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

Volume 1: Cybersecurity Best Practices for Small Healthcare Organizations

Table of Contents

Introduction

Technical Volume I provides healthcare cybersecurity best practices for small organizations. For the purpose of this volume, small organizations generally do not have dedicated Information Technology (IT) and security staff to implement cybersecurity practices due to limited resources. Without this focus, personnel may have limited awareness of the consequences of cyber threats to patients and the organization and, subsequently, the importance of implementing basic cybersecurity practices.

The primary mission of small healthcare organizations is to provide healthcare to their constituents in the most cost-effective way. Cost-effectiveness enables small organizations to sustain operations, maintain financial viability, justify future investments such as grants and, in the case of for-profit organizations, generate an acceptable profit. Conducting day-to-day business usually involves the electronic sharing of clinical and financial information with patients, providers, vendors, and other players to manage the practice and maintain business operations. For example, small organizations transmit financial information to submit invoices and insurance claims paid by Medicare, Medicaid, Health Maintenance Organizations (HMOs), and credit card companies.

In general, small organizations perform the following functions:

- Clinical care, which includes but is not limited to the sharing of information for clinical care, the transitioning of care (both Social and Clinical), electronic or "E-prescribing" and patient communication through direct secure messaging, and the operation of diagnostic equipment that is connected to a computer network, such as Ultrasound and Pictures Archiving and Communication Systems (PACS).
- Provider practice management, which includes patient access/registration, patient accounting, patient scheduling systems, claims management, and bill processing.
- Business operations, which includes accounts payable, supply ordering, human resource vendors, information technology (IT) operations, staff education, providing protection for patient information, and business continuity and/or disaster recovery in the case of emergencies such as fire, flood or storm damage.

Just as healthcare professionals must wash their hands before caring for patients, healthcare organizations must practice good cyber hygiene in today's digital world by including it as part of every-day, universal precautions. Like hand-washing, a culture of cyber awareness does not have to be complicated or expensive. In fact, simple cybersecurity practices, such as always logging off a computer when finished, are very effective at protecting information that is sensitive and private.

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

Small organizations must comply with multiple legal and regulatory guidelines and requirements. To ensure compliance, they often create an internal infrastructure of personnel and procedures, transmitting sensitive data as needed internally and with authorized external resources. Examples of the issuing entities and/or directives are:

- Electronic Health Records (EHR) interoperability guidelines

- Medicare Access and the Children's Health Insurance Program (CHIP) Reauthorization Act of 2015 (MACRA)/Meaningful Use
- Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology Economic and Clinical Health Act (HITECH)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Substance Abuse and Mental Health Services Administration (SAMHSA)
- The Stark Law as it relates to using the services of an affiliated organization

Many small practices and organizations use third-party IT support and cloud service providers to maintain operations that leverage current technologies. Given the complicated nature of IT and cybersecurity, these third-party IT organizations can be helpful in identifying, assessing and implementing cybersecurity best practices. Your IT support providers should be capable of reviewing the best practices in this publication to determine which are most applicable to your organization.

While the best practices in this volume are tailored to small organizations, it is important to note that small organizations may also benefit from selected best practices in Technical Volume 2, which is tailored to medium and large organizations. Technical Volume 2 is included with this publication and small organizations are encourage to review it as well.

Document Guide - Cybersecurity Best Practices

This volume provides small organizations with a series of best practices to reduce the impact of the five cybersecurity threats identified in Table 1 and discussed in the main document, Cybersecurity for the Healthcare and Public Health Sector.

Threat Description	Impact of Attack
Email Phishing Attack	Potential to deliver malware or conduct credential attacks. Both attacks lead to further compromise of the organization.
Ransomware Attack	Potential to lock up assets (extort) and hold them for monetary ransom. This may result in the permanent loss of patient records.
Loss or Theft of Equipment or Data	Potential for equipment to be lost or stolen, leading to a breach of sensitive information. This may lead to patient identity theft.
Accidental or Intentional Data Loss	Potential for data to be intentionally or unintentionally removed from the organization. This may lead to a breach of sensitive information.
Attack Against Connected Medical Devices that May Affect Patient Safety	Potential for patient safety, treatment and well-being to be impacted by a cyber attack.

Table 1. Five Prevailing Cybersecurity Threats to Healthcare Organizations

For the five cybersecurity threats identified in Table 1, a series of best practices, sub-practices, and baseline practices are presented in this document, as listed in Table 2.

Table 2. Best Practices, Sub-Practices and Baseline Practices are Presented for Small Organizations

Best Practice	Sub Practice	Baseline Practice	Page
Email Protection Systems	1.A	Email System Configuration	7
	1.B	Education	7
	1.C	Phishing Simulation	8
Endpoint Protection Systems	2.A	Basic Endpoint Protection	10
Access Management	3.A	Basic Access Management	12
Data Protection and Loss Prevention	4.A	Policy	14
	4.B	Procedures	15
Asset Management	5.A	Inventory	17
	5.B	Procurement	17
	5.C	Decommissioning	17
Network Management	6.A	Network Segmentation	19
	6.B	Physical Security and Guest Access	19
	6.C	Intrusion Prevention	20
Vulnerability Management	7.A	Vulnerability Management	21
Incident Response	8.A	Incident Response	22
	8.B	ISAC/ISAO Participation	23

Medical Device Security	9.A	Medical Device Security	24
Cybersecurity Policies	10.A	Policies	25

117

118

Cybersecurity Best Practice #1: Email Protection Systems

Most small practices leverage outsourced email providers, rather than establishing a dedicated internal email infrastructure. The best practices discussed below are presented in three parts:

- Email System Configuration: the components and capabilities that should be included within your email system
- Education: how to increase understanding and awareness across your staff on ways to protect your organization against email-based cyberattacks such as phishing and ransomware
- Phishing Simulations: ways to provide training and awareness to your staff on phishing emails

Baseline Practices

A. Email System Configuration

Consider the following controls to enhance the security posture of your email system. Check with your email service provider to ensure these are in place and enabled.

- Avoid "free" or "consumer" based email systems for your business: these systems are not approved to store, process, or transmit protected health information (PHI). We recommend contracting with a server provider that caters to the Healthcare or Public Health Sector.
- Ensure that Basic Spam/Antivirus software solutions are installed, active, and automatically updated wherever possible. Many spam filters can be configured to recognize and block suspicious emails before they reach employee inboxes.
- Deploy multi-factor authentication before enabling access to your email system. This prevents hackers who have obtained a legitimate user's credentials from accessing your system.
- Optimize security settings within your authorized Internet browser(s) to minimize the likelihood that an employee will open a malicious website link, including blocking specific websites or types of websites. Most browsers assess the possibility that the site is malicious, and will send a warning message to the user about the potential danger of accessing a specific site.
- Configure your email system to tag messages as "EXTERNAL" that are sent from outside of your organization. Consider implementing a tag that advises the user to be cautious when opening such emails, for example, "*Stop. Read. Think. This is an External Email*."
- Implement an email encryption module that enables users to send emails securely to external recipients or to protect information that should only be seen by authorized individuals.

B. Education

Implement the following education and awareness activities to assist your employees and partners in protecting your organization against phishing attacks.

Establish and maintain a training program for your workforce that includes a section on phishing attacks. All users in your organization should be able to recognize the phishing techniques in Table 3.

Phishing Technique	Best Practice
Check Embedded Links	Validate that the URL of the link is the same as the link itself. This can be achieved by hovering (but not clicking) your cursor over the email link and reading the website to be accessed.
Look for Suspicious *From:* Addresses	Check received emails for spoofed or misspelled *From:* addresses. For example, if your organization is "ACME" and you receive an email from user@*AMCE*.com, do not open the email without verifying that it is legitimate.
Be cautious with "Urgent" messages	If the email message requires immediate action, especially if it includes a request to access your email or any other account, do not open the email or take any action without verifying that it is legitimate.
Be cautious with "Too Good to be True" messages	If you receive an unexpected message about winning money, or gift cards (such as Amazon gift cards), do not open the email or take any action without verifying that it is legitimate.

Table 3. Train Users to Recognize Phishing Techniques

Be extra careful when sending and receiving emails that contain sensitive and private data, especially patient information. Use of an encryption module minimizes your organization's vulnerability to this information being intercepted by hackers.

C. Phishing Simulations

Implement regular (e.g., monthly or quarterly) anti-phishing campaigns with real-time training for your staff. Many third parties provide low cost, cloud based, phishing simulation tools to train and test your workforce. These tools often include pre-configured training that is easy to distribute for your workforce to complete independently.

Steps for an effective anti-phishing campaign include:

- Direct your IT specialist to send a phishing email to everyone on your staff. Track how many of your employees "bite" or open the email. This enables you to target training to those who demonstrate need as well as to monitor staff and provide opportunities for improvement. It will set the baseline for you to understand how susceptible your organization is and allow you to measure awareness over time.
- While an anti-phishing campaign cannot stop the inbound flow of phishing emails, it will help your organization to identify attacks that bypassed your established email security protections. Your workforce can become "human sensors" to inform you when a real phishing attack is occurring.
- Start your anti-phishing campaigns with easy-to-spot emails that your workforce learns to recognize. Slowly raise the level of sophistication of these simulations to increase the awareness capability of your workforce.

Threats Mitigated

1. Email Phishing Attack
2. Ransomware Attack
3. Accidental or Intentional Data Loss

Cybersecurity Best Practice #2: Endpoint Protection Systems

A small organization's endpoints must be protected. Endpoints include desktops, laptops, mobile devices or other connected hardware devices (e.g., printers, medical equipment). Because technology is highly mobile, computers often are connected and disconnected from an organization's enterprise network. Although attacks against endpoints tend to be delivered via email, as described above, they can be caused by "client-side attacks." Client-side attacks occur when vulnerabilities *within* the endpoint are exploited. Recommended security controls to protect endpoints are presented in Table 4.

Baseline Practice

A. Basic Endpoint Protection Controls

Security Control	Description
Remove administrative accounts	Most users in an organization do not need to be authorized as system administrators with expanded system access and capabilities. Remove administrative access on endpoints to mitigate the damage that can be caused by an attacker who compromises that endpoint. Only authorized personnel within an organization should be allowed to install software applications. Every organization should audit software applications on each endpoint, maintaining a list of approved software applications and removing any unauthorized software as soon as it is detected.
Keep your endpoints patched	Patching (i.e., regularly updating) systems removes vulnerabilities that can be exploited by attackers. Each patch modifies a software application, rendering it more difficult for hackers to maintain programs that are aligned with the most current version of that software application. Configure endpoints to patch automatically and ensure that third-party applications (e.g., Adobe Flash) are patched as soon as possible.
Implement Antivirus software	Like maintaining a safe and infection free operating room for surgery, it is essential to maintain safe and infection free endpoints for your organization to function smoothly. Antivirus software is readily available at low cost and effective at protecting endpoints from computer viruses, malware, spam and ransomware threats. Each endpoint in your organization should be equipped with antivirus software that is configured to update automatically.
Turn on endpoint encryption	Install encryption software on every endpoint that connects to your Electronic Health Records (EHR), especially mobile devices such as laptops. Maintain audit trails of this encryption in case the device is ever lost or stolen. This simple and inexpensive precaution may prevent a complicated and expensive breach. For devices that cannot be encrypted or that are managed by a third-party, implement physical security controls to minimize theft or unauthorized removal. Examples include installation of anti-theft cables, locks on rooms where the devices are located, and the use of badge readers to monitor access to rooms where devices are located.

Enable firewalls	Enable local firewalls for your endpoint device. This is especially important for mobile devices that may be connected to unsecured networks, for example, Wi-Fi networks at coffee shops or hotels.
Enable 2Factor Authentication for remote access	For devices that are accessed off site, leverage technologies that use 2Factor Authentication before permitting the user to access data or applications on the device. Logon with a username and password is often compromised through phishing emails.

Table 4. Effective Security Controls Protect Organization Endpoints.

If your organization leverages an EHR system, or accesses sensitive data through application systems (either on the cloud or on premise), encrypt network access to these applications. Contracts with EHR vendors should include language that requires medical/PHI data to be encrypted both at rest and during transmission between systems. Encryption applications prevent hackers from accessing sensitive data, usually by requiring a "key" to encrypt and/or decrypt data.

Threats Mitigated

1. Ransomware Attack
2. Theft or Loss of Equipment or Data

Cybersecurity Best Practice #3: Access Management

Healthcare organizations of any size need to clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems and endpoints. Just as you may use a name badge at work, proper identification and appropriate access should always be obtained and maintained for proper cybersecurity hygiene.

Baseline Practice

User accounts enable organizations to control and monitor each user's access to and activities on devices, EHRs, email and other third-party software systems. It is essential to protect user accounts and mitigate the risk of cyber threats. Your IT specialist should implement the security controls in Table 5 to manage user access of data, applications and devices.

A. Basic Access Management

Security Control	Description
Establish a unique account for each user	Assign a separate user account to each user in your organization. Train and continuously communicate to users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or email access (e.g., Gmail, Yahoo, Facebook).
Limit the use of shared or generic accounts	The use of shared or generic accounts should be avoided. If required, train and continuously communicate to users that they must "sign out" upon completion of activity or whenever they leave the device, even for a moment. Passwords should be changed after each use. Sharing accounts exposes an organization to greater vulnerabilities. For example, the complexity of updating passwords for multiple users on a shared account may result in a compromised password remaining active and allowing unauthorized access over an extended period of time.
Tailor access to the needs of each user	Tailor access for each user based on the user's specific workplace requirements. Most users require access to select common systems, such as email and file servers. This is usually called provisioning.
Terminate user access as soon as the user leaves the organization	When an employee leaves your organization, ensure that procedures are executed to terminate the employee's access immediately. This is very important for organizations that use cloud-based systems where access is based on credentials. You don't want former employees to access your patient data and other sensitive information after they have left the organization! If an employee changes jobs within the organization, it's important to terminate access required for the employee's former position before granting access based on the requirements for the new position.

Role based access	As user accounts are established, the appropriate authorization must be granted to access the organization's various computers and programs. Consider leveraging the principle of Minimum Necessary associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish the user's job or role in the organization. This limits the organization's exposure to unauthorized access and loss or theft of data if the user's identity or access is compromised.
Configure systems and endpoints with automatic lock and log-off	Configure systems and endpoints to automatically lock and log off users after a predetermined period of inactivity, such as 15 minutes.
Implement Single-Sign On	Implement Single-Sign On systems that allow a user to sign onto the network once with subsequent access properly managed. This allows the organization to maintain access centrally.
Implement Multi-Factor Authentication for the Cloud	Implement Multi-Factor Authentication for cloud-based systems used by your organization to store or process sensitive data, such as EHRs. This mitigates the risk of access by unauthorized users.

Table 5. Security Controls Enable Organizations to Manage User Access to Data

To monitor compliance with these practices, implement access management procedures to track and monitor user access to computers and programs. These procedures will ensure the consistent provisioning and control of access throughout your organization. Examples of these standard operating procedures can be found in *Appendix I of the main document*.

Threats Mitigated

1. Ransomware Attack
2. Accidental or Intentional Data Loss
3. Attack Against Connected Medical Devices that May Affect Patient Safety

Cybersecurity Best Practice #4: Data Protection and Loss Prevention

A security breach is the loss or exposure of sensitive data – information that is relevant to the organization's business or patient's PHI. Impacts to the organization can be profound if data are corrupted, lost or stolen. This includes the inability of users to complete work accurately or on a timely basis and the potentially devastating consequences to patient treatment and well-being. Establishing good cybersecurity practices to protect data and prevent data loss protects the organization and its patients.

Baseline Practice

Preventing the loss of sensitive data can be accomplished in several ways. It is based on understanding where data resides, where it is accessed, and how it is shared. Throughout this document, there are many tips to protect data and prevent loss. Information in this section is organized by policy, procedures and education.

A. Policy

First and foremost, set the expectation for how your workforce is expected to manage the sensitive data at their fingertips. Most healthcare employees work with sensitive data on a daily basis and it's easy to forget the importance of being vigilant with its protection. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of data that is lost or compromised.

Establish a data classification policy that segments data types into Sensitive, Internal Use, and Public Use categories. For each category, identify the types of records. For example, the Sensitive data category should include PHI, social security numbers, credit card numbers, and other information that must comply with regulations, may be used to commit fraud, or may damage the organization's reputation. Table 6 suggests data classifications with descriptions.

Classification	Description
Highly Sensitive	Data that can be used easily to commit financial fraud or cause significant damage to the organization's reputation. Examples of such data for patients include Social Security Numbers (SSN), credit card numbers, mental health information, substance abuse information, and sexually transmitted infections/disease information. Access to this data should be restricted to users who require access and demonstrate proper authentication at logon. This data must be managed in compliance with applicable regulatory requirements.
Sensitive	All other PHI, especially data associated with the Designated Record Set, Clinical Research data, Insurance information, human/employee data, and organizational board materials.
Internal	Data that should be protected yet is not considered sensitive. Examples include organization policies and procedures, contracts, business plans, corporate strategy and business development plans, and internal business communications.

Public	All other data that has been sanitized and approved for distribution to the public with no restrictions on use.

Prohibit the use of unencrypted storage, such as thumb drives, mobile phones, or computers. Require encryption of these mobile storage mediums before use.

B. Procedures

In addition to implementing policies to define expected workforce behaviors, it's important to establish procedures to manage sensitive data. These procedures facilitate data management by instilling consistency, reducing errors, and providing clear and explicit instructions. The following methods may be used to develop and implement data management procedures:

- Use the classifications in Table 6 to establish data usage procedures. Identify authorized users of sensitive data, and the circumstances under which this data may be disclosed.
- Train your workforce to comply with organizational procedures and ONC guidance when transmitting PHI through email. Encrypt PHI that is sent using email or text, unless patients expressly authorize their PHI to be emailed or texted to them.
- When emailing PHI, use a secure messaging application such as Direct Secure Messaging (DSM), which is a nationally adopted secure email protocol and network to transmit PHI. DSM can be obtained from EHR vendors and other HIE systems. It was developed and adopted through the Meaningful Use program, and a significant number of medical organizations now participate in these trusted networks. When texting PHI, use a secure texting system.
- Implement Data Loss Prevention Technologies to mitigate the risk of unauthorized access to PHI. Check with your IT provider to determine if this is feasible for your organization, or reference Cybersecurity Best Practice #4: Data Protection and Prevention in Technical Volume 2, for details on the applicability of these technologies to your organization.
- Train your staff to never back up data on non-controlled storage devices or personal cloud services. For example, do not permit employees to configure any workplace mobile device to back up to a personal computer unless that computer has been configured to comply with your organization's encryption and data security standards.
    - Note: Leveraging the cloud for backup purposes is fine if you have established a business associate agreement with the cloud vendor and verified the security of their systems.
- Remember to protect archived data, such as records for previous patients. It is important to monitor access to this data, which may be used infrequently, so that a cyberattack is detected immediately.
- Ensure that obsolete data are removed or destroyed properly and cannot be accessed by cyber-thieves. Much like fully shredding paper, medical records, or burning paper financial paperwork, digital data must be properly disposed of to ensure it cannot be inappropriately recovered. Discuss options for properly disposing outdated or unneeded data with your IT support. Do not assume that deleting or erasing data means that it is destroyed. See *Appendix I of the main document* for a sample data destruction form that can be used to ensure data are disposed of appropriately.

- Retain and maintain only data that is required by your organization to complete work or comply with records storage requirements. Minimize your organization's risk footprint by removing unnecessary data regularly.

C. Education

It is important to train your workforce to comply with your organization's policies. At minimum, provide annual training on the most salient policy considerations, such as the use of encryption and PHI transmission restrictions.

Threats Mitigated

1. Ransomware Attack
2. Loss or Theft of Equipment or Data
3. Accidental or Intentional Data Loss

Cybersecurity Best Practice #5: Asset Management

Organizations manage IT assets using processes referred to collectively as IT Asset Management (ITAM). ITAM is critically important to understanding and ensuring that cyber hygiene controls are maintained across all assets in your organization.

ITAM processes should be conducted for endpoints, servers, and networking equipment. ITAM processes enable organizations to understand their devices, and the best options to secure them. Additionally, the best practices described in this section may be used to support many of the best practices described in other sections of this volume. It can be difficult to implement and sustain best practices for asset management. ITAM processes should be part of daily IT operations and encompass the lifecycle of each IT asset from procurement to deployment and maintenance and, finally, to the decommissioning (i.e., replacement or disposal) of the device.

Baseline Practice

A. Inventory

A complete and accurate inventory of the IT assets in your organization facilitates the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet. The following fields should be captured for each device:

- Asset ID (primary key)
- Host Name
- Purchase Order
- Operating System
- Media Access Control (MAC) Address
- IP Address
- Deployed to (User)
- User Last Logged On
- Purchase Date
- Cost
- Physical Location

Remember to include all devices owned by your organization, including workstations, laptops, servers, portable drives, mobile devices, tablets and smart phones.

B. Procurement

Once you have established your ITAM spreadsheet, it is important to record the acquisition of each new IT asset when it is acquired. This requires establishing standard operating procedures. Generally, it's advisable to assign the responsibility of collecting information on new assets to the purchaser within your organization.

C. Decommissioning

IT assets that are no longer functional or required should be decommissioned in accordance with your organization's procedures. Small organizations often contract with an outside service provider that specializes in secure destruction processes. This ensures that all data, especially sensitive data, are properly removed from a device before it is turned over to other parties.

Additionally, your standard operating procedures should ensure that you record the decommissioning of each device. If you use a service provider to decommission or destroy devices, record the certification of destruction so there is never a question about what happened with it!

Threats Mitigated

1. Ransomware Attack
2. Loss or Theft of Equipment or Data
3. Accidental or Intentional Data Loss
4. Attack Against Connected Medical Devices that May Affect Patient Safety

Cybersecurity Best Practice #6: Network Management

Computers communicate with other computers through networks. These networks are connected through a connection that is wireless or a wired (e.g., a network cable) and must be established before systems can interoperate. Networks that are established in an insecure manner increase an organization's exposure to cyberattack.

Proper cybersecurity hygiene ensures that the network is secure and that all devices access the network in a safe and secure manner. If network management is provided by an IT support vendor, the organization must understand key aspects of proper network management and ensure that they are included in contracts for these services.

Baseline Practice

A. Network Segmentation

Configure networks to restrict access between devices to that which is required to successfully complete work. This will limit the spread of any cyberattack on your network.

- Disallow all Internet bound access into your organization's network. If you host servers that interface with the Internet, consider using a third-party vendor to provide security as part of the hosting service.
- Restrict access to assets with potentially high impact in the event of compromise. This includes medical devices and Internet of Things (IoT) items (e.g., security cameras, badge readers, temperature sensors, building management systems).
- Just as you might restrict physical access to different parts of your medical office, it's important to restrict the access of third-party entities, including vendors, to separate networks. Allow them to connect only through tightly controlled interfaces. This limits the exposure to and impact of a cyberattack on your organization as well as the third-party entity.
- Establish and enforce network traffic restrictions. These restrictions may apply to applications and websites as well as to users in the form of role-based controls. Restricting access to personal websites (e.g., social media, couponing, online shopping) limits exposure to browser add-ons or extensions, reducing the risk of cyberattacks.

B. Physical Security and Guest Access

Just as network devices need to be secured, physical access to the network equipment should be secured and restricted to IT professionals. Configure physical rooms and wireless networks to allow Internet access only.

- Keep data and network closets locked always. Grant access using badge readers rather than traditional key locks.
- Disable network ports that are not in use. Maintain network ports as inactive until an activation request is authorized. This minimizes the risk of an unauthorized user "plugging in" to an empty port to access to your network.
- Establish guest networks in conference rooms or waiting areas that separate the organizational data and systems. Validate that guest networks are configured to access authorized guest services only.

C. Intrusion Prevention

Implement intrusion prevention systems as part of your network protection plan to provide ongoing protection for your organization's network. Most modern firewall technologies that are used to segment your network include an Internet Partner Services (IPS) component. Implementing this component and configuring these systems to update automatically reduces your organization's vulnerability to known cyberattacks. Configure your intrusion prevention systems to stop well-known attacks and to automatically update their signatures.

Intrusion prevention systems are available as part of a next generation technology/network suite of applications, or as a stand-alone product that may be added to existing networks.

Threats Mitigated

1. Ransomware Attack
2. Loss or Theft of Equipment or Data
3. Accidental or Intentional Loss of Data
4. Attack Against Medical Device that May Affect Patient Safety

Cybersecurity Best Practice #7: Vulnerability Management

Vulnerability management is the process used by organizations to detect technology flaws that may be exploited by hackers. This process uses a scanning capability, often provided by an EHR or IT support vendor, to proactively scan devices and systems in your organization.

Baseline Practice

A. Vulnerability Management

As discussed in the introduction to this document, weak passwords, default passwords, outdated software, and other technology flaws identified by these scans are commonly referred to as vulnerabilities. During the process of conducting a scan, organizations may be presented with large amounts of data. The urgent need to classify, evaluate, and prioritize remediation of these flaws before an attacker can exploit them may require significant time and resources.

Vulnerability management best practices include:

- Schedule and conduct scans on servers and systems within your control/inventory to proactively identify technology flaws.
- Remediate flaws based on the severity of the identified vulnerability. This method is considered an "unauthenticated scan." The scanner has no extra sets of privileges to the server. It queries a server based on ports that are active and present for network connectivity. Each server is queried for vulnerabilities based upon the level of sophistication of the software scanner.
- Conduct web application scanning for Internet-facing webservers, such as a web-based patient portal. Specialized vulnerability scanners can interrogate a running web application to identify vulnerabilities within the application design.
- Conduct routine patching of security flaws within servers, applications (including web applications), and third-party software. Maintain software at least monthly, implementing patches distributed by the vendor community, if this isn't done automatically. A robust patch management mitigates vulnerabilities associated with obsolete software versions, which are often easier for hackers to exploit.

Threats Mitigated

1. Ransomware Attack
2. Accidental or Intentional Data Loss
3. Attack Against Connected Medical Devices that May Affect Patient Safety

Cybersecurity Best Practice #8: Incident Response

Incident response is the ability to discover cyberattacks on the network and prevent them from causing data breaches or loss. This is often referred to as the standard "blocking and tackling" of Information Security. Many types of security incidents occur on a regular basis across organizations of all sizes. Two common incidents are 1) the installation and detection of malware, and 2) the influx of phishing attacks that include malicious payloads (via attachments and links). Though neither of these incidents directly results in a data breach or loss, each event enables data breaches or loss to occur through subsequent events.

Baseline Practice

A. Incident Response

Small organizations are often challenged by incident response management. Incident response procedures may not be established. Employees who rarely encounter cyberattacks may not remember what to do. Members of the management team may not know who must be contacted to obtain or provide information about the incident. In many cases, there are no dedicated Information Security professionals within the small organization, and the reliance on the IT department becomes even more important. A common concern is the fear of penalties if the organization contacts someone to rectify a security incident.

Cyberattacks may have severe consequences for healthcare organizations. Patient safety, treatment, well-being and privacy may be comprised. Financial and credibility impacts to the organization may cause irreparable damage.

Establish and implement an Incident Response Plan. Before an incident occurs, make sure you understand who will lead your incident investigation. Additionally, make sure you understand which personnel will support the leader during each phase of the investigation. At minimum, you should identify the top security expert who will provide direction to the supporting personnel. Ensure the leader is fully authorized to execute all tasks and activities required to complete the investigation. A sample Incident Response plan is provided in *Appendix I of the main document*. Examples of actions to respond to incidents are described in Table 7.

Incident Response Execution: Once your Incident Response Plan is implemented, ensure compliance with the plan elements. At minimum, your plan should describe steps to be followed in the event of malware downloaded on a computer or upon receipt of a phishing attack.

Incident	Response Recommendation
Malware	• Re-image, rebuild, or reset computer to a known good state. • Do not trust "malware cleaning" tools until they are verified to function as described.
Phishing	• Identify malicious email messages and delete from mailboxes. • Proactively block websites (URLs) referenced in "click attacks." • Identify malware that might have been installed on computers. Execute malware play if run.

Table 7. Implementing Incident Response Recommendations Mitigates Risk of a Data Breach or Loss

B. ISAC/ISAO Participation

Establish a method to receive notifications about cyber threats that are actively targeting other organizations. The most effective way to do this is to join an Information Sharing and Analysis Organization (ISAO) or Information Sharing and Analysis Center (ISAC). Participating in an appropriate ISAO or ISAC is a great way to manage incident response. As directed by Executive Order 13691, when a member organization provides an ISAO with information about cyber-related breaches, interference, compromise or incapacitation, the ISAO must:

- Protect the individuals' privacy and civil liberties,
- Preserve business confidentiality, and
- Safeguard the information being shared.

ISAOs and ISACs establish a community of professionals who are prepared to respond to the same cyber threats. By joining this community, security and IT professionals bridge knowledge gaps with information provided by their peers via the ISAC/ISAO. ISACs and ISAOs tend to focus on a specific vertical (such as the National Healthcare Information Sharing and Analysis (NH-ISAC) within Healthcare) or community (such as the Population Health ISAO). In all cases, the primary function of these associations is to establish and maintain a channel for the purpose of sharing cyber intelligence.

Threats Mitigated

1. Phishing Attack
2. Ransomware Attack
3. Loss or Theft of Equipment
4. Accidental or Intentional Data Loss
5. Attack Against Connected Medical Devices that May Affect Patient Safety

Cybersecurity Best Practice #9: Medical Device Security

Medical devices are essential to diagnostic, therapeutic and treatment practices. These devices deliver significant benefits and are successful in the treatment of many diseases.

As technology advances and healthcare environments migrate to digitized systems, so do medical devices. For many reasons, it is highly desirable to interface medical devices directly with clinical systems. Automating data collection from these devices reduces the labor burden and exposure to human error that results from manual input of data. Automatic data interfacing also reduces errors that can occur when transcribing data from the medical device to the clinical system. Automated control of device instrumentation delivers the most accurate treatment possible to the patient. For example, bedside vital signs monitors are networked to centralized nursing station displays and alarms, and infusion pumps are networked to servers to distribute pump drug libraries and download usage data.

As with all technologies, medical device benefits are accompanied by cybersecurity challenges. Increasingly, new threats include "hacking" medical devices to cause harm by operating them in an unintended manner. For example, the 2015 document "How to Hack an Infusion Pump" describes how an infusion pump can be controlled remotely to modify the dosage of drugs, threatening patient safety and well-being.

Cybersecurity vulnerabilities are introduced when medical devices are connected to a network or computer to process required updates. Many medical devices are managed remotely by third-party vendors, which increases the attack footprint.

Baseline Practice

A. Medical Device Security

If your organization connects medical devices to a network, consider the best practices recommended in *Cybersecurity Best Practice #9: Medical Device Security* in Technical Volume 2.

Threats Mitigated

1. Attacks Against Connected Medical Devices that May Affect Patient Safety

Cybersecurity Best Practice #10: Cybersecurity Policies

Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyberattacks. They set expectations and foster a consistent adoption of behaviors by your workforce. With clearly articulated cybersecurity policies, your employees, contractors and third-party vendors know which data, applications, systems and devices they are authorized to access and the consequences of unauthorized access attempts.

Baseline Practice

A. Policies

Policies are established first and supplemented with procedures that enable the policy to be fulfilled. Policies describe what is expected, procedures describe how that expectation is met.

For example, a policy is established that privacy and security training will be completed by all users. The policy specifies that training courses will be developed and maintained for these two topics, that all users will complete this training, that a particular method will be used to conduct the training, and that specific actions will be taken to address non-compliance with the policy. The policy does not describe how your workforce will complete the training, nor does it identify who will develop the courses. Your procedures section provides these details, for example, clearly stating that your privacy and security professionals will develop and release the courses. Additionally, the procedures describe the process to access the training.

Examples of policy templates are provided in *Appendix I of the main document*.

Policy examples with descriptions and recommended users are provided in Table 8.

Policy Name	Description	User Base
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for conducting security practices, setting and establishing policy, and implementing security practices.	• All users
Education and Awareness	Describe the mechanisms by which the organizational workforce will be trained on cybersecurity practices, threats and mitigations.	• All users • Cybersecurity Department
Acceptable Use / Email Use	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how email will be used to complete work.	• All users
Data Classification	Describe how data will be classified with usage parameters for each classification.	• All users
Personal Devices	Describe the organization's position on usage of personal devices – also referred to as Bring Your	• All users

	Own Device (BYOD). If usage of personal devices is permitted, describe the expectations for how the devices will be managed.	
Laptop, Portable Device, and Remote Use	Describe the policies that relate to mobile device security and how these devices may be used in a remote setting.	• All users • IT Departments
Incident Reporting and Checklist	Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.	• All Users • Cybersecurity Department

Table 8. Effective Policies Mitigate the Risk of Cyberattacks

Threats Mitigated

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

Appendix A: 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
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
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

549