

# Volume 1: Cybersecurity Best Practices for Small Healthcare Organizations

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0990-0379. The time required to complete this information collection is estimated to average 30 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, to review and complete the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: U.S. Department of Health & Human Services, OS/OCIO/PRA, 200 Independence Ave., S.W., Suite 336-E, Washington D.C. 20201, Attention: PRA Reports Clearance Officer

30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47

## Table of Contents

Introduction .....	3
Document Guide - Cybersecurity Best Practices .....	5
Cybersecurity Best Practice #1: Email Protection Systems.....	7
Cybersecurity Best Practice #2: Endpoint Protection Systems.....	10
Cybersecurity Best Practice #3: Access Management .....	12
Cybersecurity Best Practice #4: Data Protection and Loss Prevention .....	14
Cybersecurity Best Practice #5: Asset Management .....	17
Cybersecurity Best Practice #6: Network Management.....	19
Cybersecurity Best Practice #7: Vulnerability Management .....	21
Cybersecurity Best Practice #8: Incident Response .....	22
Cybersecurity Best Practice #9: Medical Device Security .....	24
Cybersecurity Best Practice #10: Cybersecurity Policies .....	25
Appendix A: Acronyms and Abbreviations .....	27

## 48 Introduction

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

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

62 In general, small organizations perform the following functions:

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

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

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

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

- 89 • Electronic Health Records (EHR) interoperability guidelines

- 90 • Medicare Access and the Children’s Health Insurance Program (CHIP) Reauthorization Act of  
91 2015 (MACRA)/Meaningful Use
- 92 • Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology  
93 Economic and Clinical Health Act (HITECH)
- 94 • Payment Card Industry Data Security Standard (PCI-DSS)
- 95 • Substance Abuse and Mental Health Services Administration (SAMHSA)
- 96 • The Stark Law as it relates to using the services of an affiliated organization

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

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

106

107

108

109 **Document Guide - Cybersecurity Best Practices**

110 This volume provides small organizations with a series of best practices to reduce the impact of the five  
 111 cybersecurity threats identified in Table 1 and discussed in the **main document, Cybersecurity for the**  
 112 **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.

113 *Table 1. Five Prevailing Cybersecurity Threats to Healthcare Organizations*

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

116 *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

## 119 Cybersecurity Best Practice #1: Email Protection Systems

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

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

### 129 **Baseline Practices**

#### 130 **A. Email System Configuration**

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

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

#### 153 **B. Education**

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

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

Phishing Technique	Best Practice
<b>Check Embedded Links</b>	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.
<b>Look for Suspicious <i>From</i>: Addresses</b>	Check received emails for spoofed or misspelled <i>From</i> : addresses. For example, if your organization is “ACME” and you receive an email from <a href="mailto:user@AMCE.com">user@AMCE.com</a> , do not open the email without verifying that it is legitimate.
<b>Be cautious with “Urgent” messages</b>	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.
<b>Be cautious with “Too Good to be True” messages</b>	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.

158 *Table 3. Train Users to Recognize Phishing Techniques*

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

162 **C. Phishing Simulations**

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

167 Steps for an effective anti-phishing campaign include:

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



180

*Threats Mitigated*

181

1. Email Phishing Attack

182

2. Ransomware Attack

183

3. Accidental or Intentional Data Loss

184

185 **Cybersecurity Best Practice #2: Endpoint Protection Systems**

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

192 **Baseline Practice**

193 **A. Basic Endpoint Protection Controls**

Security Control	Description
<b>Remove administrative accounts</b>	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.
<b>Keep your endpoints patched</b>	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.
<b>Implement Antivirus software</b>	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.
<b>Turn on endpoint encryption</b>	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.

<b>Enable firewalls</b>	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.
<b>Enable 2Factor Authentication for remote access</b>	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.

194 *Table 4. Effective Security Controls Protect Organization Endpoints.*

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

200 ***Threats Mitigated***

- 201 1. Ransomware Attack
- 202 2. Theft or Loss of Equipment or Data

203

204 **Cybersecurity Best Practice #3: Access Management**

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

209 **Baseline Practice**

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

214 **A. Basic Access Management**

Security Control	Description
<b>Establish a unique account for each user</b>	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).
<b>Limit the use of shared or generic accounts</b>	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.
<b>Tailor access to the needs of each user</b>	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.
<b>Terminate user access as soon as the user leaves the organization</b>	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.

<b>Role based access</b>	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.
<b>Configure systems and endpoints with automatic lock and log-off</b>	Configure systems and endpoints to automatically lock and log off users after a predetermined period of inactivity, such as 15 minutes.
<b>Implement Single-Sign On</b>	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.
<b>Implement Multi-Factor Authentication for the Cloud</b>	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.

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

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

220 **Threats Mitigated**

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

## 225 **Cybersecurity Best Practice #4: Data Protection and Loss Prevention**

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

### 232 **Baseline Practice**

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

#### 237 **A. Policy**

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

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

Classification	Description
<b>Highly Sensitive</b>	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.
<b>Sensitive</b>	All other PHI, especially data associated with the Designated Record Set, Clinical Research data, Insurance information, human/employee data, and organizational board materials.
<b>Internal</b>	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.

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

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

250 **B. Procedures**

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

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

- 287
- 288
- 289
- 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.

290 **C. Education**

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

294 **Threats Mitigated**

- 295
- 296
- 297
- 298
1. Ransomware Attack
  2. Loss or Theft of Equipment or Data
  3. Accidental or Intentional Data Loss



## 299 **Cybersecurity Best Practice #5: Asset Management**

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

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

### 310 **Baseline Practice**

#### 311 **A. Inventory**

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

- 315 • Asset ID (primary key)
- 316 • Host Name
- 317 • Purchase Order
- 318 • Operating System
- 319 • Media Access Control (MAC) Address
- 320 • IP Address
- 321 • Deployed to (User)
- 322 • User Last Logged On
- 323 • Purchase Date
- 324 • Cost
- 325 • Physical Location

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

#### 328 **B. Procurement**

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

333 **C. Decommissioning**

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

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

341 **Threats Mitigated**

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

346

347

## 348 **Cybersecurity Best Practice #6: Network Management**

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

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

### 357 **Baseline Practice**

#### 358 **A. Network Segmentation**

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

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

#### 376 **B. Physical Security and Guest Access**

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

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

388 **C. Intrusion Prevention**

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

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

397 **Threats Mitigated**

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

402

## 403 **Cybersecurity Best Practice #7: Vulnerability Management**

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

### 407 *Baseline Practice*

#### 408 **A. Vulnerability Management**

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

414 Vulnerability management best practices include:

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

### 430 *Threats Mitigated*

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

434

## 435 **Cybersecurity Best Practice #8: Incident Response**

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

### 443 *Baseline Practice*

#### 444 **A. Incident Response**

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

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

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

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

Incident	Response Recommendation
<b>Malware</b>	<ul style="list-style-type: none"><li>• Re-image, rebuild, or reset computer to a known good state.</li><li>• Do not trust “malware cleaning” tools until they are verified to function as described.</li></ul>
<b>Phishing</b>	<ul style="list-style-type: none"><li>• Identify malicious email messages and delete from mailboxes.</li><li>• Proactively block websites (URLs) referenced in “click attacks.”</li><li>• Identify malware that might have been installed on computers. Execute malware play if run.</li></ul>

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

466

467 **B. ISAC/ISAO Participation**

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

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

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

483 **Threats Mitigated**

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

489

490

491

492 **Cybersecurity Best Practice #9: Medical Device Security**

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

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

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

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

511 **Baseline Practice**

512 **A. Medical Device Security**

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

515 **Threats Mitigated**

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

517



518 **Cybersecurity Best Practice #10: Cybersecurity Policies**

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

524 **Baseline Practice**

525 **A. Policies**

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

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

536 Examples of policy templates are provided in [Appendix I of the main document](#).

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

Policy Name	Description	User Base
<b>Roles and Responsibilities</b>	Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for conducting security practices, setting and establishing policy, and implementing security practices.	<ul style="list-style-type: none"><li>• All users</li></ul>
<b>Education and Awareness</b>	Describe the mechanisms by which the organizational workforce will be trained on cybersecurity practices, threats and mitigations.	<ul style="list-style-type: none"><li>• All users</li><li>• Cybersecurity Department</li></ul>
<b>Acceptable Use / Email Use</b>	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how email will be used to complete work.	<ul style="list-style-type: none"><li>• All users</li></ul>
<b>Data Classification</b>	Describe how data will be classified with usage parameters for each classification.	<ul style="list-style-type: none"><li>• All users</li></ul>
<b>Personal Devices</b>	Describe the organization’s position on usage of personal devices – also referred to as Bring Your	<ul style="list-style-type: none"><li>• All users</li></ul>

	Own Device (BYOD). If usage of personal devices is permitted, describe the expectations for how the devices will be managed.	
<b>Laptop, Portable Device, and Remote Use</b>	Describe the policies that relate to mobile device security and how these devices may be used in a remote setting.	<ul style="list-style-type: none"> <li>• All users</li> <li>• IT Departments</li> </ul>
<b>Incident Reporting and Checklist</b>	Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.	<ul style="list-style-type: none"> <li>• All Users</li> <li>• Cybersecurity Department</li> </ul>

538 *Table 8. Effective Policies Mitigate the Risk of Cyberattacks*

539

540

*Threats Mitigated*

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

546

## 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
<b>NH-ISAC</b>	National Healthcare – Information Sharing and Analysis Centers
<b>NIST</b>	National Institute of Standards and Technology
<b>NVD</b>	National Vulnerability Database
<b>OCIO</b>	Office of the Chief Information Officer
<b>OCR</b>	Office for Civil Rights
<b>ONC</b>	Office of the National Coordinator (for Healthcare Technology)
<b>PACS</b>	Pictures Archiving and Communication Systems
<b>PCI-DSS</b>	Payment Card Industry Data Security Standard
<b>PHI</b>	Personal Health Information
<b>PII</b>	Personal Identifiable Information
<b>ROM</b>	Read Only Memory
<b>SAMHSA</b>	Substance Abuse and Mental Health Services Administration
<b>SOC/IR</b>	Security Operations Center / Incident Response
<b>SSN</b>	Social Security Number
<b>SVP</b>	Senior Vice President
<b>URL</b>	Uniform Resource Locator

<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USB</b>	Universal Serial Bus
<b>VP</b>	Vice President
<b>VPN</b>	Virtual Private Network

549