Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Table of Contents

List of Tables

Introduction

Small health care organizations tend to have limited resources for managing their cybersecurity practices, but they are no less subject to cyberattacks. Indeed, the five threats identified in the Main Document can be very disruptive to small organizations. For example, if a small provider practice loses a laptop with unencrypted personal health information (PHI), a publicized breach could result. Such a breach could have consequences for both the provider's patients and the practice's reputation.

Technical Volume 1 provides health care cybersecurity practices for small health care organizations. For the purpose of this volume, *small organizations* generally do not have dedicated information technology (IT) and security staff dedicated to implementing cybersecurity practices due to limited resources. Personnel may consequently have limited awareness of the severity of cyber threats to patients and to the organization, and thus awareness of the importance of cybersecurity.

The primary mission of small healthcare organizations is to provide health care to their patients 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 sharing information for clinical care, transitioning care (both social and clinical), electronic or "e-prescribing," communicating with patients through direct secure messaging, and operating diagnostic equipment connected to a computer network, such as ultrasound and pictures archiving and communication systems (PACS).
- *Provider practice management*, which includes patient access and registration, patient accounting, patient scheduling systems, claims management, and bill processing.
- *Business operations*, which include accounts payable, supply chain, human resources, IT, staff education, protecting patient information, and business continuity or disaster recovery.

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

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

Small health care organizations must comply with multiple legal and regulatory guidelines and requirements. They often ensure compliance by creating an internal infrastructure of personnel and procedures to govern the transmission of sensitive data as needed internally and with authorized external resources. For example, organizations may be subject to directives from:

- 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 health care 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 practices. Your IT support providers should be capable of reviewing the practices in this publication to determine which are most applicable to your organization.

The practices in this volume are tailored to small organizations, but such organizations may also benefit from selected practices in Technical Volume 2, which focuses on medium and large organizations and is included with this publication. Small organizations may benefit from the cybersecurity practices in both volumes.

Document Guide: Cybersecurity Practices

This volume provides small health care organizations with a series of cybersecurity practices to reduce the impact of the five cybersecurity threats identified in Table 1 and discussed in the Main document. (See the Main document for detailed definitions and descriptions of each threat.)

Table 1. Five Prevailing Cybersecurity Threats to Health Care Organizations

Threat	Potential Impact of Attack
E-mail phishing attack	Malware delivery or credential attacks. Both attacks further compromise the organization.
Ransomware attack	Assets locked and held for monetary ransom (extortion). May result in the permanent loss of patient records.
Loss or theft of equipment or data	Breach of sensitive information. May lead to patient identity theft.
Accidental or intentional data loss	Removal of data from the organization (intentionally or unintentionally). May lead to a breach of sensitive information.
Attacks against connected medical devices that may affect patient safety	Undermined patient safety, treatment, and well-being.

The cybersecurity practices and sub-practices to mitigate these threats are listed in Table 2 below.

Table 2. Cybersecurity Practices and Sub-Practices for Small Organizations

Cybersecurity Practice	Sub-Practice for Small Organizations		Page
E-mail Protection Systems	1.S.A	E-mail System Configuration	6
	1.S.B	Education	7
	1.S.C	Phishing Simulation	7
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	9
Access Management	3.S.A	Basic Access Management	11
Data Protection and Loss Prevention	4.S.A	Policy	13
	4.S.B	Procedures	14
	4.S.C	Education	15
Asset Management	5.S.A	Inventory	16
	5.S.B	Procurement	17
	5.S.C	Decommissioning	17
Network Management	6.S.A	Network Segmentation	18
	6.S.B	Physical Security and Guest Access	18

Cybersecurity Practice #1: E-mail Protection Systems

Most small practices leverage outsourced third-party e-mail providers, rather than establishing a dedicated internal e-mail infrastructure. The e-mail protection practices in this section are presented in three parts:

- *E-mail system configuration*: the components and capabilities that should be included within your e-mail system
- *Education:* how to increase staff understanding and awareness of ways to protect your organization against e-mail–based cyberattacks such as phishing and ransomware
- *Phishing simulations:* ways to provide staff with training on and awareness of phishing e-mails

Sub-Practices for Small Organizations

1.S.A	***E-mail System Configuration***	***NIST FRAMEWORK REF:*** PR.DS-2, PR.IP-1, PR.AC-7

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

- Avoid “free” or “consumer” e-mail systems for your business; such systems are not approved to store, process, or transmit PHI. We recommend contracting with a service provider that caters to the health care 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 e-mails before they reach employee inboxes.
- Deploy multifactor authentication (MFA) before enabling access to your e-mail system. MFA prevents hackers who have obtained a legitimate user’s credentials from accessing your system.
- Optimize security settings within your authorized internet browser(s), including blocking specific websites or types of websites, to minimize the likelihood that an employee will open a malicious website link. Most browsers assess the possibility that a site is malicious and send warning messages to users attempting to access potentially dangerous sites.
- Configure your e-mail 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 e-mails, for example, “*Stop. Read. Think. This is an External E-mail*.”
- Implement an e-mail encryption module that enables users to securely send e-mails to external recipients or to protect information that should only be seen by authorized individuals.
- Provision every employee with a unique user account that is tied to a unique e-mail address. These accounts and e-mail addresses should not be shared, and should be de-provisioned when the employee leaves the organization.

1.S.B	***Education***	***NIST FRAMEWORK REF:*** PR.AT-1

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.

Table 3. Phishing Techniques

Phishing Technique	Description
Check embedded links	Validate that the URL of the link matches the text of the link itself. This can be achieved by hovering (not clicking) your mouse cursor over the link to view the URL of the website to be accessed.
Look for suspicious *From:* addresses	Check received e-mails for spoofed or misspelled *From:* addresses. For example, if your organization is "ACME" and you receive an e-mail from user@*AMCE*.com, do not open the e-mail without verifying that it is legitimate.
Be cautious with "urgent" messages	If the e-mail message requires immediate action, especially if it includes a request to access your e-mail or any other account, do not open the e-mail 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, do not open the e-mail or take any action without verifying that it is legitimate.

- Leverage an encryption module within your e-mail system to minimize the risk of information being intercepted by hackers
- Be extra careful when sending and receiving e-mails that contain sensitive and private data, especially PHI.

1.S.C	***Phishing Simulations***	***NIST FRAMEWKORK REF:*** PR.AT

Steps for an effective anti-phishing campaign include:

- 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. Such tools often include pre-configured training that is easy to distribute and that your workforce can complete independently.

- Direct your IT specialist to send a phishing e-mail to everyone on your staff. Track how many of your employees “bite”, or open the e-mail. This enables you to target training to those who demonstrate need, . This technique will also allow you to understand how susceptible your organization is and to set a baseline that you can use to measure changes in awareness over time.
- Start your anti-phishing campaigns with easy-to-spot e-mails that your workforce learns to recognize. Slowly increase the sophistication of these simulations to improve the detection capability of your workforce.

Although an anti-phishing campaign cannot stop the inbound flow of phishing e-mails, it will help your organization identify any attacks that bypass established e-mail security protections. Educated and aware staff can become “human sensors” to inform you when a real phishing attack is occurring.

Threats Mitigated

1. E-mail phishing attack
2. Ransomware attack
3. Insider, accidental or intentional data loss

Cybersecurity Practice #2: Endpoint Protection Systems

A small organization's endpoints must be protected. Endpoints include desktops, laptops, mobile devices, and other connected hardware devices (e.g., printers, medical equipment). Because technology is highly mobile, computers are often connected to and disconnected from an organization's network. Although attacks against endpoints tend to be delivered via e-mail, as described above, they can also be delivered as *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.

Sub-Practices for Small Organizations

2.S.A	***Basic Endpoint Protection Controls***	***NIST FRAMEWORK REF:*** PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3

Table 4. Effective Security Controls to Protect Organization Endpoints

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. 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	Antivirus software is readily available at low cost and is 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.

Security Control	Description
Turn on endpoint encryption	Install encryption software on every endpoint that connects to your EHR system, especially mobile devices such as laptops. Maintain audit trails of this encryption in case a 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 devices. Firewalls are especially important for mobile devices that may be connected to unsecured networks, such as Wi-Fi networks at coffee shops or hotels.
Enable Multifactor authentication for remote access	For devices that are accessed off site, leverage technologies that use multi-factor authentication before permitting users to access data or applications on the device. Logins that use only a username and password are often compromised through phishing e-mails.

If your organization leverages an EHR system or accesses sensitive data through application systems (either on the cloud or on site), 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.

Finally, educate your employees on the need to report the loss or theft of any endpoints within their control to the appropriate team inside the organization. For example, if a backpack with a laptop is stolen at an airport, the employee should report the theft promptly to the organizational leadership.

Threats Mitigated

1. Ransomware attack
2. Loss or theft of equipment or data

Cybersecurity Practice #3: Access Management

Health care organizations of all sizes 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 to identify yourself in the physical work environment, cybersecurity access management practices can help ensure that users are properly identified in the digital environment, as well.

Sub-Practices for Small Organizations

User accounts enable organizations to control and monitor each user's access to and activities on devices, EHRs, e-mail, and other third-party software systems. It is essential to protect user accounts to 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.

3.S.A	***Basic Access Management***	***NIST FRAMEWORK REF:*** PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7

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

Security Control	Description
Establish a unique account for each user	Assign a separate user account to each user in your organization. Train and regularly remind 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 e-mail 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 shared accounts are required, train and regularly remind 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 organizations 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 common systems, such as e-mail and file servers. Implementing tailored access is usually called *provisioning*.

Security Control	Description
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. Prompt user termination prevents former employees from accessing patient data and other sensitive information after they have left the organization. This is very important for organizations that use cloud-based systems where access is based on credentials, rather than physical presence at a particular computer. Similarly, if an employee changes jobs within the organization, it is important to terminate access related to the employee's former position before granting access based on the requirements for the new position.
Provide role-based access	As user accounts are established, the accounts must be granted access to the organization's computers and programs, as appropriate to each user. Consider following the "minimum necessary" principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization. This limits the organization's exposure to unauthorized access, loss, and 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 automatically manage access to all software and tools once users have signed onto the network. Such systems allows the organization to centrally maintain and monitor access.
Implement MFA for the cloud	Implement MFA authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

To monitor compliance with the practices listed in Table 5, 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 such standard operating procedures can be found in *Appendix G* of the Main document*.*

Threats Mitigated

1. Ransomware attack
2. Insider, accidental or intentional data loss
3. Attacks against connected medical devices that may affect patient safety

Cybersecurity Practice #4: Data Protection and Loss Prevention

A *security breach* is the loss or exposure of sensitive data, including information relevant to the organization's business and patient PHI. Impacts to the organization can be profound if data are corrupted, lost, or stolen. Security breaches may prevent users from completing work accurately or on time, and could result in potentially devastating consequences to patient treatment and well-being. Thus, good data protection and loss prevention practices in turn protect the organization and its patients.

Sub-Practices for Small Organizations

The loss of sensitive data can be prevented in several ways. Data loss prevention is based on understanding where data resides, where it is accessed, and how it is shared. Throughout this document, there are many tips to protect data and prevent loss. This section focuses on loss prevention policies, procedures, and education.

4.S.A	***Policies***	***NIST FRAMEWORK REF:*** ID.GV-1, ID.AM-5

- Set the expectation for how your workforce is expected to manage the sensitive data at their fingertips. Most health care employees work with sensitive data on a daily basis, so it is easy to forget how important it is to remain vigilant about data protection. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost or compromised data.
- Establish a data classification policy that categorizes data as, for example, Sensitive, Internal Use, or Public Use. Identify the types of records relevant to each category. For example, the Sensitive data category should include PHI, social security numbers (SSNs), 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 and describes possible data classifications.

Table 6. Example Data Classification Structure

Classification	Description
Highly Sensitive	Data that can easily be used to commit financial fraud or to cause significant damage to the organization's reputation. Examples of such data for patients include SSNs, credit card numbers, mental health information, substance abuse information, and sexually transmitted infection information. Access to these data should be restricted to users who require it and who demonstrate proper authentication at login. Such data must be managed in compliance with applicable regulatory requirements.

Classification	Description
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 are not considered sensitive. Examples include organization policies and procedures, contracts, business plans, corporate strategy and business development plans, and internal business communications.
Public	All data that have 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.

4.S.B	***Procedures***	***NIST FRAMEWORK REF:*** ID.GV-1, PR.AT-1, PR.DS-2, PR.DS-5, PR.DS-1, PR.IP-6, ID.GV-3

Procedures to manage sensitive data can ensure consistency, reduce errors, and provide clear and explicit instructions. Such procedures should therefore be implemented alongside data access policies. 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 such data may be disclosed.
- Train your workforce to comply with organizational procedures and ONC guidance when transmitting PHI through e-mail. Encrypt all PHI sent via e-mail or text. However, patients can request and receive access to their PHI via unencrypted electronic communications following a brief warning to the patient that unencrypted communications could be accessed by a third-party in transit and the patient confirms that they still want to receive the unencrypted communication.
- When e-mailing PHI, use a secure messaging application such as Direct Secure Messaging (DSM), which is a nationally adopted secure e-mail protocol and network for transmitting PHI. DSM can be obtained from EHR vendors and other health information exchange systems. It was developed and adopted through the Meaningful Use program, and many medical organizations nationwide now use DSM 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 Practice #4: Data Protection and Prevention** in *Technical Volume 2* for details on the applicability of these technologies to your organization.

- Train staff never to back up data on uncontrolled 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 acceptable if you have established an agreement with the cloud vendor and verified the security of the vendor’s systems.

  - Remember to protect archived data, such as records for previous patients. to It is important to monitor access to this data, which may be used infrequently, so that a cyber-attack is detected immediately.
  - Ensure that obsolete data are removed or destroyed properly so they cannot be accessed by cyber-thieves. Just as paper medical and financial records must be fully destroyed by shredding or burning, digital data must be properly disposed of to ensure that they cannot be inappropriately recovered. Discuss options for properly disposing of outdated or unneeded data with your IT support. Do not assume that deleting or erasing files means that the data are destroyed. See *Appendix G* of the Main document for a sample data destruction form that can be used to ensure that data are disposed of appropriately.
  - Retain and maintain only data that your organization requires to complete work or comply with records storage requirements. Minimize your organization’s risk by regularly removing unnecessary data.

4.S.C	***Education***	***NIST FRAMEWORK REF:*** PR.AT

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

Threats Mitigated

1. Ransomware attack
2. Loss or theft of equipment or data
3. Accidental or intentional data loss

Cybersecurity Practice #5: Asset Management

Organizations manage IT assets using processes referred to collectively as *IT asset management (ITAM)*. ITAM is critical to ensuring that the appropriate cyber hygiene controls are maintained across all assets in your organization.

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

Sub-Practices for Small Organizations

5.S.A	***Inventory***	***NIST FRAMEWORK REF:*** ID.AM-1

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 information 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.

5.S.B	***Procurement***	***NIST FRAMEWORK REF:*** ID.AM-6

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

5.S.C	***Decommissioning***	***NIST FRAMEWORK REF:*** PR.IP-6, PR.DS-3

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 specializing in secure destruction processes. Such providers can ensure 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 to it.

Threats Mitigated

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

Cybersecurity Practice #6: Network Management

Computers communicate with other computers through networks. These networks are connected wirelessly or via wired connections (e.g., network cables), and networks 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 networks are secure and that all networked devices access networks safely and securely. Even if network management is provided by a third-party IT support vendor, the organization must understand key aspects of proper network management and ensure that they are included in contracts for these services.

Sub-Practices for Small Organizations

6.S.A	***Network Segmentation***	***NIST FRAMEWORK REF:*** PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3

Configure networks to restrict access between devices to that which is required to successfully complete work. This will limit any cyberattacks from spreading across 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 who will 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 cyberattacks on both your organization and on 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, in turn reducing the risk of cyberattacks.

6.S.B	***Physical Security and Guest Access***	***NIST FRAMEWORK REF:*** PR.AC-4, PR.AC-2, PR.PT-3, PR.AC-5

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

- Always keep data and network closets locked. 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.
- In conference rooms or waiting areas, establish guest networks that separate organizational data and systems. This separation will limit the accessibility of private data from guests visiting the organization. Validate that guest networks are configured to access authorized guest services only.

6.S.C	***Intrusion Prevention***	***NIST FRAMEWORK REF:*** PR.IP-1

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 intrusion prevention systems (IPS) component. Implementing IPS and configuring them to update automatically reduces your organization's vulnerability to known types of cyber-attacks.

IPS are available as part of a suite of next-generation network applications or as stand-alone products that can be added to existing networks.

Threats Mitigated

1. Ransomware attack
2. Loss or theft of equipment or data
3. Insider, accidental or intentional loss of data
4. Attacks against medical device that may affect patient safety

Cybersecurity Practice #7: Vulnerability Management

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

Sub-Practices for Small Organizations

7.S.A	***Vulnerability Management***	***NIST FRAMEWORK REF:*** PR.IP-12

As discussed in the introduction to this document, weak passwords, default passwords, outdated software, and other technology flaws identified by vulnerability management scans are commonly referred to as *vulnerabilities*. Vulnerability scans may yield large amounts of data, which organizations urgently need to classify, evaluate, and prioritize to remediate security flaws before an attacker can exploit them.

Vulnerability management practices include:

- Schedule and conduct vulnerability scans on servers and systems under your control 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 of internet-facing webservers, such as web-based patient portals. Specialized vulnerability scanners can interrogate running web applications to identify vulnerabilities in the application design.
- Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software. Maintain software at least monthly, implementing patches distributed by the vendor community, if patching is not automatic. Robust patch management processes, as outlined in 2.S.A, mitigates vulnerabilities associated with obsolete software versions, which are often easier for hackers to exploit.

Threats Mitigated

1. Ransomware attack
2. Insider, accidental or intentional data loss
3. Attacks against connected medical devices that may affect patient safety

Cybersecurity Practice #8: Incident Response

Incident response is the ability to discover cyberattacks on the network and prevent them from causing data breach or loss. Incident response 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 security incidents that affect organizations of all sizes are 1) the installation and detection of malware, and 2) 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 breach or loss to occur through subsequent events.

Sub-Practices for Small Organizations

8.S.A	***Incident Response***	***NIST FRAMEWORK REF:*** PR.IP-9

Small organizations are often challenged by incident response management, in part because incident response procedures may not be established. Employees who rarely encounter cyberattacks may not remember what to do in the case of an incident. Members of the management team may not know whom to contact to obtain or provide information about the incident. In many cases, there are no dedicated information security professionals in small organizations, resulting in increased reliance on the IT department. A common concern is the fear of penalties from regulators if the organization contacts acknowledges and rectifies a security incident.

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 that the leader is fully authorized to execute all tasks required to complete the investigation. A sample incident response plan is provided in *Appendix G* 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's 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.

Table 7. Incident Response Recommendations to Mitigate Risk of a Data Breach

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.

Incident	Response Recommendation
Phishing	• Identify malicious e-mail messages and delete from mailboxes. • Proactively block websites (URLs) referenced in "click attacks." • Identify malware that might have been installed on computers, and remediate appropriately if present

8.S.B	***ISAC/ISAO Participation***	***NIST: DETECT*** ID.RA-2

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 communities of professionals who are prepared to respond to the same cyber threats. By joining such a 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 Health Information Sharing and Analysis Center [H-ISAC] within the health care sector) or community (such as the Population Health ISAO). In all cases, the primary function of these associations is to establish and maintain channels for sharing cyber intelligence.

Threats Mitigated

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

Cybersecurity 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 health care 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 medical devices reduces the labor burden and exposure to human error that results from manual input of dataFurthermore, 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 drug libraries as well as download usage data.

As with all technologies, medical device benefits are accompanied by cybersecurity challenges. One emerging threat is the practice of 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.

Sub-Practices for Small Organizations

9.S.A	***Medical Device Security***	***NIST FRAMEWORK REF:*** PR.PT

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

Threats Mitigated

1. Attacks against connected medical devices that may affect patient safety

Cybersecurity 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.

Sub-Practices for Small Organizations

10.S.A	***Policies***	***NIST FRAMEWORK REF:*** IG.GV-1, ID.AM-6, PR.AT, PR.AT-1, RS.CO-1

Policies are established first and are then supplemented with procedures that enable the policies to be implemented. Policies describe what is expected, and procedures describe how the expectations are met.

For example, a policy is established that all users will complete privacy and security training. The policy specifies that training courses will be developed and maintained for both privacy and security, that all users will complete the training, that a particular method will be used to conduct the training, and that specific actions will be taken to address noncompliance 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 provide these details, for example, by clearly stating that 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 G* of the Main document. Policy examples with descriptions and recommended users are provided in Table 8.

Table 8. Effective Policies to Mitigate the Risk of Cyberattacks

Policy Name	Description	User Base
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.	• All users
Education and Awareness	Describe the mechanisms by which the workforce will be trained on cybersecurity practices, threats, and mitigations.	• All users • Cybersecurity team

Policy Name	Description	User Base
Acceptable Use / E-mail Use	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how e-mail will be used to complete work.	• All users
Data Classification	Describe how data will be classified, with usage parameters for each classification. This classification should be in line with Cybersecurity Practice #4.	• All users
Personal Devices	Describe the organization's position on usage of personal devices, also referred to as *bring your own device (BYOD).* If usage of personal devices is permitted, describe the expectations for how the devices will be managed.	• All users
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 team
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 team

Threats Mitigated

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

Appendix A: Acronyms and Abbreviations

Table 9. 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

Acronym/Abbreviation	Definition
HMO	Health Maintenance Organization
HPH	Health Care 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	Intrusion Prevention Systems
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	Multifactor 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
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

Acronym/Abbreviation	Definition
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
VP	Vice President
VPN	Virtual Private Network