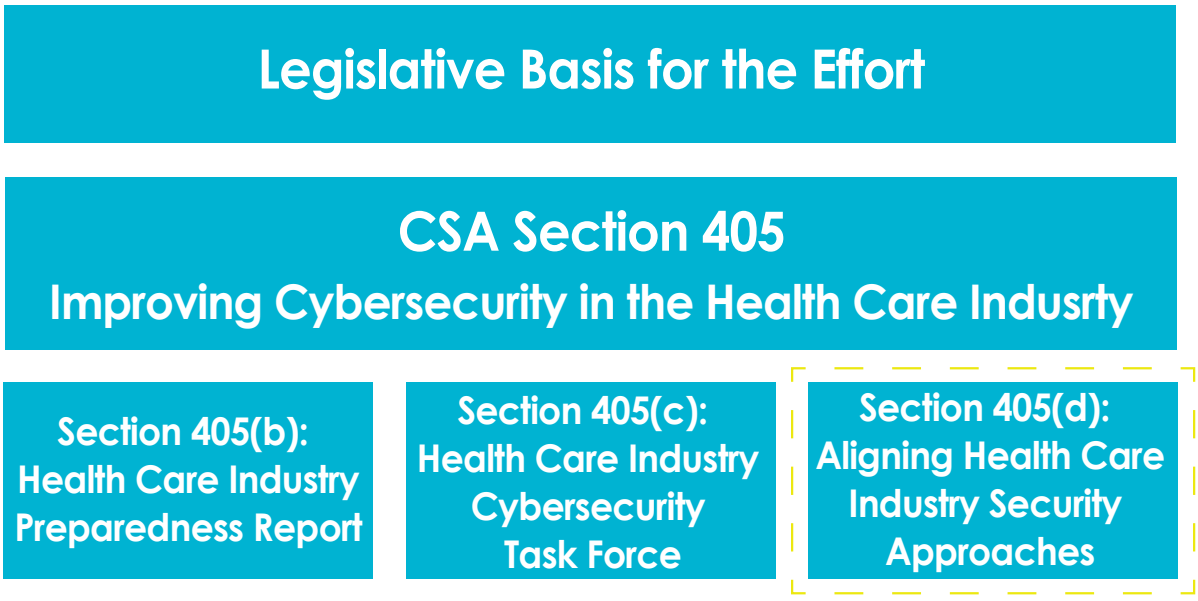


Figure 1. Section 405(d) is Part of the CSA Section 405, Which Focuses on the U.S. Healthcare Industry

Participants included subject matter experts with backgrounds and experience in the following roles:

- Chief Executive Officer (CEO) of a health care organization
- Chief Information Security Officer (CISO) and/or IT security professional
- Chief Information Officer (CIO) and/or Property Management Healthcare
- Chief Risk Officer or other risk manager
- Office of Technology leader or Hospital Administrator
- Chief Information Officer (CIO) and/or Property Management Healthcare
- Doctor, Nurse, and other Healthcare practitioners

The Task Group determined that its initial guidance document should focus on an approach that: 1) examines cybersecurity threats affecting the healthcare and public health sector as a whole; 2) identifies specific weaknesses that make organizations more vulnerable to the threat; and, 3) provides selected best practices that cybersecurity experts rank as the most effective to mitigate the threats.

Recognizing that cybersecurity recommendations are rarely a one-size-fits-all solution, the Task Group compiled best practices specific to health care organizations of varying sizes. To provide practical best practices to small physician practices as well as large university hospital systems, the Task Group created two technical volumes, which are provided as supporting material to this document:

- *Technical Volume 1* discusses cybersecurity best practices for small healthcare organizations
- *Technical Volume 2* discusses cybersecurity best practices for medium and large healthcare organizations

The goal of this publication, which includes this document and the accompanying two technical volumes, is to foster awareness, provide best practices, and move towards consistency within the sector in mitigating the currently most impactful cybersecurity threats. The five threats explored in this document are:

- Email Phishing Attacks
- Ransomware Attacks
- Loss or Theft of Equipment or Data
- Internal, Accidental or Intentional Data Loss
- Attacks Against Connected Medical Devices That May Affect Patient Safety

This publication considers the recommendations made by HHS divisions including, but not limited to, the Assistant Secretary for Preparedness and Response (ASPR), the Centers for Medicare and Medicaid (CMS), Food and Drug Administration (FDA), the Office for Civil Rights (OCR), the Office of the Chief Information Officer (OCIO), the Office of the National Coordinator for Health Information Technology (ONC) as well as guidelines and best practices from DHS and NIST.

Related HHS Cybersecurity Initiatives

Another CSA 2015 legislative requirement was the establishment of a Healthcare Industry Cybersecurity (HCIC) Task Force comprised of top subject matter experts from across industry and government. The Task Force spent one year receiving and reviewing input that came from experts inside and outside the health care industry as well as the general public. Based on this input, the Task Force developed specific recommendations and best practices for a Congressional report that was released on June 2, 2017.

The HCIC Task Force report articulates the urgency and complexity of cybersecurity risks facing the health care industry and calls for a collaborative public and private sector campaign to protect our systems and patients from cyber threats. HHS is working actively to enhance cybersecurity internally and across the Healthcare and Public Health sectors.

There were six (6) imperatives developed by the HCIC Task Force that form the basis of the report:

- Imperative 1 – Define and streamline leadership, governance, and expectations for health care industry cybersecurity
- Imperative 2 – Increase the security and resilience of medical devices and health IT
- Imperative 3 – Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
- Imperative 4 – Increase health care industry readiness through improved cybersecurity awareness and education
- Imperative 5 – Identify mechanisms to protect research and development (R&D) efforts and intellectual property (IP) from attacks or exposure
- Imperative 6 – Improve information sharing of industry threats, risks, and mitigations

HCIC Task Force

The HCIC Task Force report articulates the urgency and complexity of cybersecurity risks facing the healthcare industry. It calls for a collaborative public and private sector campaign to protect our systems and patients from cyber threats.

Each imperative includes a set of recommendations and associated action items for successful implementation.

This publication is consistent with some of the recommendations contained in the Task Force report. It also provides information to instill awareness of the common cybersecurity threats facing the healthcare and public health organizations along with best practices to mitigate those threats. This publication is organized to be regularly updated so that a stakeholder may easily obtain information on the most current cybersecurity threat and best practices.

Cybersecurity in the Healthcare and Public Health Sector

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 a ransom is paid.

Medical professionals help patients identify probable health risks, for example, based on family history medical conditions. They also help patients protect themselves against those risks by making lifestyle changes to avoid those risks and implement a regimen to detect any health conditions that might arise. In addition, medical professionals and patients respond to those conditions with appropriate medical protocols and recover as much of the patient's previous health as possible. Similarly, this document identifies common cybersecurity threats in the health sector and provides best practice recommendations. These best practice recommendations are consistent with the NIST Cybersecurity Framework (NIST Framework), discussed in *Appendix E*. The NIST Framework consists of five concurrent and continuous functions that comprise the cybersecurity lifecycle for any organization: **Identify, Protect, Detect, Respond and Recover.**

In 2016, a bold, new threat arrived on the scene: ransomware. 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. As demonstrated by ransomware attacks that occurred at hospitals in 2016 and 2017, distributed denial of service attacks, and theft of protected health information (PHI), cyber threats are capable of triggering emergencies that impact patient care and public health. Addressing this threat requires a broad, collaborative approach across a multitude of organizations within government and the private sector. HHS is working with a broad coalition of partners to enhance cybersecurity within HHS and across the Healthcare and Public Health Sector. HHS wants to do everything it can to help the sector do what it does best — care for and protect patients. Cybersecurity is a challenge of technology and tactics, which can be addressed largely through increasing training and awareness, transparency, and coordination across the sector.

The healthcare 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 healthcare technology, healthcare organizations have become vulnerable to cyber-attacks on their computer systems and the data contained within. This creates significant risks with potential high-impact consequences for healthcare organizations, their business partners, and, particularly, their patients.

Hackers of all types (nation-state actors, cyber criminals, hacktivists) have found numerous ways to make money from illegally obtained healthcare data. For example, selling this data on the black market to facilitate Medicare fraud and identity theft, or the malicious gathering of foreign intelligence. The financial value of this data has dropped as the black market became saturated with it.

Headlines in the news report major cyber-attacks on healthcare organizations. Below are two stories that were recently reported, with details removed to protect the privacy of those involved:

- *Orthopedics' Data Breach Put Patients Identities at Risk*: A popular orthopedic practice announced its computer system was hacked in multiple counties, putting over a half-million people at risk of identity theft. Victims of the breach included current members of local professional sports teams and former government workers, including FBI agents. This practice is working closely with outside experts as part to perform an ongoing review of its security measures.
- *Entire Hospital Computer System Scrapped due to Cyberattack*: A rural hospital had to replace its entire computer network after a ransomware cyberattack froze the hospital's electronic health record system. Doctors were unable to review their patients' medical history 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 FBI and cybersecurity experts, hospital officials made the difficult decision to replace the entire system.

4 in 5

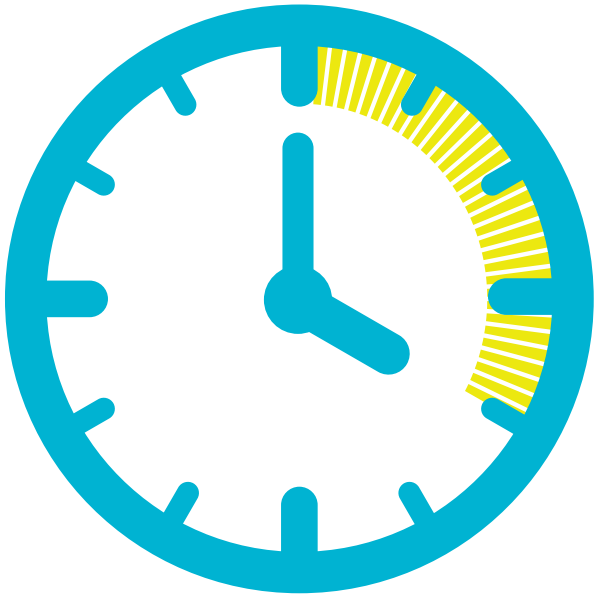
U.S. physicians have experienced some form of a cybersecurity attack

2

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 being something that only happens to large hospital systems? Just imagine for a moment that one of these news reports was about your practice.

64%

of physicians who experienced a cyberattack experienced up to



4 hours

of downtime before they resumed operations

3

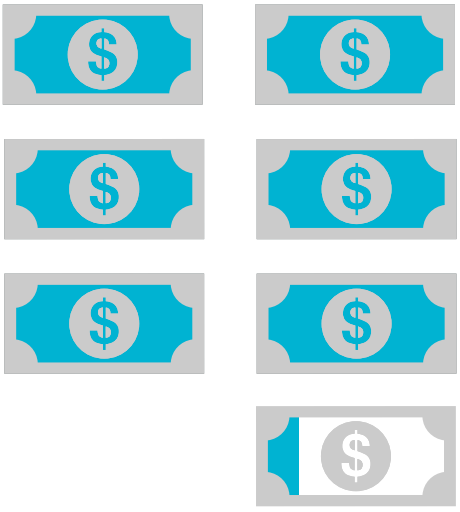
As a Healthcare Professional, Why Should You Worry About Cybersecurity?

Healthcare organizations are committed to providing the very best healthcare to their patients. While the thought of risking patient safety due to a cyberattack is terrifying for any healthcare professional, it can be difficult to justify investments in cybersecurity when there are pressing opportunities to invest in equipment, materials, training and personnel that are more visibly tied to patient care.
Most healthcare 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 the ability of healthcare personnel to provide life-changing and life-saving capabilities. They impede the ability to disseminate patient data appropriately to other healthcare entities, which is a key benefit of digitization. Healthcare organizations require current and resilient cybersecurity that is appropriately compatible across organizations without restricting innovative efforts around population health, precision medicine, and transparency.

Effective cybersecurity is a shared responsibility, involving the people, processes and technologies that protect digital data and technology investments. It is a continual battle as hackers constantly find creative ways to defeat cyber threat defense initiatives. Healthcare data is increasingly transmitted electronically, through mobile devices, cloud-based applications, medical devices and technology infrastructures. Often, these capabilities are deployed without cybersecurity safeguards, making them an appealing target for hackers.

This document provides a foundation of best practices to implement basic cybersecurity in your health care organization. It is written and will be maintained to inform stakeholders in the healthcare community about current cybersecurity threats, what makes these threats effective for hackers, and what best practices can be implemented to thwart them. Cybersecurity incidents impact patient care and may represent a serious threat to patient safety. Failing to address cyber issues can negatively impact an organization's bottom line or result in loss of credibility and patient trust. It is the Task Group's intention to help those who read this guidance document to understand the importance of cybersecurity and to provide the information in a distilled, useable format.



$6.2 billion

lost by U.S. Healthcare System in 2016 due to data breaches

[4]

Can It Happen to Me?

It's tempting for those who own a healthcare practice or are part of a small to medium-sized healthcare organization 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 IBM X-Force Threat Intelligence Index 2017*, a recent study designed to track cybersecurity incidents around the globe, identified the top-targeted cyberattack industries, stating: "It is worth noting that the healthcare 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."

2017 Ponemon Study: Small to Medium Businesses Under Attack

51% of respondents experienced a ransomware attack within the past 3 to 12 months

53% of the 51% had more than one ransomware attack during this period.

79% said the ransomware was through a phishing/ social engineering attack.

The "smaller targets" mentioned in the report may include small or medium-sized organizations. Hackers look for targets that require the least amount of 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 be out there. Whether you are a small practice physician or the Chief Information Security Officer of a large healthcare entity, your job is to make it difficult for these attackers to succeed.

Hand Hygiene for Cybersecurity

Doctors and nurses know that hand sanitizing is critical to prevent the spread of germs. That doesn't mean health care workers wash up as often as they should. Similarly, we know that cybersecurity best practices reduce the risk of cyber-attacks and data breaches. Since we know how to protect our patients from infection, we should be able to protect patient data, allowing physicians and caregivers to trust the data and systems that enable quality healthcare.

Just as healthcare professionals must wash their hands before caring for patients, 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 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 workforce's knowledge of cybersecurity. This will enable you to advance to the next series of best practices, expanding your organization's awareness of and ability to thwart cyber threats.

$2.2 million

is the average cost of a data breach for healthcare organizations

[5]

Common Threat Scenarios Facing the Health Sector

Threat vs. Vulnerability Definitions:

Threat = Danger,
i.e. the flu virus, a hacker

Vulnerability = Weakness;
i.e. No flu shot, shared password

In this section, we introduce common cybersecurity threats and some of the associated vulnerabilities that currently affect the healthcare 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 reason is simple: the first critical issue in cybersecurity is to understand the threats to your organization and the vulnerabilities under attack by those threats. In cybersecurity, threats and vulnerabilities are constantly reviewed. The ability to distinguish between the two helps determine which 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 and authorized individual.

Explaining Threats, Vulnerabilities, Impact and Best Practices

Although threats and vulnerabilities go hand-in-hand, they are often incorrectly interchanged as being the same. 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, and accidental threats. A threat may be a person, including an existing employee, who decides to steal data or do harm to your practice.

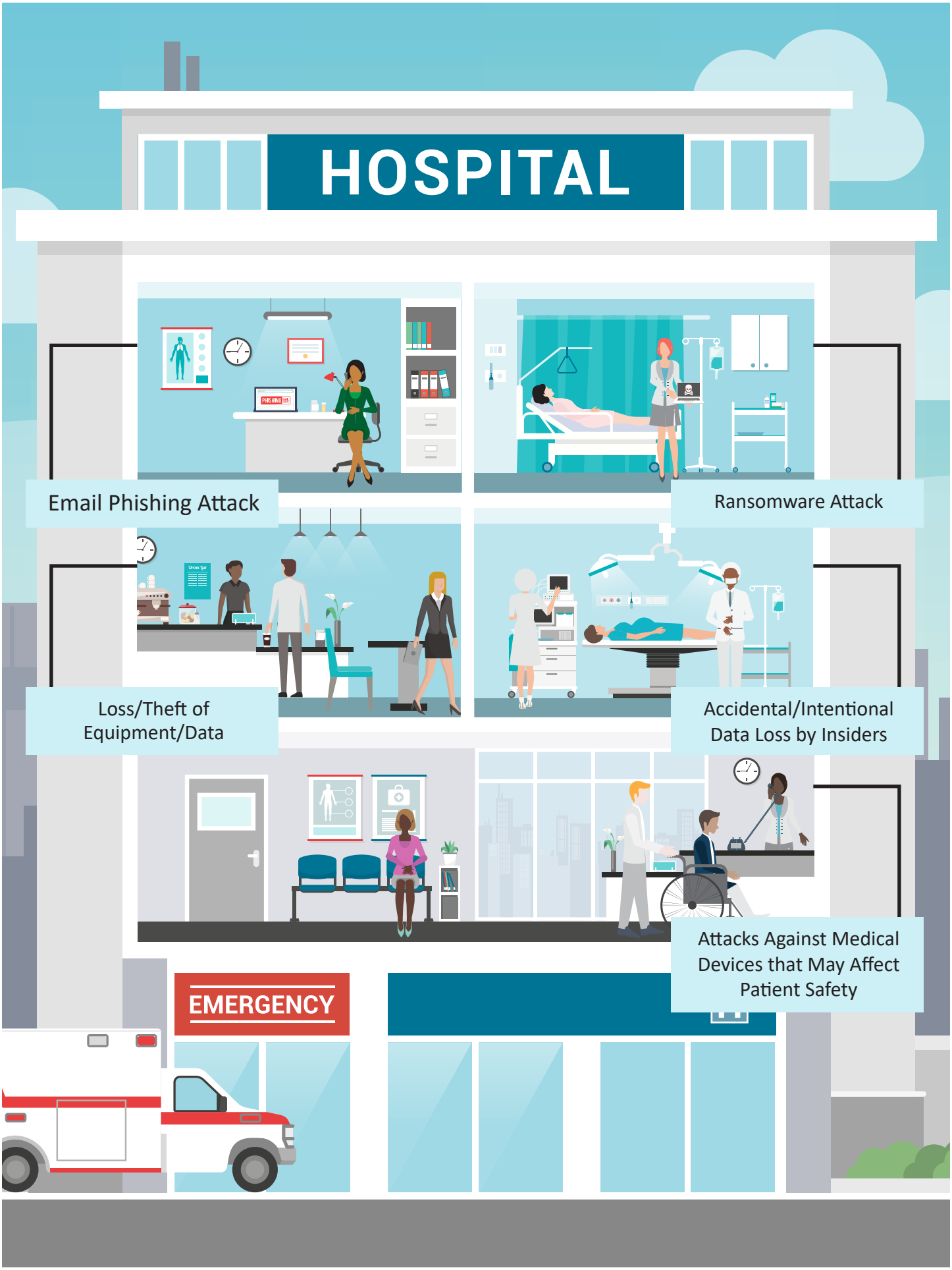
A threat is anything, or anyone, with the potential to harm something of value. Let's take an example that most healthcare practitioners are familiar with: the influenza virus. The flu can infect nearly anyone who is exposed to the virus. The extent of harm caused by the virus depends on that person's 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 an elderly person more vulnerable?

Vulnerabilities are weaknesses that, if exposed to a threat, may result in harm and, ultimately, some form of loss. A vulnerability is often exploited by a threat. Using the above example, most people would assume that an elderly person is more vulnerable than a college athlete to being harmed by the flu. This is due to the diminished function of an aged immune system, reduced physical strength, and, even compromised mental capabilities which 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 the vulnerability to harm of an infected elderly person even further.

A Translation: Threats, Vulnerabilities, Impact and Best 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 healthcare organizations. Just like our flu shot 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	Vulnerabilities	Impact	Best Practices
Influenza	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 Common Threats to the Healthcare and Public Health Sector

This next section describes five of the most common cybersecurity threats to healthcare organizations. Currently, five of the most common cybersecurity threats are:

1. Email Phishing Attack
2. Ransomware Attack
3. Loss/Theft of Equipment/Data
4. Accidental/Intentional Data Loss by Insiders
5. Attacks Against Medical Devices that May Affect Patient Safety

Each of these threats is discussed in the following sections. Vulnerabilities that may determine the impact from the specific threat are listed in a table at the end of each section. We have included best practices for each threat to help you determine effective ways to address your vulnerabilities and mitigate the risk of damage.

Threat: Email Phishing Attack

Description:

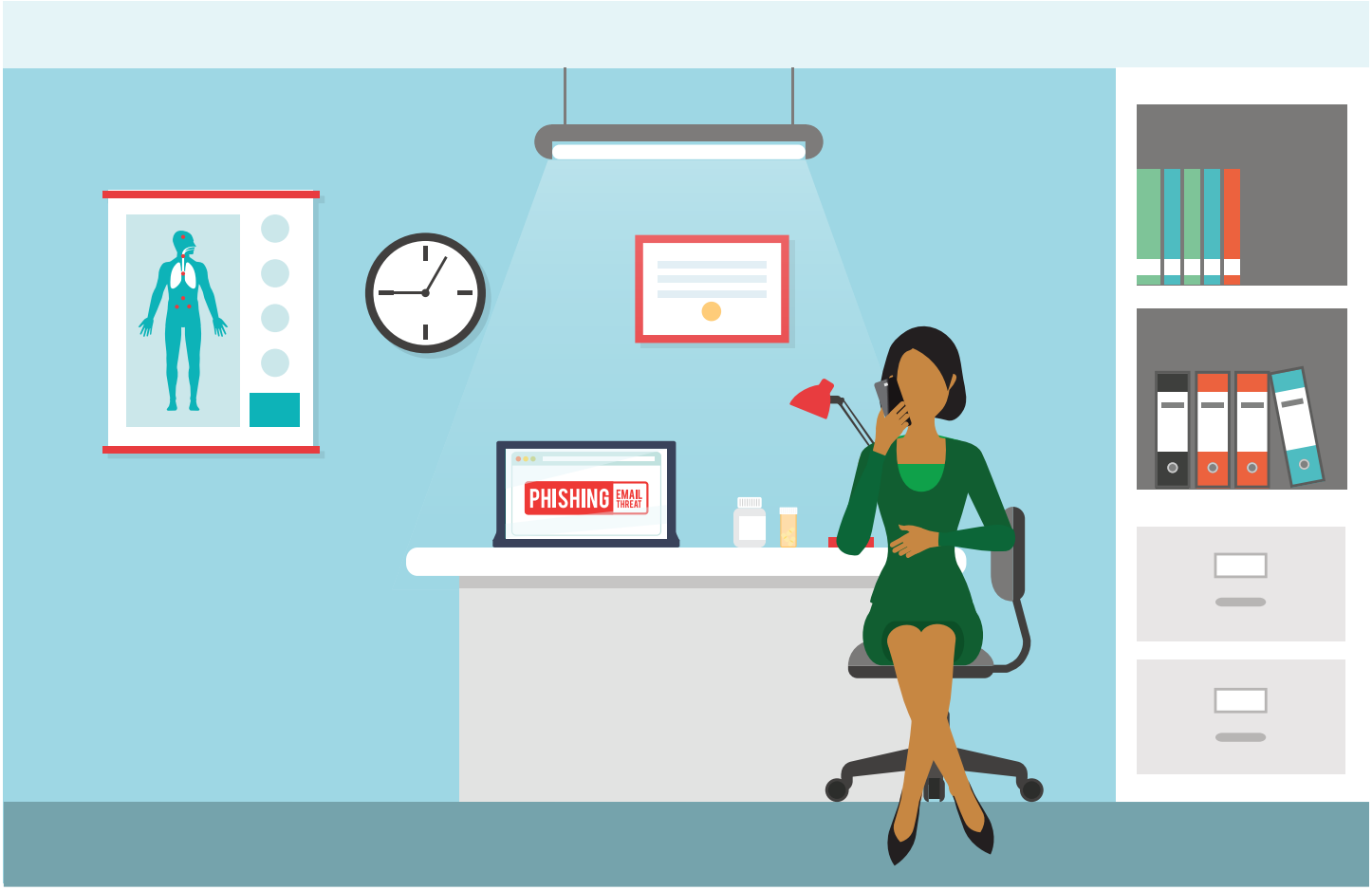
An attempt to trick you, a colleague, or someone else in the workplace into giving out information using email. The inbound email includes an active link or file (often a picture or graphic). The email appears to be sent from a legitimate source, for example, a friend, co-worker, manager, company or even from your own email. Clicking to open the link or file takes the user to a website where sensitive information may be solicited or the site may infect the computer proactively. 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.[6]

Real-World Scenario:

A fraudulent email is received 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 financial and patient data for your organization.

Impact:

A pediatrician learns that patient data was stolen using a phishing attack and used in an identity theft crime.



Vulnerabilities	Impact	Best Practices to Consider
Lack of awareness training. Lack of IT resource for managing suspicious emails. Lack of software scanning emails for malicious content or bad links. Lack of email detection software testing for malicious content. Lack of email sender and domain validation tools.	Loss of reputation in the community (referrals dry up, patients leave the practice). Stolen access credentials being used for access to sensitive data. Erosion of trust or brand reputation. Potential negative impact to the ability to provide timely and quality patient care. Patient safety concerns.	Be suspicious of emails from unknown senders or emails that request sensitive information such as PHI, personal information, or include a call to action that stresses urgency or importance. Train staff to recognize suspicious email and know where to forward them. Never open email attachments from unknown senders. Tag external email to make them recognizable to staff. Allocate dedicated staff and implement procedures to deal with suspicious email. Implement advanced technologies for detecting and testing email for malicious content or links. Implement Multi-Factor Authentication. Implement proven and tested response procedures when employees click on phishing emails. Establish cyber threat information sharing with other healthcare organizations.

Table 1. Suggested Best Practices to Combat Email Phishing Attacks

Threat: Ransomware Attack

Description:

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

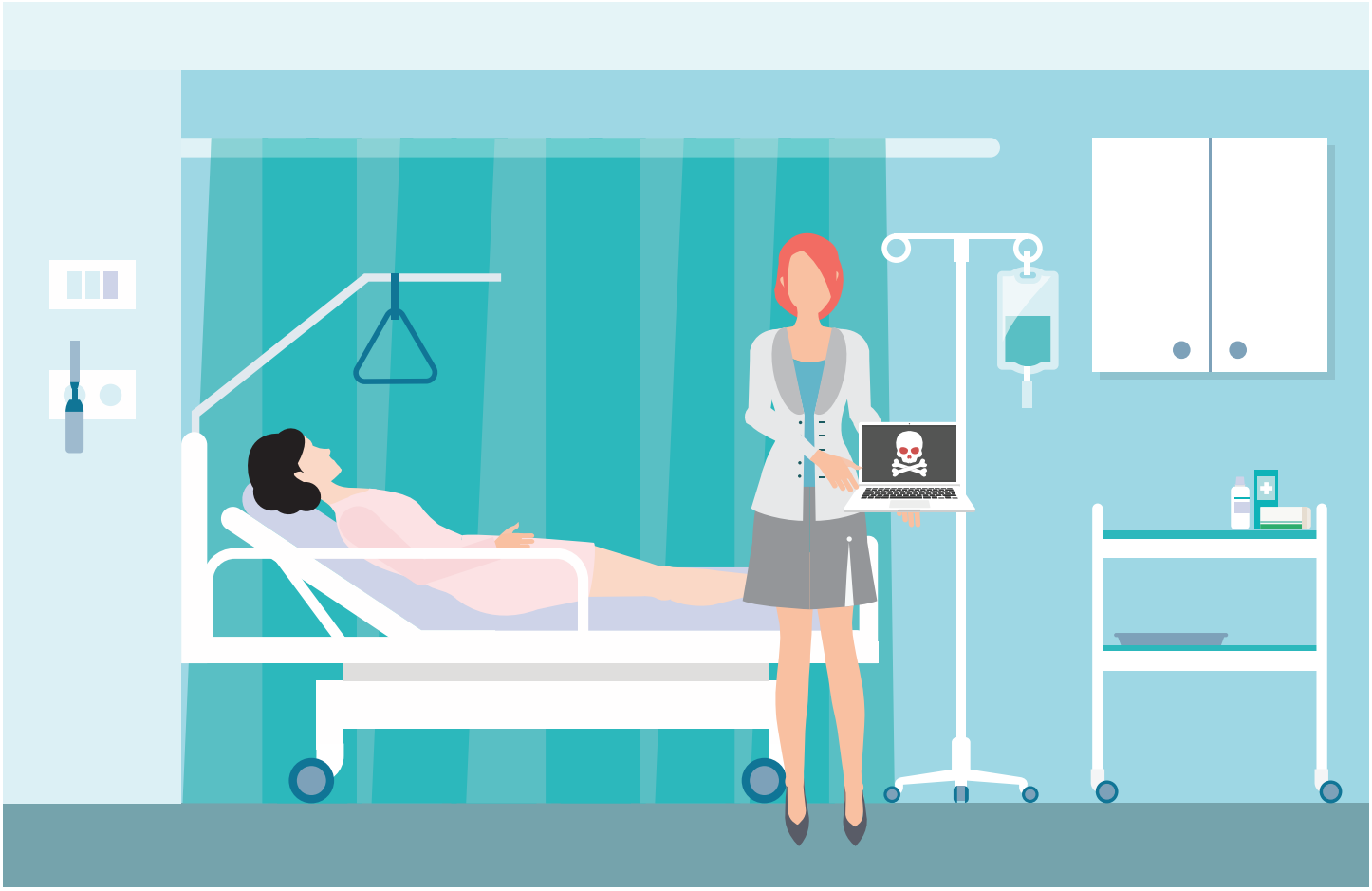
Paying a ransom does not guarantee that the hacker will unencrypt or unlock the data that is stolen and locked. Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats. For example, ransomware may launch from other threats, like phishing.

Real-World Scenario:

Through an email that appears to have originated from a credit card company, a user is directed to a fake website and tricked into clicking on a security update. The security update is a malicious program designed to find and encrypt data, rendering it inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data.

Impact:

A practitioner cannot view the patient charts because of a ransomware attack that has made the Electronic Health Record (EHR) system inaccessible.



Vulnerabilities	Impact	Best Practices to Consider
Lack of system backup. Lack of anti-Phishing capabilities. Unpatched software. Lack of anti-malware detection and remediation tools. Lack of testing and proven data back-up and restoration. Lack of network security controls such as segmentation and access control.	Partial or complete clinical and service disruption. Patient care and safety concerns. Expenses for recovery.	Ensure users understand authorized patching procedures. Update software patching according to authorized procedures. Be clear what computers may access and store sensitive or patient data. Use strong/unique username and passwords with multi-factor authentication. Limit users who can log in from remote desktop. Implement an account lockout policy to thwart brute force attacks by setting a maximum number of failed attempts. Deploy anti-malware detection and remediation tools. Separate critical or vulnerable systems away from threats. Maintain a complete and updated inventory of assets. Implement a proven and tested data back-up and restoration test. Secure backups and ensure backups are not connected permanently to the computers and networks they are backing up. Implement proven and tested business continuity plans and downtime procedures. Implement proven and tested incident response procedures. Establish cyber threat information sharing with other healthcare organizations. Develop a ransomware recovery playbook and test it regularly.

Table 2. Suggested Best Practices to Combat Ransomware Attacks[7]

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 a hacker. Theft of equipment and data is an ever present and on-going threat for all organizations. While the value of the device is one loss, far greater are the consequences of losing a device that contains accessible data, especially sensitive data. In cases where the lost device wasn't appropriately safeguarded or password protected, losing the device may result in unauthorized access, dissemination and illegal use of sensitive data. Even if the device is recovered, the data may have been erased and completely lost. This loss or malicious use of data may result in a business disruption, and compromised patient safety concerns with the organization required to notify patients, applicable regulatory agencies and/or the media of the event.

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 made it to the dark web for sale.

Vulnerabilities	Impact	Best Practices to Consider
Lack of asset inventory and control. Lack of encryption. Data at rest is data stored on a hard drive at any location. Lack of physical security practices. Open offices and poor physical access management give attackers opportunities. Lack of simple safeguards such as computer cable locks to secure devices within office environments. Lack of awareness that theft of IT assets from the office accounts for nearly as much as from cars. Lack of effective vendor security management, including controls to protect equipment or data sensitive data. Lack of "End-of-Service" process to clear sensitive data before medical devices are discarded or transferred to other users or other organizations.	Inappropriate access to or loss of sensitive patient information occurs. This may involve proprietary or confidential company information or intellectual property. Theft or loss of unencrypted PHI or personally identifiable information (PII) may result in a data breach requiring notification to affected patients, relevant regulatory bodies and the media. Lost productivity occurs. Damage to reputation occurs.	Encrypt sensitive data, especially when transmitting data to other devices or organizations. Implement proven and tested data backups, with proven and tested restoration of data. Implement proven and tested business continuity plans, and downtime procedures when data backups aren't available or can't be restored in a timely manner. Acquire and use Data Loss Prevention Tools. Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices. Promptly report loss/theft to designated company individuals to terminate access to the device and/or network. 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. Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device. Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished or resold.

Table 3. Suggested Best Practices to Combat Loss or Theft of Equipment or Data[8]

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: 1) accidental and 2) intentional.

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

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

Real-World Scenario:

A staff member of a physical therapy center is contacted by an imposter of the hospital staff, in need of verifying patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.

Impact:

The patient's personal health information was compromised and used in an identity theft case.

Vulnerabilities	Impact	Best Practices to Consider
Files containing sensitive data are accidentally emailed to incorrect or unauthorized addressees. Lack of adequate monitoring, tracking and auditing of access to patient information on the electronic medical record (EMR). Lack of adequate logging and auditing of access to critical technology assets, such as email and file storage. Lack of technical controls to monitor the emailing 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 email and unencrypted mobile storage results in reportable data breaches. Reportable incidents occur involving patients who are victims of employees who inappropriately view patient information. Financial loss occurs from insiders being social engineered into not following proper procedures. Financial loss occurs due to an employee inadvertently giving an attacker access to banking and routing numbers because the attacker used a phishing email disguised as the practice bank. Patients are given the wrong medicines because of an accidental deletion of data in the EMR.	Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors. Implement and use of workforce access auditing to health record system and sensitive data. Implement and use Privileged Access Management Tools for reporting access to critical technology infrastructure and systems. Implement and use Data Loss Prevention Tools to detect and block leakage of PHI and PII via email and web uploads. Institute a policy of third-party assurance certification for vendors.

Table 4. Best Practices are Suggested to Combat Insider, Accidental or Intentional Loss of Data

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

Description:

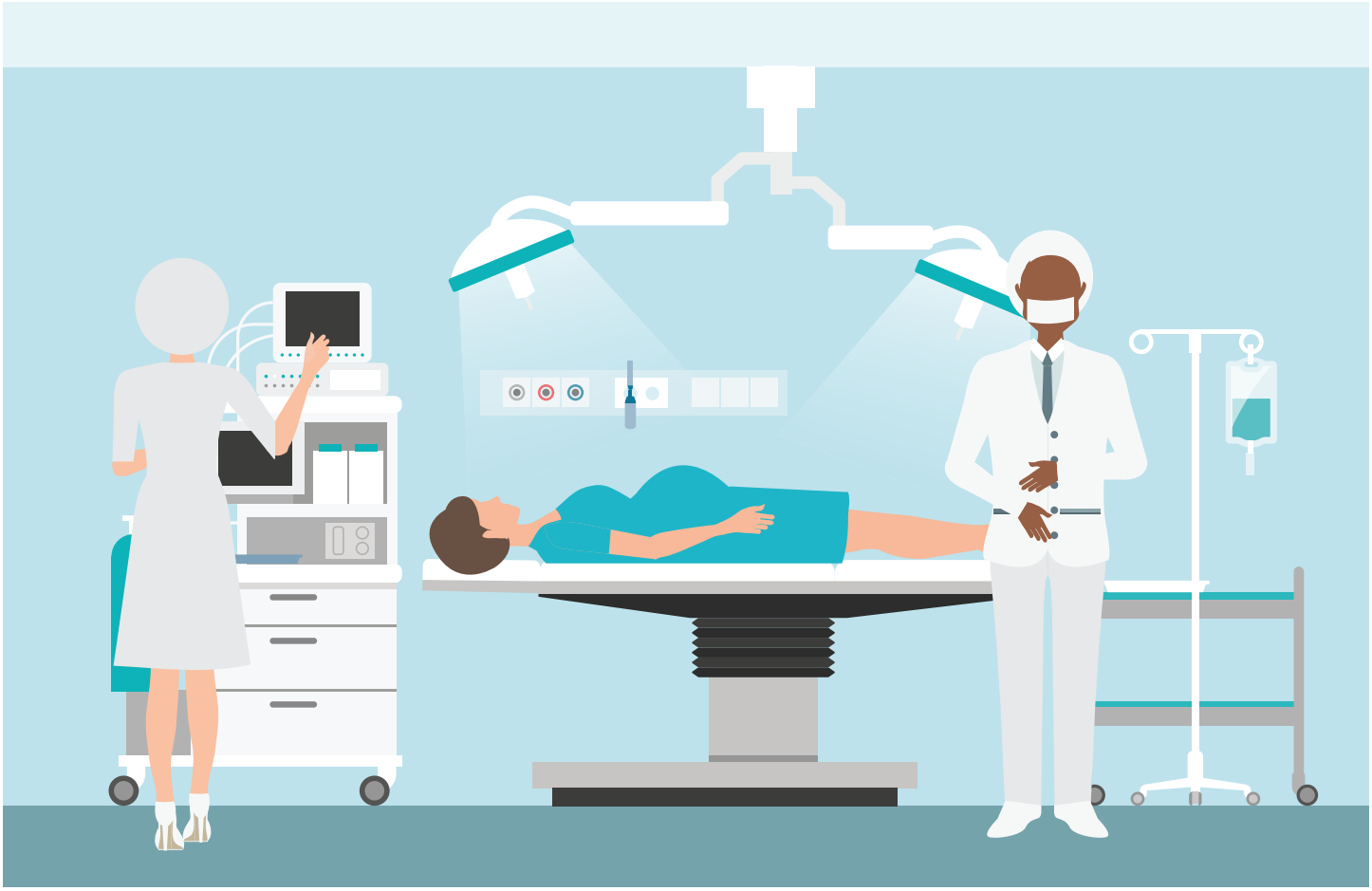
The FDA defines a medical device as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement 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 email 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.



Vulnerabilities	Impact	Best Practices to Consider
Patches are not implemented promptly. This includes regular and routine commercial system patches to maintain medical devices. Equipment is not current or legacy equipment is in use that is outdated and lacks current functionality. Most medical devices, unlike IT equipment, cannot be monitored by an organizations Intrusion Detection System. The safety of patients and protection of data integrity is dependent on identifying and understanding the threats and threat scenarios. However, it's the challenge of identifying and addressing vulnerabilities in medical devices that augments the risk of threats compared to managed IT products. For medical devices, the cyber security profile information is not readily available at healthcare organizations, making cyber security optimization more challenging. This may translate into missed opportunities to identify and address vulnerabilities, increasing the likelihood for threats to result in adverse impacts. The heterogeneity of medical devices means that the vulnerability identification and remediation process is complex and resource intensive. This increases the likelihood that devices will not be assessed or patched, leading to missed opportunities to close vulnerabilities.	Broad hospital operational impact occurs due to unavailable medical devices and systems. Medical devices do not function as required for patient treatment and recovery. Patient safety is compromised due to breach.	Establish and maintain communication with Medical Device manufacturer's product security teams. Patch devices after the patch has been validated, distributed by the medical device manufacturer and properly tested. Assess current security controls on networked medical devices. Assess inventory traits such as information technology components that may include the MAC address, IP address, network segments, operating systems, applications and other elements relevant to managing information security risks. Implement pre-procurement security requirements for vendors. Engage information security as a stakeholder in clinical procurements. Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities. Utilize a template for contract language to use with medical device manufacturers and others. Implement access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, two factor authentication, minimum necessary or least privilege. Implement security operations practices for devices which includes hardening, patching, monitoring and threat detection capabilities. Develop and implement network security applications and practices for device networks. Institute a policy of third-party assurance certification for vendors.

Table 5. Suggested Best Practices to Combat Attacks Against Medical Devices

Introduction to Cybersecurity Best Practices

Healthcare organizations must implement safeguards to mitigate the impact of the threats discussed in the previous section. The broad and complex spectrum 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 best practices must be determined based on the organization's particular needs, exposures, resources and capabilities. As presented in *Technical Volumes 1 and 2*, best practices will range from training and awareness of personnel 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 best 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, best practices, and appropriate references across organizations to improve cybersecurity competencies; and,
- Enabling organizations to prioritize actions and investments — know what to ask — to improve cybersecurity.

This guidance document, and the accompanying technical volumes, is intended to be descriptive, rather than prescriptive. There are best practices that can be reviewed for applicability within your organization to reduce the potential impacts of the five common threats discussed in the previous section. These best practices are voluntary guidance to raise the level of cybersecurity across health care organizations. They may be implemented in whole or in part. A method to assess and prioritize which best practices to implement is described later in *Appendix F*.

The intent of these best practices is not to introduce a new framework, new methodology, or new regulatory requirement into the cybersecurity space, but rather to introduce voluntary guidance that will help raise the floor across the health sector in our defensive and responsive cybersecurity practices.

The best practices discussed in the two technical volumes are aligned with the outcomes listed in the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (Framework). The NIST Framework is organized around five steps to manage cyber threats: Identify, Protect, Detect, Respond and Recover. The best 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 care sector.

Where Do I Fit?

The process to implement cybersecurity best practices will be impacted by an organization's 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 facilitate this understanding, the implementation practices are segmented by small, medium and large organization.

Selecting the correct organization size to choose can be more complicated than it seems. It may be crystal clear, for example, if you are a small practice with 1-2 providers and no affiliations or exchanges with other care systems. This configuration is not as common as it used to be. 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 6* provides guidance in deciding which size tier is your "best fit."

		Small Tier	Medium Tier	Large Tier
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 on a break/fix or project by project basis.	Dedicated IT resources are on staff. None or limited dedicated security resources on staff.	Dedicated IT resources with dedicated budget. CISO or dedicated security leader with dedicated security staff.
	Cybersecurity Investment	Non-existent or limited funding.	Funding allocated for specific initiatives. Potentially limited future funding allocations. Cybersecurity budgets are blended with IT.	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)[9]	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 ACO 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 6. Selecting the "Best Fit" For Your Organization

The best practices discussed in the two technical volumes are written to be consistent with the organization you identify with the most. For *Technical Volume 1: Cybersecurity Best Practices for Small Healthcare Organizations*, the best practices are written in a manner that is intended to be self-contained specifically for small organizations.

For *Technical Volume 2: Cybersecurity Best Practices for Medium and Large Organizations*, the best practices are written differently. For each best practice, a series of *Baseline Practices* and *Advanced Practices* are provided. Medium organizations are advised to start with the *Baseline Practices*. Large organizations are advised to review *Baseline Practices* and *Advanced Practices*. Medium organizations are encouraged to adopt *Advanced Practices* as applicable to their particular 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. Best practices in tiers other than your identified "best fit" may be considered as part of your cybersecurity strategy.

Overview of Technical Volumes

Two Technical Volumes are provided with this document.

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

The Technical Volumes are organized according to the following ten most effective cybersecurity best practices selected by the 405(d) Task Group to mitigate common threats:

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. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Each Technical Volume presents these ten best practices, followed by a series of 88 sub-practices, identified in *Tables 7, 8 and 9*, with implementation recommendations. 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 is provided as *Appendix F: Best Practices Assessment and Roadmap*. This methodology offers guidance to select and prioritize the sub-practices that are most relevant to you.

Small Organization		
Best Practice	**Sub Practice**	**Baseline Practice**
1	1.A	Email System Configuration
1	1.B	Education
1	1.C	Phishing Simulation
2	2.A	Basic Endpoint Protection
3	3.A	Basic Access Management
4	4.A	Policy
4	4.B	Procedures
5	5.A	Inventory
5	5.B	Procurement
5	5.C	Decommissioning
6	6.A	Network Segmentation
6	6.B	Physical Security and Guest Access
6	6.C	Intrusion Prevention
7	7.A	Vulnerability Management
8	8.A	Incident Response
8	8.B	ISAC/ISAO Participation
9	9.A	Medical Device Security
10	10.A	Policies

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

Medium Organization		
Best Practice	**Sub Practice**	**Baseline Practice**
1	1.A	Basic Email Protection Controls
1	1.B	Multifactor Authentication for Remote Email Access
1	1.C	Email Encryption
1	1.D	Workforce Education
2	2.A	Basic Endpoint Protection Controls
3	3.A	Identity
3	3.B	Provisioning, Transfers and De-Provisioning Procedures
3	3.C	Authentication
3	3.D	Multi-Factor Authentication (MFA) for Remote Access
4	4.A	Classification of Data
4	4.B	Data Use Procedures
4	4.C	Data Security
4	4.D	Backup Strategies
4	4.E	Data Loss Prevention
5	5.A	Inventory of Endpoints and Servers
5	5.B	Procurement
5	5.C	Secure Storage for Inactive Devices
5	5.D	Decommissioning Assets
6	6.A	Network Profiles and Firewalls
6	6.B	Network Segmentation
6	6.C	Intrusion Prevention Systems
6	6.D	Web Proxy Protection
6	6.E	Physical Security of Network Devices
7	7.A	Host/Server Based Scanning
7	7.B	Web Application Scanning
7	7.C	System Placement and Data Classification
7	7.D	Patch Management, Configuration Management, and Change Management
8	8.A	Security Operations Center
8	8.B	Incident Response
8	8.C	Information Sharing/ISACs
9	9.A	Framework for Management
9	9.B	Endpoint Protections
9	9.C	Identity and Access Management
9	9.D	Asset Management
9	9.E	Network Management
10	10	Policies

Table 8. Best Practices and Sub-Practices for Medium Organizations

Large Organization		
Best Practice	**Sub Practice**	**Advanced Practice**
1	1.A	Advanced and Next Generation Tooling
1	1.B	Digital Signatures
1	1.C	Analytics Driven Education
2	2.A	Automate the Provisioning of Endpoints
2	2.B	Mobile Device Management
2	2.C	Host Based Intrusion Detection/Prevention Systems
2	2.D	Endpoint Detection and Response
2	2.E	Application Whitelisting
2	2.F	Micro-segmentation/Virtualization Strategies
3	3.A	Federated Identity Management
3	3.B	Authorization
3	3.C	Access Governance
3	3.D	Single-Sign On
4	4.A	Advanced Data Loss Prevention
4	4.B	Mapping of Data Flows
5	5.A	Asset Pre-Configuration
5	5.B	Automated Discovery and Maintenance
5	5.C	Integration with Network Access Control
6	6.A	Additional Network Segmentation
6	6.B	Command and Control Monitoring of Perimeter
6	6.C	Anomalous Network Monitoring and Analytics
6	6.D	Network Based Sandboxing / Malware Execution
6	6.E	Network Access Control
7	7.A	Remediation Planning
8	8.A	Advanced Security Operations Centers
8	8.B	Advanced Information Sharing
8	8.C	Incident Response Orchestration
8	8.D	Baseline Network Traffic
8	8.E	User Behavior Analytics
8	8.F	Deception Technologies
9	9.A	Vulnerability Management
9	9.B	Security Operations and Incident Response
9	9.C	Procurement
9	9.D	Contacting the FDA
10	10	Policies

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

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 healthcare. We constantly share best practices with federal and private sector stakeholders 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. 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 HPH Sector organizations. We develop and maintain cybersecurity guidelines, such as 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 best 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 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 healthcare professional from data entry specialists to physicians to board members. Importantly, patients 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, of providing safe, accurate and uninterrupted treatment.

Paradigm Shift:

To adequately protect patient safety and our sector's information and data, there must be a culture change, a paradigm shift to the **importance and necessity of cybersecurity as an integrated part of patient care.**

The changes and effort will not abate but rather change with the times, technologies, threats and events. Now is the time to start and, together, we can achieve real results.

Appendix A: Glossary of Terms

Definitions from Division N, Title 1, Section 102 of the Cybersecurity Information Act of 2015[10]

Cybersecurity threat - An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term ``cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber threat indicator - Information that is necessary to describe or identify: malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- any combination thereof.

Defensive measure - An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term ``defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by:

- the private entity operating the measure; or
- another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

Federal entity - A department or agency of the United States or any component of such department or agency.

Information system - Has the meaning given the term in section 3502 of title 44, United States Code; and includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

Local government - Any borough, city, county, parish, town, township, village, or other political subdivision of a State.

Malicious cyber command and control - A method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

Malicious reconnaissance - A method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

Monitor - To acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

Non-federal entity - Any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof). The term ``non-Federal entity'' includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States. The term ``non-Federal entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Private entity - Any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof. The term ``private entity'' includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services. The term ``private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Security control - The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security vulnerability - Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Tribal - The term ``tribal'' has the meaning given the term ``Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

Other Terms

Asset - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. *Source(s): CNSSI 4009-2015*

Breach - A breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident." OMB M-18-02 and subsequent OMB Guidance: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. *Source: Department of Homeland Security DHS Directives System Instruction Number: 047-01-006 Revision Number: 00 Issue Date: DECEMBER 4, 2017*

Business Continuity Plan – The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. *Source(s): NIST SP 800-34 Rev. 1; CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)*

Capacity Planning - Systematic determination of resource requirements for the projected output, over a specific period. *Source(s): businessdictionary.com*

Category - The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes." *Source(s): NIST Cybersecurity Framework*

Controls (Also see Security Controls) - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. *Source(s): FIPS 200 (FIPS 199); FIPS 199; CNSSI 4009-2015 (FIPS 199); NIST SP 800-128 (FIPS 199); NIST SP 800-137 (FIPS 199); NIST SP 800-18 Rev. 1 (FIPS 199); NIST SP 800-34 Rev. 1 (FIPS 199); NIST SP 800-37 Rev. 1 (FIPS 199); NIST SP 800-39 (FIPS 199, CNSSI 4009); NIST SP 800-60 Vol 1 Rev. 1 (FIPS 199); NIST SP 800-30 (FIPS 199, CNSSI 4009); NIST SP 800-82 Rev. 2 (FIPS 199)*

Critical Infrastructure - Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. *Source(s): PPD-21*

Cybersecurity - The process of protecting information by preventing, detecting, and responding to attacks. *Source(s): NIST Framework*

Defense-in-depth - Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. *Source(s): CNSSI 4009-2015 (NIST SP 800-53 Rev. 4); NIST SP 800-39 (CNSSI 4009); NIST SP 800-53 Rev. 4; NIST SP 800-30 (CNSSI 4009)*

Denial of Service Attack (DOS) - Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed. *Source(s): NIST SP 800-24*

Disaster Recovery – A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. *Source: SP 800-34*. Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan. *Source: CNSSI-4009*

Disaster Recovery Plan (DRP) – A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. *Source(s): NIST SP 800-34 Rev. 1; CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)*

Endpoint Protection Platform (or End-Point Protection Platform) - Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.). *Source(s): NIST SP 800-128*

Event - Any observable occurrence on a system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). *Source: NIST Framework*

Firmware - Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. *Source(s): Techterms.com*

Framework - A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework." *Source(s): NIST Framework*

Incident - An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. *Source(s): NIST Framework*

Internet of Things (IoT) – In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems. *Source: Strategic Principles for Securing the Internet of Things DHS: November 15, 2016*

Mobile Device - A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device. *Source(s): CNSSI 4009-2015 (Adapted from NIST SP 800-53 Rev. 4)*

Network Access - Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). *Source(s): NIST SP 800-53 Rev. 4*

Overlay - A fully specified set of security controls, control enhancements, and supplemental guidance derived from tailoring a security baseline to fit the user's specific environment and mission. *Source(s): NIST SP 800-53 Rev. 4*

Port - The entry or exit point from a computer for connecting communications or peripheral devices. *Source(s): NIST SP 800-82*

Profile - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. *Source(s): NIST Framework*

- Target Profile - the desired outcome or 'to be' state of cybersecurity implementation
- Current Profile - the 'as is' state of system cybersecurity

Protocol - A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. *Source(s): NIST SP 800-82*

Remote Access - Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). *Source(s): NIST SP 800-53*

Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. *Source(s): NIST SP 800-82*

Risk Management - The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. *Source(s): FIPS 200*

Risk Tolerance - The level of risk that the organization is willing to accept in pursuit of strategic goals and objectives. *Source(s): NIST SP 800-53*

Router - A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. *Source(s): NIST SP 800-82*

Security Control - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. *Source(s): NIST SP 800-82*

Supporting Services - Providers of external system services to the organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. *Source(s): NIST SP 800-53*

Switch - A network device that filters and forwards packets between LAN segments. *Source(s): NIST SP 800-47*

Third-Party Relationships - Relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties. *Source(s): DHS*

Third-party Providers - Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. *Source: NIST Special Publication 800-53 (Rev. 4)*

Threat - A possible danger to a computer system. *Source(s): NIST SP 800-28 Version 2*

Thresholds - A value that sets the limit between normal and abnormal behavior. *Source(s): NIST SP 800-94*

Vulnerability - A security weakness in a computer. *Source(s): NIST SP 800-114*

Appendix B: Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
AHIP	America's Health Insurance Plans
ASL	Assistant Secretary for Legislation
ASPR	Assistant Secretary for Preparedness and Response
BYOD	Bring Your Own Device
CEO	Chief Executive Officer
CHIO	Chief Health Information Officer
CHIP	Children's Health Insurance Program
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Security Systems Professional
CMS	Centers for Medicare and Medicaid
CNSSI	Committee on National Security Systems Instruction
COO	Chief Operations Officer
CSA	Cybersecurity Act of 2015
DHS	Department of Homeland Security
DoD	Department of Defense
DOS	Denial of Service
DRP	Disaster Recovery Plan
DSM	Direct Secure Messaging
EHR	Electronic Health Record
EMR	Electronic Medical Record
EPHI	Electronic Private Health Information
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standards
HCIC	Health Care Industry Cybersecurity
HHS	Department of Health and Human Services
HIMSS	Health Information Management and Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HIT	Health Information Technology
HITECH	Health Information Technology Economic and Clinical Health Act
HMO	Health Maintenance Organization
HPH	Healthcare and Public Health
HRSA	Health Resources and Services Administration
IA	Information Assurance
IBM	International Business Machines
ICU	Intensive Care Unit

Acronym/ Abbreviation	Definition
INFOSEC	Information Security
IoT	Internet of Things
IP	Intellectual Property or Internet Protocol
IPS	Internet Partner Services
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
ITAM	Information Technology Asset Management
LAN	Local Area Network
LLC	Limited Liability Corporation
MAC	Media Access Control
MACRA	Medicare access and the Children's Health Insurance Program Reauthorization Act
MFA	Multi-Factor Authentication
NCCIC	National Cybersecurity and Communications Integration Center
NH-ISAC	National Healthcare – Information Sharing and Analysis Centers
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCIO	Office of the Chief Information Officer
OCR	Office for Civil Rights
ONC	Office of the National Coordinator (for Healthcare Technology)
PACS	Pictures Archiving and Communication Systems
PCI-DSS	Payment Card Industry Data Security Standard
PHI	Personal Health Information
PII	Personal Identifiable Information
ROM	Read Only Memory
SAMHSA	Substance Abuse and Mental Health Services Administration
SOC/IR	Security Operations Center / Incident Response
SSN	Social Security Number
SVP	Senior Vice President
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
VP	Vice President
VPN	Virtual Private Network

Appendix C: CSA Steering Committee Members

Last Name	First Name	Organization
Barrett	Matthew	NIST
Bollerer	Chris	HHS/OCIO/OIS
Bradsher	Kris	HHS/ASL
Csulak	Emery	HHS/CMS
Cummings	Stacy	DoD Program Office
Curren	Stephen	HHS/ASPR
Dar	Cristina	HHS/FDA
MacGabhann	Lucy	HHS/OGC
Hall	Bill	HHS/ASPA
Heesters	Nick	HHS/OCR
Jackson	Helen	DHS
Lawrence	Courtney	HHS ASL
Lemott	Sonja	DoD Program Office
Maimone	Christian	HHS/OGC
Mosely-Day	Serena	HHS/OCR
Niemczak	Stephen	HHS/OIG
Nsahlai	Rose-Marie	HHS/ONC
O'Connor	Kerry	DHS
Ross	Aftin	HHS/FDA
Schwartz	Suzanne	HHS/FDA
Todd	Nickol	HHS/ASPR
Vantrease	Scott	HHS/OIG
Wolf	Laura	HHS/ASPR

Appendix D: Task Group Membership

Last Name	First Name	Title	Organization
Adams	Kenneth	Director, Federal Advisory	KPMG
Alicea	Michael	Chief Information Officer (CIO)	Synergy Healthcare Services, LLC
Alvarez	Bayardo	Director, Information Technology (IT)	Boston PainCare Center
Anastasiou	Peter	Director, Security Strategy	Tufts Health Plan
Anderson	Carl	Vice President (VP)	HITRUST
Barrera	Connie	Director, Information Assurance (IA) and Chief Information Security Officer (CISO)	Jackson Health System
Barrett	Lee	Executive Director	Electronic Healthcare Network (EHNAC)
Barrett	Matthew	Cybersecurity Framework Lead	NIST
Becknel	Damon	CISO	Horizon Blue Cross Blue Shield of New Jersey
Belfi	Catherine	Manager – Emergency Management and Enterprise Resilience	New York University Langone Medical Center
Blanchette	Karen	Executive Director	PAHCOM
Blass	Gerard	President and Chief Executive Officer (CEO)	ComplyAssistant
Bollerer	Chris	Supervisory IT Specialist	HHS/OIS
Bontsas	Jeff	VP and CISO	Ascension Information Services
Bowden	Daniel	CISO	Sentara Healthcare
Branch	Robert	Director, Information Systems and Technology	Munroe Regional Medical Center
Carr	Joseph	CIO	New Jersey Hospital Association
Castillo	Janella	Junior Information Security Analyst	HITRUST
Chaput	Robert	CEO	Clearwater Compliance LLC
Chua	Julie	HHS Security Risk Management Division Manager	HHS/OCIO/OIS
Cline	Bryan	VP, Standards and Analytics	HITRUST
Cofran	Wendy	CIO	Natick VNA/Century Health Systems
Coughlin	Jeff	Senior Director, Federal and State Affairs	HIMSS
Coyne	Andrew	CISO	Mayo Clinic
Csulak	Emery	CISO	HHS/CMS

Last Name	First Name	Title	Organization
Cullen	Mike	Senior Manager, Cybersecurity and Privacy	Baker Tilly
Cummings	Allana	CIO	Children's Healthcare of Atlanta
Curran	Sean	Senior Director	West Monroe Partners
Curren	Stephen	Director, Division of Resilience	HHS/ASPR
Curtiss	Rich	CISO	Clearwater Compliance LLC
Dar	Cristina	Research Officer	HHS/FDA
Davis	Cynthia	CHIO	Methodist Le Bonheur Healthcare
Decker	Erik	Chief Security and Privacy Officer	University of Chicago Medicine
Donat	Terry	Surgeon and Illinois Professional Emergency Manager	CGH Medical Center
Dunkle	Stephen	CISO	Geisinger Health
Durbin	Kenneth	Strategist, Certified Information Systems Security Professional (CISSP)	Symantec
Echols	Mike	CEO	IACI - International Association of ISAOs
Edmonson	Vladimir	Chief Privacy Officer & Senior Compliance Director	Ohio Health
Etherton	Anna	IT Specialist (INFOSEC)	DHS/CS&C
Farabella	Helena	National Chairperson	PAHCOM
Finn	David	Health IT Officer	Symantec
Fleet	Eli	Director of Federal Affairs	HIMSS
Frederick	Michael	VP Operations	HITRUST
Goldman	Julian	Clinician: Attending Anesthesiologist, Massachusetts General Hospital / Harvard Medical School	Harvard Med
Goldstein	Eric	Branch Chief, Partnerships and Engagement	DHS CS&C
Gomez	John	CEO	Sensato
Gorme	Craig	IT Security Manager	UF Health and Shands Hospital
Grillo	Jorge	CIO/VP Facilities, Safety, Security, Construction and EVS	St Lawrence Health System
Heesters	Nick	Health Information Privacy Security Specialist	HHS/OCR/HIPAA
Hicks	Andrew	Managing Principal	Coalfire
Hinde	William	Managing Director	West Monroe Partners
Holtzman	David	VP, Compliance Strategies	CynergisTek, Inc.

Last Name	First Name	Title	Organization
Jackson	Helen	Program Analyst	DHS/CS&C
James	Bruce	Director of Cybersecurity Architecture	Intermountain Healthcare
Jarrett	Mark	Chief Quality Officer, Association Chief Medical Officer	Northwell Health
Jobes	Kathy	VP and CISO	Ohio Health
Kacer	Wendy	Sr. Director, Cybersecurity Governance, Risk and Compliance	Dignity Health
Kim	Lee	Director of Privacy and Security	HIMSS
Klein	Sharon	Partner	Pepper Hamilton
Krigstein	Leslie	VP, Congressional Affairs	CHIME
Lacey	Darren	CISO	Johns Hopkins
Lee	Wayne	Chief Cybersecurity Architect	West Monroe Partners
Levy	Lenny	VP and CIS	Spectrum Health
Love	Talvis	Senior Vice President (SVP), Enterprise Architecture, eCommerce and CISO	Cardinal Health
Maksymow	Michael	VP and CIO	Beebe Healthcare
Marquette	Casey	Sr. Director, Information Security (INFOSEC)	CVS Health
McAllister	Guy	VP and CIO	Tift Regional Medical Center
McDonald	Blair	IT INFOSEC Analyst	HHS/OS/OCIO
McLendon	John	VP and CIO	Johns Hopkins All Children's Hospital
Nonneman	Lisa	IT Director	Mary Lanning Healthcare
Nordenberg	Dale	Executive Director	MDISS
Palmer	Dennis	Sr. Assurance Associate	HITRUST
Quinn	Jessica	SVP, Chief Compliance Officer	Ohio Health
Quinn	Matthew	Sr. Advisor, Health Technology	HRSA
Riethmiller	Erika	Director, Corporate Privacy Incident Program	Anthem
Ross	Aftin	Senior Science Health Advisor	FDA.HHS/OCIO/OIS
Royster	Curtis	IT Specialist	DC Government/Department of Health Care Finance
Savickis	Mari	VP, Federal Affairs	CHIME & AEHIS
Savoie	Don	Chief Operating Officer (COO)	Meridian Behavioral Health Center

Last Name	First Name	Title	Organization
Schwartz	Suzanne	Associate Director for Science and Strategic Partnerships	FDA.HHS/OCIO/OIS
Shaikh	Munzoor	Director	West Monroe Partners
Siler	Kendra	President	CommunityHealth IT
Skinner	Rich	Head of Strategy and Business Development-Cyber Security	West Monroe Partners
Smith	Philip	President	MedMorph LLC
Stephens	Timothy	Sr. Advisor	Biologics Modular
Stevens	Deborah	VP and CISO	Tufts Health Plan
Stine	Kevin	Chief of the Applied Cybersecurity Division	NIST
Tennant	Rob	Director, HIT Policy	Medical Group Management Association
Teyf	Daniel	Security Architect	Colorado Governor's Office of IT, Office of Information Security, CISO
Thomas	Mitchell	Chief Security Officer	HealthSouth Inc.
Tierney	Logan	Project Manager	Greater New York Hospital Association
Todd	Nickol	Deputy Director, Division of Resilience	HHS/ASPR
Voigt	Leah	Chief Privacy and Research Integrity Officer	Spectrum Health
Wang	May	Chief Technology Officer and Co-founder	ZingBox
Watson	Kelli	Cybersecurity Operative and Researcher	Sensato
Webb	Tim	Partner	InfoArch Consulting, Inc.
West	Karl	CISO	Intermountain Healthcare
Wheatley	Cathleen	System Chief Nurse Executive and VP of Clinical Operations	Wake Forest Baptist Health
Willis	David	Medical Director	Heart of Florida Health Center
Wilson	Chad	Director of Information Security	Children's National Health System
Wilson	Kafi	Principle/CEO	KWMD LLC
Wivoda	Joe	Sr. Director of Healthcare at Analysts	Analysts
Wolf	Laura	Supervisory Program Analyst	HHS/ASPR
Worzala	Chantal	VP, Health Information Policy	American Hospital Association
Wright	Michael	Sr. Manager	Baker Tilly
Zigmund-Luke	Marilyn	Sr. Counsel	America's Health Insurance Plans (AHIP)

Appendix E: Best Practices and the NIST Cybersecurity Framework

The 405(d) Task Group identified the following ten most effective best practices to mitigate common threats across the large, complex U.S. healthcare sector:

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. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Each best practice is aligned to the NIST Cybersecurity Framework (NIST Framework). The NIST Framework articulates a consistent structure with five cybersecurity functions: identify, protect, detect, respond, and recovery. It describes the intended cybersecurity outcome. With the best practices **identified** in this document, organizations are encouraged to embark on the **protective, detective, responsive,** and **recovery** activities in each of the 10 practice areas.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.D	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 1. Function and Catrgory Unique Identifiers

For example, Best Practice #1: Email Protection Systems, outlines a series of steps to protect the organization from phishing, ransomware, and data leakage. These practices align to the Protect function of the NIST Framework. Specifically, they map back to the PR.AC-1, PR.AC-7, PR.AT-1, PR:.DS-1, PR.DS-2, PR.DS-5, and PR.PT-4.

Within the two technical volumes, each of the ten best practices has a set of sub-practices, which vary depending on the size of the organization. For each best practice, *Table 2* identifies the number of sub-practices provided for small, medium and large organizations. Large organizations will benefit from sub-practices for both medium and large organizations.

Best Practice	Sub Practices, Small	Sub Practices, Medium	Sub Practices, Large
Email Protection Systems	3	4	3
Endpoint Protection Systems	1	1	6
Access Management	1	4	3
Data Protection and Loss Prevention	2	5	2
Asset Management	3	4	3
Network Management	3	5	5
Vulnerability Management	1	4	1
Incident Response	2	3	6
Medical Device Security	1	5	4
Cybersecurity Policies	1	1	1

Table 2. Best Practices Have Multiple Sub-Practices for Small, Medium and Large Organizations

Appendix F: Best Practices Assessment and Roadmaps

Within this the Technical Volumes, there are a total of 88 practices. It would be a daunting task to implement all these practices at once. In some cases, an identified practice may not be the best option for your organization. An assessment methodology is provided below to assist you with selecting and prioritizing the practices of greatest relevance.

Self Assessment Methodology

As stated during the introduction, this document is focused on the five most prevailing threats currently impacting our sector. These five threats, summarized in *Table 1*, should be front of mind as you assess which practices to implement first.

Many models exist to help enumerate priority and criticality based on risk. Below is a simple model that may be followed:

Step 1: Enumerate and Prioritize Threats
Step 2: Review Best Practices Tailored to Mitigate Threats
Step 3: Determine Gaps Compared to Best Practices
Step 4: Identify Improvement Opportunity and Implement
Step 5: Repeat for Next Threats

Step 1: Enumerate and Prioritize Threats

The first step in implementing a threat centric approach to mitigate cyber-attacks is to evaluate and prioritize the threats that are listed below. Organizations may have different perspectives on their threat susceptibility, causing variations in the threats to be mitigated.

Full details of conducting a threat assessment can be found within NIST Special Publication 800-30. For the purposes of this document, one should review the impacts these threats can cause to determine which is of the highest priority.[11]

Threat #	Threat Description	Impact of Attack
A	Email Phishing Attack	Potential to deliver malware or conduct credential attacks. Both attacks lead to further compromise of the organization.
B	Ransomware Attack	Potential to lock up assets (extort) and hold them for monetary "ransom." May result in the permanent loss of patient records.
C	Loss or Theft of Equipment or Data	Potential for equipment to be lost or stolen and lead to a breach of sensitive information. This may lead to identity theft of patients.
D	Accidental or Intentional Data Loss	Potential for data to be intentionally or unintentionally removed from the organization. May lead to a breach of sensitive information.
E	Attacks Against Connected Medical Devices and Patient Safety	Potential for patient safety to be impacted by a potential cyberattack. May could cause adverse safety events to the patient.

Table 1: Top 5 Threats to Health Sector

Step 2: Review Best Practices Tailored to Mitigate Threats

Once you have selected the first threat to mitigate, the next step is to review the series of best practices that exist to mitigate that threat. *Table 2* correlates threats mitigated to Cybersecurity Best Practices.

Practice #	Cybersecurity Best Practices	Threats Mitigated
1	Email Protection Systems	A, B, D
2	Endpoint Protection Systems	B, C
3	Access Management	B, C, E
4	Data Protection and Loss Prevention	B, C, D
5	Asset Management	B, C, D, E
6	Network Management	B, C, D, E
7	Vulnerability Management	B, C, E
8	Incident Response	A, B, C, D, E
9	Medical Device Security	E
10	Cybersecurity Policies	A, B, C, D, E

Table 2: Cybersecurity Best Practices Mapped to Threats Mitigated

As the best practices in this document mitigate multiple threats, it is advisable to consider the practices that provide the best breadth of protection, followed by the practices that provide the most depth to mitigate the threat.

For example, if your first start is protection against Phishing attacks, then a logical path would be to begin with Best Practice #10: Policies, followed by Best Practices #1: Email Protection Systems. This approach ensures the policy is established when you update your email protection capabilities.

Step 3: Determine Gaps Compared to Best Practices

Now that you have selected the best practices to mitigate identified threats, the next step is to review the sub-practices associated with these selections, comparing the sub-practice to the current state of your existing safeguards. Identify any gaps between the existing state and the identified best practice.

Step 4: Identify Improvement Opportunity and Implement

Assess each identified gap to determine if the reviewed practices will provide sufficient protection for your organization considering the projected cost to implement them. If it is determined to be a cost-effective solution, then identify the practice for implementation.

Leveraging common project management methodologies is ideal to ensure effective implementation of complicated practices.

Step 5: Repeat for Next Threats

After you have successfully iterated through the first prioritized threat, repeat Steps 1 through 4 for the next threats. In doing so, you create a roadmap to implement best practices that fit within your organization's resource and cost constraints.

Example Assessment

The five-step process is described in an example for a fictitious small provider practice in *Table 3*.

Step	Analysis	Outcome
Step 1: Threat Assessment	Reviewed all threats. Threat most likely to occur is phishing.	Determined that phishing attacks could cause the most damage to the organization. Start here.
Step 2: Review Best Practices	Reviewed all 10 Best Practices.	Identified three practices that would help mitigate this threat: Email Phishing Protection, Security Operations Center / Incident Response (SOC/IR), Policies and Procedures.
Step 3: Determine Gaps	Reviewed the sub-practices identified within the three practices.	Email phishing protection controls are sufficient. No education or phishing simulation conducted.
Step 4: Identify Improvement Opportunities and Implement	Phishing education comes with no direct costs. Phishing simulations would be too expensive for the small practice.	Deferred the implementation of Phishing simulation. Established a workforce phishing education program and implemented.
Step 5: Repeat	Reviewed additional 4 threats, determined next most critical is ransomware.	Start the process anew.

Table 3. A Small Provider Practice Applies the Five-Step Process to a Phishing Attack Scenario

Appendix G: References

44 U.S. Code § 3502 - Definitions

- https://www.law.cornell.edu/uscode/text/44/3502

Division N – Cybersecurity Act of 2015

- https://www.epic.org/privacy/cybersecurity/Cybersecruity-Act-of-2015.pdf

First Amendment

- https://www.law.cornell.edu/constitution/first_amendment

Health Insurance Portability and Accountability Act of 1996

- https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

IBM X-Force Threat Intelligence Index 2017

- https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/

Indian Self-Determination and Education Assistance Act, as Amended

- https://www.bia.gov/sites/bia.gov/files/assets/bia/ots/ots/pdf/Public_Law93-638.pdf

National Institute of Standards and Technology Act

- https://www.nist.gov/sites/default/files/documents/2017/05/09/NIST-Organic-Act.pdf

PUBLIC LAW 111–5—FEB. 17, 2009

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

TITLE 50—WAR AND NATIONAL DEFENSE

- https://www.gpo.gov/fdsys/pkg/USCODE-2009-title50/pdf/USCODE-2009-title50-chap36-subchapI-sec1801.pdf

Appendix H: Resources

Below is a list of free resources with supplemental information for the threats and concepts addressed in this document. This list is not intended to be comprehensive or complete.

HHS Resources

HHS Cybersecurity Task Force Report

- https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx

Critical Infrastructure Protection for the Healthcare and Public Health Sector

- https://www.phe.gov/preparedness/planning/cip/Pages/default.aspx

My entity just experienced a cyber-attack! What do we do now? A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

- https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

Cyber-Attack Quick Response

- https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif

FACT SHEET: Ransomware and HIPAA

- https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es

Cybersecurity Awareness Training

- https://www.hhs.gov/sites/default/files/fy18-cybersecurityawarenesstraining.pdf

Security 101 for Covered Entities

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Protecting the Healthcare Digital Infrastructure: Cybersecurity Checklist

- https://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-checklist.pdf

DHS Resources

Department of Homeland Security Component Overview

- https://www.dhs.gov/sites/default/files/publications/DHS%20Cybersecurity%20Overview_2.pdf

(US-Cert) Cybersecurity Framework

- https://www.us-cert.gov/ccubedvp/cybersecurity-framework

(ICS-CERT) Standard and References

- https://ics-cert.us-cert.gov/Standards-and-References#plan

DHS Stop.Think.Connect. Campaign

- https://www.dhs.gov/stopthinkconnect

NIST Resources

SP 800-30, Risk Management Guide for Information Technology Systems

- https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

SP 800-39, Managing Information Security Risk: Organization, Mission, Information System View,

- https://csrc.nist.gov/publications/detail/sp/800-39/final

SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

- https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

SP 800-28 Version 2, Guidelines on Active Content and Mobile Code,

- https://csrc.nist.gov/publications/detail/sp/800-28/version-2/final

SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access,

- https://csrc.nist.gov/publications/detail/sp/800-114/archive/2007-11-01

SP 800-177, Trustworthy Email

- https://csrc.nist.gov/publications/detail/sp/800-177/final

SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

- https://csrc.nist.gov/publications/detail/sp/800-181/final

SP 800-184, Guide to Cybersecurity Event Recovery

- https://csrc.nist.gov/publications/detail/sp/800-184/final

SP 800-63-3, Digital Identity Guidelines

- https://csrc.nist.gov/publications/detail/sp/800-63/3/final

SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

- https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

- https://www.nist.gov/publications/guide-enterprise-telework-remote-access-and-bring-your-own-device-byod-security

Appendix I: Templates

About Templates and How to Use Them

This section provides practical document templates that can be used by providers to aid in strengthening the privacy, security and cyber-security protocols of their practice. This section is not meant to provide all policies and procedures required to be in place for covered entities and business associates subject to various federal and state privacy and security requirements. However, a sampling of templates are provided for cyber-security protection and related topics. Future editions of this document may include additional templates and checklists.

The following templates ARE:

- Available to be used at no charge
- Designed to be carefully reviewed and revised by the provider (by merging technical system and office staff policy and workflow into the documents) so that they reflect business practice
- Representing different levels of content and style which may be more suited for small, medium, large organizations

ARE NOT:

- Representative of a complete set of privacy and/or security Policies and Procedures
- Including required state/federal laws and regulations. Each provider/practice is responsible to understand how sensitive information such as Protected Health Information (PHI) and/or Personally Identifiable Information (PII) is handled and to gain and maintain compliance with required laws/regulations separate from this section

How to Use These Templates-Policy Template Instructions

Using templates

Highlight the desired section/template. Copy the file to your hard drive. You may copy the Template file for your own use and cut sections from it to paste into your own documents, or start with these if current documentation is not in place.

Carefully review the language and assure it is applicable to your practice and business operation. Modify it as necessary to assure language is easy for your workforce members to understand.

How Policy Templates are Organized

This section includes various templates with a wide variety of style. However, in general, Policy and Procedures often have key sections. Below is a description of methods of organization. Choose the format that works best for your organization.

Sections – Think about the overall grouping of topics for your documentation. For example, you may choose to group together those policies that address workforce behavior. These may include topics like Acceptable Use and Workstation protocols. Another category often grouped together would be those policies governing HIPAA Security that are the responsibility of the Security Officer (versus those types of policies applying to all workforce members (like Email Usage). It may be helpful to group together the technical systems specific policies, and/or those dealing with Incident Response and Reporting and Breach Notification. This is an attempt to organize the material in a logical sequence, to make it easier for a user to find a particular template, and to facilitate ease in the next step of the compliance life cycle – which is training. Users may want to adopt a similar organizational format for their policy manuals. Keeping policies and procedures current becomes an ongoing process so choosing one format makes the revision and educational processes easier to manage.

Policy Template Structure – Templates are often divided into several parts, as follows:

Responsibility: Generic titles for personnel responsible for implementing the policy should be listed. If your chosen template has this section, users should change the titles to match their organization's terminology, organizational structure and division of duties. It is not practical to list individual names, but tying together the titles of those responsible for certain functions assures that all reading the document understand the individual(s) accountable for assuring the policy is in place.

Background: Some templates do not contain a background section. However, those that do, offer this as this section describes what the policy is trying to accomplish. Users should consider including background descriptions in their final policies, as a guide to understanding the issues and concepts behind the policy.

Policy: Provides suggested wording for the policy. The templates included herein are written to incorporate the relevant regulatory requirements in the policy section. Due to the detailed nature of some of the regulations, this sometimes results in very detailed policy statements. However, keeping a distinction between requirements (policy) and options to accomplish the requirements (procedure) is a good way to assure the documents are representative of your practice, but maintain their alignment with the required regulation or law for which they are written. Users are strongly cautioned to understand the overall regulations for which a policy is needed prior to making substantive changes to the policy sections of template documents.

Procedure: The policy can be thought of as the "What." The procedure is the "How." Users should augment and/or modify the procedure sections of these templates as necessary to fit their organization/ department's way of doing things.

Notes - Notes are included in some templates. When notes are available, they are to provide further guidance and explanation in applying the policy.

Definitions - Understanding definitions is an essential part of a complete set of policies and procedures. Users should be sure to include a Definitions section in their final privacy, security/cyber security documentation.

Revision History - Once compliance is gained, being able to keep the document in alignment with your organization's practices and to prove ongoing revision, having a Revision History is key. A routine annual review for possible revisions is suggested as a Best Practice. Frequency may be more often as necessary due to systems and operational changes. A good example of a history block is apparent in the examples that follow from SANS.

Information about These Templates

In order to provide a sampling of policy and procedure templates that may be more appropriate for smaller versus larger organizations, template samples have been donated by some companies that provide HIPAA Privacy and Security Toolkits. This document, and this section specifically are in no way recommending or suggesting the purchase of vendor materials, but instead offering samples that were donated or otherwise made available to this initiative by the following organizations:

- Federal Communications Commission Cyber Security Planning Guide - https://transition.fcc.gov/cyber/cyberplanner.pdf. While this Planning Guide does not offer specific "templates", it does include a depth of information which may pertain directly to small provider offices to the degree they serve as a small business environment. Be sure to review the section on Preventing Phishing, and potentially leverage the Definitions and Security Links (for Training and other Cyber Security Reporting information).
- Health IT Gov - https://www.healthit.gov/node/289 - Security Policy Templates were gathered as the Regional Extension Centers assisted Primary Care Providers to gain HIPAA/HITECH compliance. A series of templates and forms are available at no charge. A helpful on-line "Top 10 Tips on Cyber-Security" specific to providers can be found at https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf.
- The Office of the National Coordinator has recently published a draft document on "Trusted Exchange Framework and Common Agreement" with goals and principles to be voluntarily adopted as our industry continues to increase shared information. To aid the providers for which this document is provided, a "Do's and Don't's Template for Trusted (data) Exchange" has been provided which mirrors these principles. It can be used as a handy desk reference to aid in healthcare/information technology business decision making processes. More information can be found at https://www.healthit.gov/newsroom/21st-century-cures-act-trusted-exchange-framework-and-common-agreement-webinar-series
- SANS – Specific to Security, this suite of templates from The SANS Institute is available at no charge and can be downloaded at https://www.sans.org/security-resources/policies.

Small Provider Example – Portable Devices

To customize this template document, replace all of the text that is presented in brackets (i.e. "[" and "]") with text that is appropriate to your organization and circumstances. Many of the procedure statements below represent "best practices" for securing mobile computing. These may not be feasible or available for your practice. Be sure this document reflects the actual practices and safeguards currently in place!

Laptop, Portable Device, and Remote Use Policy and Procedure

[Organization name]

Purpose: This organization considers safeguarding its electronic information, personally identifiable information, intellectual property and any patient information, e.g. "sensitive information" of paramount importance. [Organization name] has developed a series of privacy and security policies and procedures as well as a series of computer and internet use policies and procedures.

Certain employees and contractors of [organization] use portable and mobile computing devices including [Insert as applicable]:

- Laptop Computers
- Tablet Computers
- iPADs or their equivalent
- Smartphones
- Other mobile devices [specify]

For work related tasks while traveling or at home. This sometimes entails remote access to our networks, to our applications that create, store, maintain or transmit ePHI, or to websites that create, store, maintain or transmit ePHI.

It is the policy of [organization] that all remote use and/or access will be done with established security safeguards.

Procedure:

1. Laptops and [insert type of device(s)-for example, "Smartphone and Tablet"] that are assigned to individuals for remote use will be accounted for on a computer asset inventory.
2. Laptops and [insert type of device(s)-for example, "Smartphone and Tablet"] must be configured with the standard configuration prior to use remotely.
3. The standard laptop and if available [insert type of device(s)-for example, "Smartphone and Tablet"] configuration will require a unique user login ID and password complexity equal to that of the network if feasible. The current policy on password strength and change will be in force.
4. The standard laptop and [insert type of device(s)-for example "Smartphone and Tablet"] configuration will require the laptop to automatically log off after a period of [enter timeout period-portable devices should have a lower timeout than devices secured in your medical practice because they are more susceptible to theft] minutes of inactivity.
5. The standard configuration will require documents to be written to the [organization] server where possible. [Organization] will use appropriate technology tools to synchronize all laptop and [insert type of device(s)-for example, "Smartphone and Tablet"] files with the network server and thus ensure the laptop files are a) resident on the server and b) part of the routine backup. Note: A variety of software applications ensure that data on mobile devices can be automatically synchronized to your network or cloud server-such as Dropbox, Evernote, Apple iCloud, Microsoft Office 365 or other synchronization tools and so forth.

6. The standard configuration will require network drive folder level passwords where feasible, when the files relate to confidential or proprietary information.
7. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”], will be encrypted at either the entire drive or solid-state memory level, or with a partition encryption where the partition contains ePHI.
8. Encryption keys will be separate from the device and maintained with appropriate complexity by the Security Official or their designee. NOTE: Organizations are required by HIPAA to appoint a Privacy and Security Officer. However depending upon the size and complexity of the organization, this official may be the Office Manager, Physician in charge or “responsible security individual”.
9. Screenshots with ePHI shall not be saved to laptops or [insert type of device(s)-for example, “Smartphone and Tablet”] unless encryption is enabled.
10. The standard configuration will require malicious software protection to be enabled on the laptop and [insert type of device(s)-for example, “Smartphone and Tablet”], along with automatic live updates. Note: Smartphones, tablets and other mobile devices are also susceptible to viruses or spyware!
11. If laptops [insert type of device(s)-for example, “Smartphone and Tablet”] are used, the security official will enable automatic updating of security patches.
12. When laptop or mobile device security patches or updates are not automatically downloadable but otherwise can be downloaded from a website, the security official will notify, by email, all employees who have a laptop or [insert type of device(s)-for example, “Smartphone and Tablet”], requesting they download and install the update. The security official will request a confirmation receipt of the email and notification of the update. The security official will track responses and if necessary take possession of the device to ensure updates.
13. [Optional] Laptops or [insert type of device(s)-for example, “Smartphone and Tablet”] will be configured with remote security controls that will remotely wipe the device upon loss or theft, scan for malware, provide Global Position System (GPS) tracking, encrypt partitions or memory that stores ePHI, alert or block introduction of unauthorized Subscriber Identity Module (SIM) cards.
14. Smartphones and tablets that are used to access, receive or transmit ePHI via email shall only do so with this medical practice’s secure domain mail server or [insert type of secure encrypted email system]. Email settings shall be configured to limit the number of recent or emails stored on the device.
15. Smartphones and tablets that are used to access, receive or transmit ePHI shall be configured to limit the number of text messages stored on the device. Only secure text messaging systems shall be used.
16. Laptops or [insert type of device(s)-for example, “Smartphone and Tablet”] that use wireless communications including Bluetooth will be configured to always turn off the “Discoverable Mode” to ensure the device is not viewable by unauthorized persons. Alternatively, where “Discoverable Mode” is necessary for proper pairing, the user shall be trained to disable this mode when in public places where data and conversations can be discovered by nearby unauthorized individuals.
17. Laptop and [insert type of device(s)-for example, “Smartphone and Tablet”] users will be trained and periodically reminded to pair their devices with the pairing laptop in private locations, and not public locations. Users will be trained to understand that there may be eavesdroppers who may be hacking, sniffing, or setting up malicious code.
18. Laptop and [insert type of device(s)-for example, “Smartphone and Tablet”] users are not allowed to change any setting or security rule on their laptops or [insert type of device(s)-for example, “Smartphone and Tablet”] without permission from the Security Official.
19. Laptop and [insert type of device(s)-for example, “Smartphone and Tablet”] users must adhere to the general [organization] computer and internet use policy including not downloading software, introducing foreign media, and so forth.

20. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”], when in transit, must be carried in the user’s immediate vicinity with appropriate covers or containers. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”] should not be left unattended.
21. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”] when in use at the employee/contractor’s home should be used in a secure location and only by the employee/contractor and not by family/friends or other unauthorized individuals. Users may not use their devices or remotely access ePHI in the immediate presence of any unauthorized person, family or friend who might view the information.
22. Flash drives and other media copying of ePHI will only be used if password protection is enabled and the drive or media is encrypted and provided by the Security Official.
23. All remote access to the [organization] networks or cloud-based applications with ePHI shall be done with the use of a secure access [insert the type of access; for example if you have set up a VPN].

I have read this policy and procedure and will adhere to its requirements:

_____ _____

_____

Name of Employee/Contractor Date Employer Date

Mid-Large Provider Example – Incident Reporting and Checklist; Workforce Training At-a-Glance One Page Reference Sheet

SECURITY INCIDENT PROCEDURES: RESPONSE AND REPORTING

RESPONSIBILITY: Security Official, Director of Information Systems, and Privacy Official

BACKGROUND: Development of an internal mechanism to identify and address privacy/security incidents is required by regulations. Formal report and response procedures are an integral component of a security program. A security incident can be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Including privacy incidents or "wrongful disclosures" means the incidents can not only come from an information system, but also from paper documents or any other place across the organization where PHI is created, handled, maintained or stored.

[Note: This policy can be easily expanded to address Red Flag issues (see https://www.consumer.ftc.gov for information). Many examples under the Procedure section can also be considered triggers.]

POLICY:

1. [ENTITY] maintains a comprehensive internal security control program, which is coordinated by the Information Systems department. [ENTITY] also maintains a base compliance program which functions to keep PHI protected and addresses issues of breach of security and privacy policies and procedures by monitoring and mitigating such issues. The internal privacy/security incident reporting process is the mechanism of both the security control and compliance programs, which allows for the organization to identify, investigate, respond, and resolve known and suspected privacy and security incidents. The actual reporting of incidents occurs in two ways:
   1.1. Through the use of a Privacy/ Security Incident Reporting Form (Note: This is used for all of the [ENTITY] workforce members and may also be utilized by outside organizations/individuals such as contractors or business associates.)
   1.2 As a result of monitoring pre-configured automated system security reports, and use of internal audits and monitoring reviews to identify issues.
2. Regardless of mode of receipt, a chain of command process is used to first address and resolve the issue, report to the impacted individual or other parties (e.g. regulators) where applicable and communicate any necessary curriculum changes resulting from the incident(s) to all workforce members as a core component of training.

PROCEDURE:

1. All workforce members are trained to use the Privacy/Security Incident Reporting Form to report any suspicious privacy/security activities. Specific occurrences which will trigger the completion of the form may include but not be limited to the following:
   1.1 Any suspicious or known breach of privacy/security by any workforce member for any reason known to be a violation or contradiction of [ENTITY]'s philosophy of protecting and safeguarding PHI.
   1.2 Any suspicious or known breach of privacy/security by an external third party for any reason known to be a violation or contradiction of [ENTITY]'s philosophy of protecting and safeguarding PHI.
   1.3 Any suspicious activity uncovered as a result of a review of routine or random audit trail.
   1.4 Request for audit log review of user activity (special authorization required)
   1.5 Suspected or proven violation of protection of malicious software (introduction of malicious software)

1.6 Violation of Login Attempt (Using or attempting to guess another users log in and/or password)

1.7 Sharing of passwords

1.8 Inappropriate access to the internet

1.9 Improper network activity

1.10 Improper Email Activity / Phishing

1.11 Inappropriate access by customer, client, member, contractor or business associate

1.12 Suspicious documents (inconsistent identification information, photo or physical description, suspected altered or forged signatures)

1.13 Suspicious Medical Information (Member unaware of or denies information previously collected in the medical record, or other trigger that member information is inconsistent with that previously found)

1.14 Suspicious requests (mail returned even though attempts at verifying address have occurred), patterns of usage inconsistent with previous history, frequent ID card requests or replacement requests with change of address

1.15 Personal Information Suspicious (known fraud associated with personal information, inability for person to authenticate via challenge/secret questions, personal information inconsistent with other information on file or that provided via external source, duplicate identifiers (SSN, Medicaid, Medicare cards))

Note: Consider reviewing the "Identity Theft Resource Center" compiled list of breaches as a way to identify patterns, trends and any information to better communicate examples of occurrences that should trigger workforce members to identify and complete an incident report.

2. Forms must be accurately and thoroughly completed within (XXX) hours of the incident (or sooner if the suspected or known breach causes serious risk to the organization) and forwarded immediately to the attention of the workforce member's direct supervisor and the Privacy and Security Officers. In the event an organization or individual outside [ENTITY] provides the report, the same time frame and reporting procedure applies to the [ENTITY] workforce member in receipt of the report. [Note: This template assumes the form itself is only in hard copy form. An organization may consider the supply and use of the form in electronic mode. Additionally a procedure should be in place for workforce members to forward the incident report directly to the Privacy and Security Officers in cases when the suspect is the issuer's direct supervisor. Telephone, anonymous hotlines and ot other automated processes may exist and should be merged into this procedural section as they relate to the practice. It is also important to train members of the workforce to keep incident information confidential in order to prevent the suspect from learning of the report. This action may serve to prevent the suspect from trying to cover their tracks.] Form may be copied in duplicate in order to facilitate this process and should include at least the following information:

   2.1 Date,

   2.2 Name,

   2.3 Title of submitter,

   2.4 Reason for report,

   2.5 Indication of whether or not the activity is suspected or known,

   2.6 Indication of what application (s) or system(s) have been violated

   2.7 Identification of the user in question if appropriate, form may include a listing of the more common reasons for completing the report (listed above) and checkbox style.

   2.8 A section of the form should include date received and notes for investigation, mitigation and further actions.

3. Upon receipt of completed Security Incident Report, or automated system security report, the Privacy and Security Officers will review (and conduct superficial investigation if necessary) in order to confirm the validity and level of risk associated with the reported incident in order to place the report in priority with other reports for committee review.

4. The Security Officer, Privacy Official, Director of Information Systems, and any other affected department Director/Manager will convene within a reasonable period of time (depending upon the level of risk of the incident) and as frequently as necessary to determine the following:

   4.1 Investigate and validate the facts included in the incident report, this should include assessment of possible damage to the organization.

   4.2 Determine if the incident needs to be reported to law enforcement, other authorities or the CERT Coordination Center.

   4.3 Determine if unsecured protected health information was acquired or disclosed in a breach situation. If so, determine method to report to Secretary of DHHS (log book or direct report) see DUTY TO REPORT SECURITY OR PRIVACY BREACH, NOTIFY AND MITIGATE THE EFFECT.

   4.4 Determine application of sanctions as necessary in accordance with the Sanctions Policy.

   4.5 Lessen or mitigate any harmful effects to the extent necessary and applicable.

   4.6 Determine if issue should be evaluated as part of a larger review (such as part of ongoing risk analysis), and whether or not systems configuration and/or changes to other related [ENTITY] policies andprocedures are necessary.

   4.7 Address communication and training to all affected workforce members if policies and procedures are to be implemented or modified in accordance with MAINTENANCE OF POLICIES AND PROCEDURES document.

5. All necessary actions, including outcomes, will be handled promptly and documented in accordance with [ENTITY] policy.

6. On a routine basis (quarterly or monthly) the Privacy/Security Officers should provide to the organization's senior management level representatives, aggregate reporting of all received privacy/security incident reports, and the organization's response, including level of sanctions applied, mitigation attempts, and/or resulting changes to policies and procedures. (NOTE: One may also include members of the organization's board of directors if applicable).

   REFERENCE: 45 CFR §§ 164.308(a)(6)(i), (ii) NOTE: Names of other policies appearing in all CAPS should be appropriately cross-referenced to other practice policies.

Access Control Procedure for [SYSTEM NAME]

OVERVIEW

The purpose of this procedure is to ensure that the proper processes and safeguards are in place for the use of *[SYSTEM NAME]* by the *[DEPARTMENT(S) NAME]* at the *[ORGANIZATION NAME]*. This procedure outlines the requirements for the creation, deletion and review of user accounts and access for *[SYSTEM NAME]*, and complies with the Enterprise Access Control, Responsibilities and Oversight, Personally Owned Device, and Electronic Media Protection Policies.

SCOPE

This procedure applies to all user accounts created within *[SYSTEM NAME]* for *[ORGANIZATION NAME] [AND EXTERNAL]* users in *[DEPARTMENT(S)]. [It also applies to mobile devices used to access (SYSTEM NAME)].*

PROCEDURES

A. Roles

Information Owner	[JOB ROLE]
Information System Owner	[JOB ROLE]
IT Custodian(s)	[JOB ROLE]

B. Account Creation

1. The following roles and privileges are identified for *[SYSTEM NAME]*:

(Example:)

JOB ROLE	YSTEM PRIVILEGE	SYSTEM ROLE
IT Custodian	Read/Write Create/Delete User Accounts	System Administrator
JOB ROLE 2 (e.g., analyst, nurse, etc.)	Read/Write	General User
External UCM/BSD User	Read Only	External User

2. All requests for internal and external user accounts must be directed to *[JOB ROLE]* by the employee's immediate manager or *[EXTERNAL CONTACT PERSON]* and submitted *[in writing, via email, through a SARF, etc.]*. All requests for access to *[SYSTEM NAME]* must include the following information:
   a. User's name, job title, and system job role/privileges requested
   b. Detailed business justification for the type of access sought
3. *[JOB ROLE]* is responsible for communicating with *[VENDOR NAME/CONTACT PERSON]* within *[TIMEFRAME]* when a user's account should be created.
4. *[JOB ROLE]* is responsible for ensuring that accounts are created with the appropriate system privileges as outlined in Section B.

6. All user accounts created will be documented in the *[SYSTEM USER ACCESS DOCUMENT]* by *[JOB ROLE]*, including the user's name, date user account was created, job role, name of user's manager who approved system access, system privileges and system role assigned to the account.

7. Passwords for *[SYSTEM NAME]* should not be the same as users' UCM login passwords, should comply with the Access Control Policy, and consist of the following minimum requirements:
   a. A minimum of 8 characters.
   b. Include mixed case letters and numbers or special characters.
   c. Password must be changed at least every 120 days (whether *[SYSTEM NAME]* technically enforces it or not.)
   d. Passwords must not be the same as the username.
   e. Passwords may not be reused until 3 additional passwords have been used.
8. If users are sent a default password when an account is created, users must be informed to change their *[SYSTEM NAME]* account password immediately, and comply with the above requirements.

C. Account Deletion

1. A user's immediate manager will notify *[JOB ROLE]* within *[TIMEFRAME] [via email, form, SARF, etc.]* when the user leaves, is terminated or is transferred to ensure access to *[SYSTEM NAME]* is deleted or disabled or privileges are changed within a timely manner.

2. *[JOB ROLE]* is responsible for communicating with *[VENDOR NAME/CONTACT PERSON]* within *[TIMEFRAME]* when a user's account should be disabled or deleted, or privileges should be changed. [JOB ROLE] will communicate changes to user accounts with *[VENDOR NAME/CONTACT PERSON] [via email/ calling vendor help desk, etc.]* (OR *[JOB ROLE]* is responsible for disabling, deleting or changing privileges for user accounts within the system administrator console within *[TIMEFRAME]* of being notified of the change.)

3. *[JOB ROLE]* will follow up with *[VENDOR NAME/CONTACT PERSON]* within *[TIMEFRAME]* to ensure that the user account was deleted/disabled/changed by the vendor appropriately and within the timeframe specified.

4. All user accounts deleted, disabled, or changed will be documented in the *[SYSTEM USER ACCESS DOCUMENT].*

D. Account Review

1. *[JOB ROLE]* is responsible for monitoring account creation, deletion and privileges/roles for *[SYSTEM NAME].*

2. Accounts should be reviewed every *[TIMEFRAME]* by *[JOB ROLE(S)].*
   a. *[JOB ROLE]* will contact *[VENDOR/CONTACT PERSON]* to receive an accounts report from *[VENDOR NAME]* for confirmation of active user accounts and privileges (or login to the Administrator console for *[SYSTEM NAME]* to verify active user accounts and roles).
   b. Vendor reports should be compared with the *[SYSTEM USER ACCESS DOCUMENT]* in order to verify user account access and privileges.
4. Discrepancies in user account access and privileges will be addressed immediately by *[JOB ROLE]* in order to mitigate inappropriate access to the system.

E. Mobile Devices

1. The use of *[SYSTEM NAME]* on mobile devices is allowed if the following conditions are met:
    a. *[JOB ROLE]* coordinates with the Help Desk to ensure that users' mobile devices are enrolled in the [ORGANIZATION NAME] Mobile Device Management System.
    b. Mobile devices must have an antivirus application installed and running.
    c. Mobile devices must be encrypted.
    d. Mobile devices must be password/fingerprint/pin protected.
    e. Mobile devices will have remote wipe capabilities.
2. *[JOB ROLE]* ensures that the Personally Owned Device Policy and Electronic Media Protection Policy are followed.

Date	Revision	Author
99/99/99	Created Access Control Procedures	[AUTHOR NAME]

Privacy and Security Incident Report

NAME

<<Address>>

<<Phone>>

The Privacy/Security Incident Report form is an internal mechanism used to report suspicious privacy/security activities. Forms must be accurately and thoroughly completed within 24 hours of the incident (or sooner if the suspected or known breach causes serious risk to the organization) and forwarded immediately to their direct supervisor. Supervisors will forward the report to the PSO who will conduct a Risk Assessment and determine whether to enter reported activities into Breach Notification and Tracking Log.

Date Incident Report completed:_____

Name and Title of person reporting incident:_____

A. Incident

Describe the incident (description of incident/ reason for report, identification of user in question if applicable)*:				
Date and time or estimate of incident*:				
Was incident suspected or known (check one)*:		Suspected		Actual/Known
List application(s)/system(s) violated:				
Location (workstation location):				
What form was the PHI? (check all that apply)		Digital		Verbally Spoken
		Hard Copy		Electronic
What happened to the PHI? (check all that apply)		Taken		Transferred
		Corrupted		Accessed

B. Office Use

Date report received*:					
Violation type (check one):		Administrative		Physical	
		Technical			
Was incident considered unsecured ePHI?		Yes		No	
Has incident been verified?		Yes		No	
When?		By Whom?			
Who has been identified as the individual responsible for committing the incident?*					
Complete Risk Assessment Worksheet. What is the level of probability (high, medium or low) that the PHI was compromised?					
If necessary, has Notification been completed?		Yes. Date:			No
Describe the corrective action plan to mitigate:					
Are sanctions applied?		Yes			No
30 Day Tracking: Has 30 day follow up and tracking been completed?		Yes			No
Is the corrective action plan in place?		Yes			No
Are modifications needed?		Yes			No

* Required information

1.What is the nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification? Include specific details about the type of information: • Clinical, Financial and/or Demographic • Paper and/or Electronic • Spoken Be sure to list elements considered inherently **higher risk** such as: • Social security numbers • Financial/credit card information • Diagnosis of Mental Illness/Drug and Alcohol addiction • HIV diagnosis • Family planning • Genetic testing Include consideration of any types of data with enough variation to allow for someone to commit identity theft.	
1.A. Was the information breached "unsecured PHI?" (Document your answer and rationale.)	
1.B. Was the impermissible acquisition, access, use, or disclosure that of a "Limited Data Set" (LDS)? If so, did the LDS contain birth dates or ZIP codes? NOTE: An LDS not containing birth dates or ZIP codes has been deemed by the Secretary as an automatic "**low probability**."	
Who was the unauthorized person who used the PHI or to whom the disclosure was made?	
Was the PHI actually acquired or viewed? (Document answer and rationale.)	
Does the incident fall under one of the exceptions of the breach definition? (Document your answer and rationale.)	
Describe the extent to which the risk to the PHI has been mitigated.	
Describe any other reasonable factors related to the incident.	
What is your final conclusion based on the response of the above factors? Is the final probability that the PHI was compromised deemed **low**, **medium** or **high**?	

Privacy and Security Policies
Workforce At-A-Glance Guidelines

Question	Guideline(s)	Policy References
Who is the [ABC Provider] privacy and security contact person?	Contact the [ABC Provider] Privacy/Security Official (PSO): [Name] [Address] [Phone/Email]	
Guidelines Regarding Workforce Member Set Up and Termination		

What do I need to do upon initial employment?	• Attend all [ABC Provider] privacy and security training and learn about your organization's Privacy and Security controls and guidelines for handling Protected Health Information.
	• Review and sign all forms and agreements provided by [ABC Provider] including but not limited to:
	  • Acceptable Use Agreement
	  • Remote Worker Set Up Checklist (if applicable)
	• Agree to keep information confidential and follow all [ABC Provider] policies regarding the protection of data and any specific client policies
	• Take steps to implement data backup procedures	

What do I need to do if I terminate (or change) my relationship (employment or independent contract) with [ABC Provider]?	• Back up all confidential/proprietary information and/or ePHI residing on employee or contractor computer. Saved items must be encrypted according to [ABC Provider] policies and procedures. • Relinquish keys, hardware etc. as directed by [ABC Provider] PSO. • Access to confidential/proprietary information and/or ePHI residing on [ABC Provider] network will be terminated or modified by the [ABC Provider] PSO. • Dispose of all extraneous PHI and sensitive patient information by permanently deleting (destroying) it in accordance with [ABC Provider] policies and procedures and as instructed by PSO or his/her designee.	

Question	Guideline(s)	Policy References
Guidelines on Safeguarding Sensitive Information and Protected Health Information		

How should I safeguard sensitive or protected health information residing on?
• Computer
• Mobile device
• Hardcopy
• Removable media
• Databases
	• Review and abide by [ABC Provider] policies and procedures and related resources including but not limited to:
	  • General safeguards policy & procedures
	  • Acceptable Use Agreement
	  • Home Office Worker Checklist
	  • NIST/CMS Secure Remote Access Info (safeguards)
	• Never leave PHI unattended. Lock or log out of workstation before leaving it unattended. Lock away, turnover or otherwise make hard copies containing PHI inaccessible to local foot traffic.
	• Position computer screens so that only authorized persons can read the display
	• Shred paper documents when no longer needed. PHI must be rendered unusable, unreadable or indecipherable to unauthorized individuals before it can be considered disposed of properly.
	• Information (data) stored on removable media should be encrypted and/or password protected. Removable media should be carried separate from laptop or mobile device (when possible, keep jump-drives and other removable media separate from the laptop or other mobile device). All passwords, login instructions and authentication tools should be kept separate from the laptop or mobile device.
	• Do protect computer screen from others
	• Do use password enabled screen savers and logons
	• Do mask PHI when making copies or copy/pasting information into another document
	• Do follow home office set-up guidelines
	• Do encrypt (or password protect) PHI on mobile devices (PDS's, USB's, DVD's and other storage media
	• Do follow the organization's data retention protocols
	• Do advise PSO of any personal databases containing PHI
	• Do watch for unauthorized uses and disclosures, and advise PSO	

Question	Guideline(s)	Policy References
Guidelines on Safeguarding Sensitive Information and Protected Health Information		
How should I safeguard sensitive or protected health information residing on? • Computer • Mobile device • Hardcopy • Removable media • Databases	• Back up device data according to [ABC Provider] policies. Includes only retaining the amount necessary for your files to keep data-at-rest in a secure/encrypted manner. • Do not discuss PHI in open areas or with people who do not have a need to know • Do not transmit PHI by e-mail unless the sender is using a secure e-mail system. • Do not download PHI to a Personal Digital Assistant (PDA) without permission of the Privacy/Security Official. • Do not maintain a separate database containing PHI without specific permission of the Privacy/Security Official	
How should I safeguard sensitive or protected health information when sending faxes?	• Use [ABC Provider] FAX Cover Sheet • Confirm the accuracy of fax numbers by calling intended recipients to check the fax number, notify them the fax is on the way, and request verification of receipt of the fax once received. • When expecting a fax that contains PHI, schedule with the sender when possible so that the fax can be collected upon arrival. • If it is discovered that PHI has been sent to the wrong fax number, the sender must immediately send a second fax to the number that was contacted in error reiterating the confidentiality message above and asking the recipient to telephone the sender immediately to arrange proper disposition of the information. • Any instance of transmitting PHI to the wrong destination number must be reported to the Privacy/Security Officer immediately	

Question	Guideline(s)	Policy References
Frequently Asked Questions		
What should I do if I'm asked to handle PHI (e.g., handling individual rights requests) outside of my usual job/ project functions?	• Review non-standard activities involving the handling of PHI with [ABC Provider] PSO or his/her designee. • Refer to [ABC Provider] policies on general uses & disclosures, authorization documents, and processing individual (patient/ member) rights.	
What should I do if I observe unauthorized acquisition, access, use or disclosure of PHI or other breach?	Report any suspicious privacy/security activities immediately to [ABC Provider] PSO by completing and submitting the [ABC Provider] Privacy/Security Incident Report form.	
What should I do if I receive a complaint about [ABC Provider]'s privacy policies, procedures or actions?	Inform the [ABC Provider] PSO of any privacy or security complaints immediately upon receipt of such complaint. [ABC Provider] PSO will ask that complainant complete and submit a Complaint Form.	
What should I do if I need access to information residing on [ABC Provider] network?	• Contact [ABC Provider] PSO	
What should I do if I experience data loss?	• Avoid data loss by backing up your data according to [ABC Provider] procedures and performing ongoing computer maintenance tasks • Contact [ABC Provider] PSO to report your data loss and to receive instruction on data recovery from backup processes	
What should I do if I have any Privacy or Security related questions?	• Contact [ABC Provider] PSO or his/her designee. (See contact information above.)	

Security Specific Example Templates from SANS

Clean Desk Policy

Free Use Disclaimer: This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.

Things to Consider: Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.

Last Update Status: Updated June 2014

1. **Overview**

   A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. **Purpose**

   The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. **Scope**

   This policy applies to all <Company Name> employees and affiliates.

4. **Policy**

   1.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

   1.2 Computer workstations must be locked when workspace is unoccupied.

   1.3 Computer workstations must be shut completely down at the end of the work day.

   1.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

   1.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

   1.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

   1.7 Laptops must be either locked with a locking cable or locked away in a drawer.

   1.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

   1.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

   1.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

1.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

1.12 Lock away portable computing devices such as laptops and tablets.

1.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up. **Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team (may use "Security Department" of "Technical Resource" in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

None.

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Disaster Recovery Plan Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives <Company Name> a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Company Name> that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

4. Policy

4.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. (See https://www.fema.gov/emergency-planning-exercises for more information).During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.4 Related Standards, Policies and Processes
None.

6. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/Disaster

7. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Email Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated*

1. **Overview**

   Electronic email is pervasively used in almost all industries and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2. **Purpose**

   The purpose of this email policy is to ensure the proper use of <Company Name> email system and make users aware of what <Company Name> deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within <Company Name> Network.

3. **Scope**

   This policy covers appropriate use of any email sent from a <Company Name> email address and applies to all employees, vendors, and agents operating on behalf of <Company Name>.

4. **Policy**

   4.1 All use of email must be consistent with <Company Name> policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

   4.2 <Company Name> email account should be used primarily for <Company Name> business-related purposes; personal communication is permitted on a limited basis, but non-<Company Name> related commercial uses are prohibited.

   4.3 All <Company Name> data contained within an email message or an attachment must be secured according to the *Data Protection Standard.*

   4.4 Email should be retained only if it qualifies as a <Company Name> business record. Email is a <Company Name> business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

   4.5 Email that is identified as a <Company Name> business record shall be retained according to <Company Name> Record Retention Schedule.

   4.6 The <Company Name> email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any <Company Name> employee should report the matter to their supervisor immediately.

   4.7 Users are prohibited from automatically forwarding <Company Name> email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain <Company Name> confidential or above information.

4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct <Company Name> business, to create or memorialize any binding transactions, or to store or retain email on behalf of <Company Name>. Such communications and transactions should be conducted through proper channels using <Company Name>-approved documentation.

4.9 Using a reasonable amount of <Company Name> resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a <Company Name> email account is prohibited.

4.10 <Company Name> employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

4.11 <Company Name> may monitor messages without prior notice. <Company Name> is not obliged to monitor email messages.

4.12 <Company Name> will conduct routine training for all workforce members on the importance of preventing successful phishing attacks via email. These may include embedding links in emails that redirect employees to unsecure websites; inadvertently installing malicious email attachments; spoofing or attempting to obtain sensitive or restricted information over the phone by email by impersonating a known company vendor or IT department. Workforce members are the first line of defense to aid in preventing phishing from causing damage to data or the Company.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.4 Related Standards, Policies and Processes

Data Protection Standard

6. Definitions and Terms

None.

7. Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Updated and converted to new format.

Do's and Don'ts for Secure Exchange from TEFCA- One Page Chart

The following key do's and don'ts have been extracted and simplified to create this handy one page checklist specifically for the Small Provider Practice. The Office for the National Coordinator has provided a document on the Trusted Exchange Framework Common Agreement that includes concepts and principles summarized below - https://www.healthit.gov/buzz-blog/interoperability/trusted-exchange-framework-common-agreement-common-sense-approach-achieving-health-information-interoperability/

Do's and Don'ts

DO:

- Know the data you handle. If it is subject to HIPAA, know how it is created, received, maintained and transmitted throughout your organization. Know if it is encrypted in use, in transmit and at rest.
- Follow industry standard methods for privacy and security compliance (HIPAA/HITECH policies and procedures); for following electronic standard transactions (ASC X12N or NCPDP EDI) and for creating data for exchange with others (Consolidated Clinical Data Architecture (C-CDA) and Meaningful Use protocols) and to be provided to patients (HIPAA Privacy Individual Rights of Access, Amendment, Accounting for Disclosure, Restriction and others).
- Make sure your HIPAA compliance program is comprehensive and up to date, including ongoing training, policy review and risk assessments. Be sure the workforce members know how to identify, handle and report breach situations to business partners and to the authorities.
- Encourage your vendors to follow industry accepted methods of creating data, functionality and sharing (use of Certified Electronic Health Record Technology – Office of the National Coordinator).
- Implement technology in a manner that makes it easy to use and that allows others to connect to data sources, innovate, and use data to support better, more person-centered care, smarter spending, and healthier people.
- Conduct all exchange openly and transparently. Make terms, conditions, and contractual agreements that govern the exchange of data available.
- Clearly specific the permitted uses and disclosures of data handling.
- Ensure that data is exchanged and used in a manner that promotes patient safety, including consistently and accurately matching Health Information to an individual.
- Update clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization.
- Work collaboratively with standards development organizations (SDOs), health systems, and providers to ensure that standards, such as the C-CDA, are implemented so that data can be received and accurately rendered by the receiving healthcare organization. When required by federal or state law, appropriately capture a patients' permission to exchange or use their PHI.
- Ensure that Individuals and their authorized caregivers have easy access to their data including having a way to learn how their information is shared and used.

DON'T:

- Don't Support (or support your vendor's use of) proprietary technologies and data handling and exchange.
- Don't impede the ability of patients to access and direct their own data to designated third parties as required by HIPAA.
- Do not seek to gain competitive advantage by limiting access to individuals' data such as by establishing internal policies and procedures that use privacy laws or regulations as a pretext for not sharing health information.
- Do not implement technology in a manner that permits limiting the sharing of data.
- Do not use methods that discourage or impede appropriate health information exchange, such as throttling the speed with which data is exchanged, limiting the data elements that are exchanged with healthcare organizations that may be a competitor, or requiring burdensome testing requirements in order to connect and share data with another trading partner.
- Do not impose limitations through internal policies and procedures that unduly burden the patient's right to get a copy or to direct a copy of their health information to a third party of their choosing.

Appendix J: Notes

1. https://www.phe.gov/preparedness/planning/cip/Pages/default.aspx
2. 2017 “Taking the Physicians Pulse” Study by the American Medical Association and Accenture
3. 2017 “Taking the Physicians Pulse” Study by the American Medical Association and Accenture
4. Ponemon 6th Annual Benchmark Study on Privacy & Security of Healthcare Data
5. Ponemon 6th Annual Benchmark Study on Privacy & Security of Healthcare Data
6. https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/draft
7. https://csrc.nist.gov/publications/detail/sp/800-184/final
8. https://csrc.nist.gov/publications/detail/sp/800-184/final
9. https://www.ncbi.nlm.nih.gov/books/NBK264167/
10. https://www.congress.gov/bill/114th-congress/house-bill/2029/text
11. NIST SP 800-30