

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30

# **Volume 2: Cybersecurity Best Practices for Medium and Large 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

31 **Table of Contents**

32 Introduction ..... 3

33 Cybersecurity Best Practices for Medium Healthcare Organizations..... 3

34 Cybersecurity Best Practices for Large Organizations ..... 5

35 Document Guide – Cybersecurity Best Practices ..... 7

36 Cybersecurity Best Practice #1: Email Protection Systems..... 12

37 Cybersecurity Best Practice #2: Endpoint Protection Systems..... 21

38 Cybersecurity Best Practice #3: Identity and Access Management ..... 27

39 Cybersecurity Best Practice #4: Data Protection and Loss Prevention ..... 37

40 Cybersecurity Best Practice #5: IT Asset Management ..... 46

41 Cybersecurity Best Practice #6: Network Management..... 51

42 Cybersecurity Best Practice #7: Vulnerability Management ..... 58

43 Cybersecurity Best Practice #8: Security Operations Center and Incident Response ..... 63

44 Cybersecurity Best Practice #9: Medical Device Security ..... 75

45 Cybersecurity Best Practice #10: Cybersecurity Policies ..... 83

46 Appendix A: Acronyms and Abbreviations ..... 86

47

48

49

50

## 51 Introduction

### 52 *Cybersecurity Best Practices for Medium Healthcare Organizations*

53 Medium healthcare organizations perform critical functions for the Healthcare and Public Health (HPH)  
54 Sector. These organizations include critical access hospitals in rural areas, management practice  
55 organizations that support physician practices, revenue cycle or billing organizations, mid-sized device  
56 manufacturers, and group practices. Generally speaking, a medium healthcare organization employs  
57 hundreds of personnel, maintains between hundreds and a few thousand Information Technology (IT)  
58 assets, and may be primary partners with and interfaces between small and large healthcare  
59 organizations. It's typical for a medium organization to have several critical systems that are  
60 interconnected to enable work activities in support of the organization's mission.

61 These organizations tend to have a fairly diverse inventory of assets that support multiple revenue  
62 streams. They also tend to have narrow profit margins, limited resources, and limited flexibility to  
63 implement robust cybersecurity practices. For example, unless connected to a larger system, it is rare  
64 for a medium organization to have a 24x7 security operations center (SOC). Yet, these organizations are  
65 essential to care for patients in more rural settings, for example, a rural critical access hospital or an  
66 operational support provider for health care organizations located in rural areas.

67 Medium organizations tend to focus on preventing cybersecurity events, implementing a more rigid  
68 security policy with few exceptions permitted. This is often due to a lack of resources required to  
69 support a more open and flexible cybersecurity model that larger organizations can afford. Medium  
70 organizations usually struggle to obtain cybersecurity funding that is separate and distinct from a  
71 standard IT budget. The top security professional in an organization of this size might often feel  
72 overwhelmed by compliance and cybersecurity duties, wear multiple hats, and be constrained around  
73 execution plans.

74 Medium organizations operate in complex legal and regulatory environments that include but not  
75 limited to:

- 76 • ONC Certified Electronic Health Information Technology interoperability regulations
- 77 • Medicare Access and CHIP Reauthorization Act of 2015 (MACRA)/Meaningful Use
- 78 • Multiple enforcement obligations under the Food and Drug Administration (FDA)
- 79 • The Joint Commission accreditation processes
- 80 • HIPAA/HITECH requirements
- 81 • The Payment Card Industry Data Security Standard (PCI-DSS)
- 82 • Substance Abuse and Mental Health Services Administration (SAMHSA) requirements
- 83 • The Gramm-Leach-Bliley Act for financial processing
- 84 • The Stark Law as it relates to being able to provide services to affiliated organizations
- 85 • The Family Educational Rights and Privacy Act (FERPA) for those institutions participating within  
86 Higher Education
- 87 • The Genetic Information Nondiscrimination Act (GINA)
- 88 • The new General Data Protection Regulation (GDPR) in the European Union

89 ***IT Assets Utilized by Medium Organizations***

90 Medium organizations may have up to a few thousand IT assets, with a mix of dozens to a hundred  
91 information systems. All assets are capable of having cybersecurity vulnerabilities and are susceptible to  
92 cyber threats. The important factor in securing these assets is understanding their relationship within  
93 the organization’s IT ecosystem, how they are leveraged and used by the workforce, and the data that is  
94 generated, stored, and processed within. Not all assets are equally important: some are mission critical  
95 and must be fully operational at all times while others might be able to be offline for days or weeks  
96 without harming the organization’s mission. Some assets have large repositories of sensitive data that  
97 represent a significant risk, but are not as critical to the enterprise business drivers. In all cases, IT assets  
98 are used by the organization for a business reason and should be protected with proper cyber hygiene  
99 controls.

100 Examples of assets that can be found in medium organizations include but are not limited to:

- 101 • Static devices used by the workforce, such as shared workstations and clinical  
102 workstations used strictly for patient care with select mobile devices, such as laptops  
103 and smartphones. There may not be a large number of mobile devices due to their  
104 increased cost.
- 105 • Large numbers of “Internet of Things” (IoT) devices, for example, medical devices, smart  
106 televisions, printers and copiers, and security cameras.
- 107 • Data that includes sensitive health information stored and processed on devices,  
108 servers, applications, and the cloud. These data include names, medical record  
109 numbers, birth dates, social security numbers, diagnostic conditions, prescriptions, and  
110 potentially highly sensitive mental health, substance abuse, or sexually transmitted  
111 disease information. These sensitive data are generally referred to as Protected Health  
112 Information (PHI) or Personal Identifiable Information (PII).
- 113 • Assets related to the IT infrastructure, for example, firewalls, network switches and  
114 routers, Wi-Fi (both corporate and guest), servers supporting IT management systems,  
115 and file storage systems (cloud or on premise).
- 116 • Applications or Information Systems that support the business processes. This includes  
117 Human Resource (HR) or Enterprise Resource Planning (ERP) systems, pathology lab  
118 systems, blood bank systems, medical imaging systems, pharmacy systems, revenue  
119 cycle systems, supply chain/materials management systems, specialized oncology  
120 therapy systems, radiation oncology treatment systems, and data warehouses (e.g.,  
121 clinical, financial).

122 Personal devices, often referred to as BYOD (Bring Your Own Device), generally are not permitted due to  
123 the organization’s inability to dedicate the security controls required to secure their access.

124 ***Cybersecurity Best Practices***

125 Medium organizations should consider the *Baseline Practices* discussed in each best practice presented  
126 in this volume. Nothing in this volume is intended to exclude medium organizations from adopting  
127 advanced best practices. Advanced best practices that are determined to be relevant should be  
128 considered for adoption by any organization.

129

130 **Cybersecurity Best Practices for Large Organizations**

131 Large healthcare organizations perform a range of different functions. These organizations may be  
132 integrated with other healthcare delivery organizations, academic medical centers, insurers that provide  
133 healthcare coverage, clearinghouses, pharmaceuticals, or medical device manufacturers. In most cases,  
134 a large organization employs thousands of employees, maintains tens of thousands to hundreds of  
135 thousands of IT assets, and has intricate and complex digital ecosystems. While smaller organizations  
136 operate with a few critical systems, large organizations can have hundreds if not thousands of  
137 interconnected systems with complex functionality.

138 Large organizations have the broadest mission scope and a large volume of assets to fulfill this mission.  
139 Even so, they often struggle to obtain funding to maintain security programs as well as control of their  
140 assets (shadow IT, rogue devices, unmanaged/unpatched devices), how sensitive data flows in and out  
141 of the organization’s environment, and understanding system boundaries and segmentation that  
142 determine where one entity’s responsibilities end and another’s starts.

143 The missions of large organizations are diverse and varied. They include providing standard general  
144 practice care, providing specialty or subspecialty care for complicated medical cases, conducting  
145 innovative medical research, providing insurance coverage to large populations of patients, supporting  
146 the healthcare delivery ecosystem, and supplying and researching new therapeutic treatments (such as  
147 drugs or medical devices). Overall, these organizations are responsible for complicated healthcare  
148 issues and tend to operate in complex environments.

149 Large organizations operate in a legal and regulatory environment that is as complicated as their digital  
150 ecosystems. It includes but not limited to:

- 151 • ONC Certified Electronic Health Information Technology interoperability standards
- 152 • CMS Medicare Access and CHIP Reauthorization Act of 2015 (MACRA)/Meaningful Use
- 153 • Multiple obligations under the Food and Drug Administration (FDA)
- 154 • The Joint Commission accreditation processes
- 155 • HIPAA/HITECH requirements
- 156 • Minimum Acceptable Risk Standards (MARS) for payers
- 157 • State privacy and security rules
- 158 • Federal Information Security Modernization Act (FISMA) requirements for federal  
159 contracts and research grants through agencies such as the National Institutes of Health  
160 (NIH)
- 161 • The Payment Card Industry Data Security Standard (PCI-DSS)
- 162 • Requirements under the Substance Abuse and Mental Health Services Administration  
163 (SAMHSA)
- 164 • The Gramm-Leach-Bliley Act for financial processing
- 165 • The Stark Law as it relates to being able to provide services to affiliated organizations
- 166 • The Family Educational Rights and Privacy Act (FERPA) for those institutions that  
167 participate in Higher Education

- 168 • The Genetic Information Nondiscrimination Act (GINA)
- 169 • The new General Data Protection Regulation (GDPR) in the European Union.

### 170 *IT Assets Utilized by Large Organizations*

171 As mentioned, large organization operations are supported by a complicated ecosystem of IT assets. All  
172 assets are capable of having cybersecurity vulnerabilities and are susceptible to cyber threats. The  
173 important factor in securing these assets is understanding their relationship within the organization's IT  
174 ecosystem, how they are leveraged and used by the workforce, and the data that is generated, stored,  
175 and processed within. Not all assets are equally important: some are mission critical and must be fully  
176 operational at all times while others might be offline for days or weeks without harming the  
177 organization's mission. Some assets have large repositories of sensitive data that represent a significant  
178 risk, but are not as critical to the enterprise business drivers. In all cases, IT assets are used by the  
179 organization for a business reason and should be protected with proper cyber hygiene controls.

180 Examples of assets that can be found in large organizations include but are not limited to:

- 181 • Devices used by the workforce such as mobile phones, tablets, voice recorders and  
182 laptop computers for dictation (all with Internet connectivity).
- 183 • Personal devices that are often referred to as BYOD.
- 184 • Extremely large deployments of IoT assets that include medical devices, smart  
185 televisions, printers and copiers, security cameras, refrigeration sensors, blood bank  
186 monitoring systems, building management sensors and more.
- 187 • Data that includes sensitive health information stored and processed on devices,  
188 servers, applications and the cloud. These data include names, medical record numbers,  
189 birth dates, social security numbers, diagnostic conditions, prescriptions, and potentially  
190 highly sensitive mental health, substance abuse, or sexually transmitted disease  
191 information. The sensitive data captured here are generally referred to as PHI or PII.
- 192 • Assets related to the IT infrastructure, for example, firewalls, network switches and  
193 routers, Wi-Fi (corporate and guest), servers supporting IT management systems, and  
194 file storage systems (cloud or on premise).
- 195 • Applications or Information Systems that support the business processes. This includes  
196 ERPs, pathology lab systems, blood bank systems, medical imaging systems, pharmacy  
197 systems (retail and specialized), revenue cycle systems, supply chain/materials  
198 management systems, specialized oncology therapy systems, radiation oncology  
199 treatment systems, data warehouses (clinical, financial, research), vendor management  
200 systems, and so much more.

201

202 **Document Guide – Cybersecurity Best Practices**

203 This volume is intended to provide medium and large organizations with best practices to reduce the  
204 impact of these five currently prevailing threats:

- 205 • Email Phishing Attacks
- 206 • Ransomware Attacks
- 207 • Loss of Theft of Equipment or Data
- 208 • Internal, Accidental or Intentional Data Loss
- 209 • Attacks Against Medical Devices that can Affect Patient Safety

210 The intent of this section is to help you navigate the document this document. Each best practice is  
211 broken up into three core segments: Baseline Practices, Advanced Practices and the Key Risks that are  
212 Mitigated by the Practice. Additionally, each Best Practice contains a series of suggested metrics to  
213 measure the effectiveness of those practices.

214 “Baseline Practices” apply to both Medium and Large organizations. “Advanced Practices” apply to  
215 Large organizations, and any other organization that is interested in their adoption.

216 A summary of each of the Best Practices is outlined in the following ten tables.

Best Practice 1: Email Protection Systems	
Data that may be affected	Passwords and PII
Baseline Practices	A. Basic Email Protection Controls B. MFA for Remote Access C. Email Encryption D. Workforce Education
Advanced Practices	A. Advanced and Next Generation Tooling B. Digital Signatures C. Analytics Driven Education
Key Mitigated Risks	<ul style="list-style-type: none"><li>• Email Phishing Attacks</li><li>• Ransomware Attacks</li><li>• Accidental or Intentional Data Loss</li></ul>

217

Best Practice 2: Endpoint Protection Systems	
Data that may be affected	Passwords, ePIL, ePHI
Baseline Practices	A. Basic Endpoint Protection Controls
Advanced Practices	A. Automate the Provisioning of Endpoints B. Mobile Device Management C. Host Based Intrusion Detection/Prevention Systems D. Endpoint Detection Response E. Application Whitelisting F. Micro-segmentation/virtualization strategies
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Theft or Loss of Equipment or Data</li> </ul>

218

Best Practice 3: Identity and Access Management	
Data that may be affected	Passwords
Baseline Practices	A. Identity B. Provisioning, Transfers, and Deprovisioning Procedures C. Authentication D. Multi-Factor Authentication for Remote Access
Advanced Practices	A. Federated Identity Management B. Authorization C. Access Governance D. Single-Sign On (SSO)
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

219

Best Practice 4: Data Protection and Loss Prevention	
Data that may be affected	Passwords, ePIL, ePHI
Baseline Practices	A. Classification of Data B. Data Use Procedures C. Data Security D. Backup Strategies E. Data Loss Prevention (DLP)
Advanced Practices	A. Advanced Data Loss Prevention B. Mapping of Data Flows
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Loss of Theft of Equipment or Data</li> <li>• Accidental or Intentional Data Loss</li> </ul>

220



Best Practice 5: IT Asset Management	
Data that may be affected	Passwords, ePIL, ePHI
Baseline Practices	A. Inventory of Endpoints and Servers B. Procurement C. Secure Storage for Inactive Devices D. Decommissioning Assets
Advanced Practices	A. Asset Pre-Configuration B. Automated Discovery and Maintenance C. Integration with Network Access Control
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Loss of Theft of Equipment or Data</li> <li>• Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

221

Best Practice 6: Network Management	
Data that may be affected	-
Baseline Practices	A. Network Profiles and Firewalls B. Network Segmentation C. Intrusion Prevention Systems D. Web Proxy Protection E. Physical Security of Network Devices
Advanced Practices	A. Additional Network Segmentation B. Command and Control Monitoring of Perimeter C. Anomalous Network Monitoring and Analytics D. Network Based Sandboxing/Malware Execution E. Network Access Control (NAC)
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Loss of Theft of Equipment or Data</li> <li>• Accidental or Intentional Data Loss</li> <li>• Medical Devices and Patient Safety</li> </ul>

222

Best Practice 7: Vulnerability Management	
Data that may be affected	-
Baseline Practices	A. Host/Server Based Scanning B. Web Application Scanning C. System Placement and Data Classification D. Patch Management, Configuration Management, Change Management
Advanced Practices	A. Remediation Planning

Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Insider, Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices</li> </ul>
---------------------	---

223

Best Practice 8: Security Operations Center and Incident Response	
Data that may be affected	-
Baseline Practices	A. Security Operations Center B. Incident Response C. Information Sharing and ISACs/ISAOs
Advanced Practices	A. Advanced Security Operations Center B. Advanced Information Sharing C. Incident Response Orchestration D. Baseline Network Traffic E. User Behavior Analytics F. Deception Technologies
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Phishing Attacks</li> <li>• Ransomware Attacks</li> <li>• Loss or Theft of Equipment</li> <li>• Insider, Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices</li> </ul>

224

Best Practice 9: Medical Device Security	
Data that may be affected	ePHI
Baseline Practices	A. Medical Device Management B. Endpoint Protections C. Identity and Access Management D. Asset Management E. Network Management
Advanced Practices	A. Vulnerability Management B. Security Operations and Incident Response C. Procurement and Security Evaluations D. Contacting the FDA
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

225

Best Practice 10: Cybersecurity Policies	
Data that may be affected	-
Baseline Practices	A. Policies

Advanced Practices	-
Key Mitigated Risks	<ul style="list-style-type: none"><li>• Email Phishing Attacks</li><li>• Ransomware Attacks</li><li>• Loss or Theft of Equipment or Data with Sensitive Information</li><li>• Accidental or Intentional Data Loss</li><li>• Attacks Against Connected Medical Devices and Patient Safety</li></ul>

226

227

228

## Cybersecurity Best Practice #1: Email Protection Systems

229 According to the 2017  
 230 Verizon Data Breach Report,  
 231 “weak or stolen passwords  
 232 were responsible for 80% of  
 233 the hacking related  
 234 breaches” (Zaw 2017). This  
 235 report further identifies the  
 236 phishing attack (which is a  
 237 hacking attack) as the most  
 238 common first point of  
 239 unauthorized entry into an  
 240 organization. After  
 241 monitoring 1,400 customers  
 242 and 40 million simulated

Best Practice 1: Email Protection Systems	
Data that may be affected	Passwords and PII
Baseline Practices	A. Basic Email Protection Controls B. MFA for Remote Access C. Email Encryption D. Workforce Education
Advanced Practices	A. Advanced and Next Generation Tooling B. Digital Signatures C. Analytics Driven Education
Key Mitigated Risks	<ul style="list-style-type: none"> <li>Email Phishing Attacks</li> <li>Ransomware Attacks</li> <li>Accidental or Intentional Data Loss</li> </ul>

243 phishing campaigns, the PhishMe 2017 Enterprise Resiliency and Defense Report concluded that the  
 244 average susceptibility of an organization to a phishing attack is 10.8% (How susceptible are you to  
 245 enterprise phishing? 2017). Though other areas of significant threat exist, including in the web  
 246 application space, the effectiveness of phishing attacks allows attackers to bypass most perimeter  
 247 detections by “piggy backing” on the legitimate workforce user. Think about it, if an attacker obtains an  
 248 employee’s password and that employee has remote access to the organization’s IT assets, the attacker  
 249 has made significant progress toward penetrating the organization.

250

251 The two most common methods deployed by phishing attacks include a credential theft attack and a  
 252 malware dropper attack. An organization’s cybersecurity practices must address these two attack  
 253 vectors – leveraging email to conduct a credential harvesting attack on the organization and delivery of  
 254 malware through an email that can compromise the organization’s endpoints. For both vectors, email is  
 255 the vector leverage and the focus for additional security controls.

256 **Baseline Practice**

257 **A. Basic Email Protection Controls (NIST Framework: PROTECT)**

258 Basic protections that should be implemented in any email system are standard anti-spam and anti-virus  
 259 filtering controls, both of which are implemented directly on the email platform. These controls assess  
 260 inbound and outbound emails from known malicious senders or patterns of malicious content. Table 3  
 261 provides a list of suggested security implementations for email protection controls.

Control	Description
<b>Real-time Blackhole List (RBL)</b>	Community-based lists of IP addresses and host names of known or potential spam originators. Consider Spamhaus, Spamcop, DNSRBL or lists provided by your email technology.

<b>Distributed Checksum Clearinghouse (DCC)</b>	The DCC is a distributed database that contains a checksum of messages. Email messages are run through a checksum algorithm and then checked against the database. Depending upon the threshold of checksum matches, these can be determined to be spam or malicious messages.
<b>Removal of Open Relays</b>	Open Relays are Simple Mail Transfer Protocol (SMTP) servers that enable the relay of third party messages. SMTP is critical for the delivery of messages but must be configured to allow messages only from trusted sources. Failure to do this may permit a spammer or hacker to leverage the “trust” of your mail server to transmit malicious content.
<b>Spam/Virus check on outbound messages</b>	Spam/Virus checks of outbound emails can detect malicious content, indicating a compromised account and potential security incident in the organization. Email spam/virus rules should be reviewed as part of <i>Best Practice #8: Security Operations Center and Incident Response</i> .
<b>Antivirus check</b>	All email content should be scanned against an antivirus (AV) engine with up-to-date signatures. If possible, this control should unpack compressed files (such as zip files) to check for embedded malware.
<b>Restrict the “Send As” permission for Distribution Lists</b>	Limit distribution lists to essential members. Distribution lists can be popular mechanisms for a compromised account to disseminate malicious content and should not be accessible to large numbers of users.
<b>Implement Sender Policy Framework (SPF) Records</b>	A Domain Name System (DNS) record identifies which mail servers are permitted to send email on behalf of your domain. This enables the receiving mail server to verify the authenticity of the sending mail server.
<b>Implement Domain Key Identified Mail (DKIM)</b>	A method of email authentication that leverages cryptography to ensure email messages are sent from authorized email servers. A public key is stored within the organization’s DNS as a text record (TXT). All messages sent from that domain are digitally signed with a DKIM signature that can be validated through the DNS public key TXT record.
<b>Implement Domain-based Message Authentication Reporting and Conformance (DMARC)</b>	An authentication technology that leverages both SPF and DKIM to validate that an email’s “From:” address (i.e., the sender) is valid. DMARC enables the receiving mail system to check SPF and DKIM records which ensures conformance to the sending host as well as the From: address. It instills trust that the sending party’s email address has not been spoofed, a common attack type to trick users into opening malicious emails.

262

*Table 3. Email protection controls*

263

In most cases, email protection controls do not operate alone. When combined to evaluate an

264

organization’s emails, they contribute information that provides a more complete assessment of each

265 message. In modern systems, this is accomplished by scoring email content on each pass through the  
266 protection controls.

267 It is highly recommended to leverage this scoring technique and to set at least three thresholds: OK for  
268 Delivery, Quarantine, or Block/Drop. Each email should be scored to determine which of the three  
269 thresholds are met. Based on that threshold, automated actions should be executed. Emails cleared for  
270 delivery pass through automatically for additional processing. Block/Drop emails are discarded and  
271 never seen by the user. Quarantine actions allow the user to evaluate the message in a secured  
272 environment, not the user's regular email box, for final verification. In most cases, these quarantine  
273 messages are delivered on a daily basis to the user in a single email digest for verification.

274 Adding X-Headers to the delivery of email messages is a good way to flag potential spam or malicious  
275 email before sending it to the user. There are two common methods for deploying this:

276 *Spam X-Header:* If a message is scored to a threshold where it cannot be definitely classified as  
277 spam/malicious, it can be tagged with an X-Header. The Subject or top of the Body of the message is  
278 modified to include a [POSSIBLE SPAM] tab. This advises the user to verify the legitimacy of the message  
279 before opening it.

280 *External Sender X-Header:* Another common practice is to add an [EXTERNAL] tag or message to  
281 inbound messages from external senders. This tag can be configured to be highly visible, such as  
282 **“WARNING: Stop. Think. Read. This is an external email.”** This method is effective at catching  
283 messages that might be spoofed or pretend to come from within the organization. It also informs the  
284 email recipient to be cautious when clicking links or opening attachments from these sources.

285 *DMARC:* If you leverage DMARC, you might consider exempting the External Sender X-header tag for  
286 messages that pass the DMARC authentication. Generally speaking, this will help the email users  
287 understand the trust environment setup and when it is necessary to be extra vigilant.

288 In addition to tagging messages that fail DMARC authentication, messages can be tagged, or digitally  
289 signed, when they originate from approved hosting or cloud based services with a legitimate need to  
290 spoof an internal address. This is common for communications platforms, such as marketing systems,  
291 emergency management communications systems or alert management systems.

## 292 **B. Multifactor Authentication (MFA) for Remote Email Access (NIST Framework: PROTECT)**

293 It is a common and expected practice for sensitive information to be shared and submitted through  
294 email systems. Email is the primary mechanism used by most organizations to communicate  
295 electronically. It is also a common practice to access email remotely as the workforce has become  
296 increasingly mobile.

297 Given the prevalence of credential harvesting attacks, if remote email systems are made available, the  
298 only control that prohibits a malicious user from accessing sensitive information within transmitted  
299 emails is a password. The susceptibility of organizations to phishing attacks makes this a critical  
300 exposure.

301 As discussed in *Cybersecurity Best Practice #3: Identity and Access Management*, Two Factor  
302 Authentication, or Multi Factor Authentication, is the process of verifying a user's identity using more  
303 than one credential, such as a password. The most common method is to leverage a soft token. The  
304 soft token is a second credential that can be delivered through a mobile phone or tablet, two devices  
305 that most of have close at hand. The soft token could be the delivery of a short message service (SMS)

306 text message with a code or an application installed on the phone that provides the code and/or asks for  
307 independent verification after a successful password entry.

308 Implementation of Two Factor Authentication on your remote access email platform mitigates the risk  
309 of a compromised credential, such as a user password. With Two Factor Authentication, a hacker  
310 requires both the phone and the user's password, which significantly reduces the likelihood of a  
311 successful attack. This is one of the most effective controls to protect your organization's data.

312 **C. Email Encryption** **(NIST Framework: PROTECT)**

313 Email is the most common form of delivering content, including sensitive information, to other members  
314 in an organization. Though this might not be the preferred method for most organizations, one must  
315 assume users will leverage this common and easy-to-use communication channel.

316 Deploying encryption techniques within an email message is an important protection control for users to  
317 leverage. Multiple techniques exist, though the most common invoke a third party application to  
318 conduct encryption by tagging the outbound message in some form. This can be done by putting a  
319 trigger in the subject line (e.g., #encrypt, #confidential), or by invoking it through the email client itself.  
320 It all depends upon the technology solution deployed.

321 When organizations have established partnerships with third parties, fully encrypted transparent email  
322 delivery can be provisioned between the two entities' email systems. In this model, leveraging transport  
323 layer security (TLS) enables both systems to be configured to require TLS encryption when sending or  
324 receiving messages from one another. This ensures the messages are delivered over the Internet in a  
325 manner that cannot be intercepted.

326 Whichever encryption technique is implemented, the organization's workforce must be trained to  
327 leverage the technique when transmitting sensitive information. This best practice may be integrated  
328 into the Data Protection best practices discussed in *Cybersecurity Best Practice #4: Data Protection and*  
329 *Loss Prevention*. Messages that are not encrypted by the user as required can be automatically  
330 encrypted or simply blocked.

331 **D. Workforce Education** **(NIST Framework: PROTECT)**

332 A study released in 2017 determined the average measured susceptibility of an organization for phishing  
333 attacks is 10.8%. Maintaining a workforce to be vigilant and aware of cyberattacks is incredibility  
334 important. Organizations should implement security awareness programs that provide context around  
335 email-based attacks. The challenge presented to security departments is how to deliver a distilled  
336 message or spot a technical attack when the workforce's knowledge level does not match the hacker's  
337 level of sophistication. For example, it's easy to make a phishing email appear to originate from the  
338 company itself, incorporating logos, department names, and management names. It's difficult to train  
339 your entire workforce to detect that fake message.

340 When implementing information security and cybersecurity programs, a few key principles should be  
341 considered. Leverage the following techniques from the 2015 HBR Article from Keith Ferrazzi, (Ferrazzi  
342 2015):

- 343 • *Ignite each managers' passion to coach their employees* – Engage and train your  
344 management team. Leverage them to communicate security practices and information  
345 to staff in all areas of the organization.

- 346 • *Deal with the short-shelf life of learning and development needs* – Security information  
347 changes continuously. Implement continuous and ongoing campaigns to maintain  
348 awareness of current trends, issues and events.
- 349 • *Teach employees to own their career development* - Customize cybersecurity training to  
350 the needs of employees in different positions or units in the organization. Develop  
351 training that is clearly relevant to the user’s job.
- 352 • *Provide flexible learning options* – Provide options, including on-demand and mobile  
353 training solutions that allow the workforce to schedule and complete training  
354 independently.
- 355 • *Serve the learning needs of virtual teams* – Recognize that many employees work  
356 remotely and virtually. Training solutions should fit within the work environment of  
357 virtual employees.
- 358 • *Build trust in organizational leadership* – Leaders must be open and transparent and  
359 lead by example. Managers must demonstrate to the workforce that they are fully  
360 engaged in security strategy and committed to successful execution of security controls  
361 and techniques.
- 362 • *Match different learning options to different learning styles* – Effective training  
363 accommodates the different learning styles and requirements of employees who  
364 function in diverse work environments within a single organization. Consider multiple  
365 options to conduct a single training course to maximize training effectiveness and  
366 efficiency.

367 Organizations should implement a multifaceted training campaign that engages users to catch phishing  
368 through multiple channels. Points to include in your training campaign are:

369 *Sender Verification:* Users should look very carefully at the sender of the email message. It is common  
370 to spoof the organization’s name by changing a simple character, for example, “google.c0m” rather than  
371 “google.com.” Be on the lookout for emails where the organization’s name is given with a separate  
372 email domain, such as “ACME.google.com” rather than “acme.com.”

373 *Follow the Links:* Every link in an email message is suspect. Organizations should limit the use of links in  
374 corporate messages to those that are required. Users should hover the cursor over each link to check  
375 the corresponding URL and determine if it is credible. Specifically, URLs that are mismatched – the  
376 name of the link in the email does not match the corresponding URL – are highly suspect.

377 *Beware of Attachments:* Though it can be difficult to determine if an attachment is malicious based on  
378 the content of an email message, often there are clues. Be wary of messages that require immediate  
379 action, for example, such as “you must read this right away.” Be cautious when receiving attachments  
380 from senders you do not regularly correspond with. It’s important to detect malicious attachments  
381 which may contain malware or exploit scripts that permanently compromise your computer.

382 *Suspect Content:* In most cases, hackers entice you to follow a link or open an attachment. They will use  
383 messages to play with your curiosity and emotions. These messages vary widely from urgent messages  
384 such as “your account will be deactivated unless you re-register” to scary messages such as “the IRS is  
385 suing you and you must fill out the attached form.” Hackers also prey on hopes and desires. Examples  
386 of these messages include “You have won a \$100 Amazon Gift card!” to the old fashion Nigerian Prince  
387 messages which everyone knows about.



388 As you establish your awareness campaigns, keep this simple goal in mind: you want your workforce to  
389 be human sensors detecting malicious activity and reporting these incidents to your cybersecurity  
390 department. As they say in the New York subway systems, “If you see something, say something.” The  
391 earlier that security personnel become aware of a phishing attack, the faster they can execute  
392 *Cybersecurity Best Practice #8: Security Operations Center and Incident Response*.

393 The following are a list of recommended channels to leverage for these awareness campaigns:

394 *Ongoing and Targeted Training* – Although these not the most effective means of awareness, phishing  
395 content should be added to your organization’s ongoing privacy and security training.

396 *Monthly Phishing Campaigns* – The most effective means of training your workforce to detect a phishing  
397 attack is to conduct simulated phishing campaigns. Your authorized security personnel or third party  
398 provider crafts and sends phishing emails to your employees. These emails are embedded with tracking  
399 components (like link clicks). Employees who detect the email as a phishing attack as well as those who  
400 don’t detect the attack and open the email or emailed links are identified with the appropriate training  
401 and feedback provided as soon as possible after the event. These methods provide a cause-and-effect  
402 training opportunity and are incredibly effective. Consider conducting phishing simulations on at least a  
403 monthly basis for the entire workforce. Specialized simulations can be developed for the higher risk  
404 areas within your organizations. These could be based on the type of department (such as finance and  
405 human resources) or on data received that identifies your highest risk users.

406 *Departmental Meetings* – Leverage departmental meetings to disseminate information on information  
407 security and cybersecurity events and trends. Brief presentations or informal conversations provide  
408 face-to-face context and build relationships between security personnel and the organization’s  
409 workforce. These relationships encourage a continuous dialogue that elevates the visibility of  
410 cybersecurity across the organization.

411 *Email Campaigns* – Leverage the email platform to deliver a pointed message or alert about specific  
412 attacks. Leverage Secure Multipurpose Internet Mail Extensions (S/MIME) or other digital certificates as  
413 evidence that these messages are authentic. Remember that the attackers will attempt to do the same  
414 thing!

415 *Newsletters* – Work independently or with your marketing departments, develop and distribute your  
416 own cybersecurity newsletter. Write articles that explain how to catch a phishing attack – better yet,  
417 provide an example of an actual phishing attack, highlighting the warning signs that might have  
418 prevented the attack.

## 419 *Advanced Practices*

### 420 **A. Advanced and Next Generation Tooling**

421 Many sophisticated solutions have been developed to help combat the phishing and malware problem.  
422 These solutions can be referred to as Advanced Threat Protection services. They use threat analytics  
423 and real-time response capabilities to provide protection against phishing attacks and malware.

424 The following list describes some of these tools:

425 *URL Click Protection via Analytics* – In a modern phishing attack, the hacker will create a web page on  
426 the Internet for the purpose of harvesting credentials or dropping malware. The hacker will conduct an  
427 email campaign, sending emails with a link to a web page that does not have malicious content. The  
428 organization’s traditional spam and anti-virus protections clear the email and it is delivered to the user.  
429 As soon as the emails are sent and delivered, the hacker changes the link’s web page to the newly

430 created malicious web page. This allows the hacker to bypass many traditional email protections and  
431 leaves the organization to rely on the user’s vigilance and awareness.

432 Protection technologies that rely on analytics leverage the ability to re-write links that are embedded in  
433 an email message. The re-written URL instead points to a secure portal that applies analytics to  
434 determine the maliciousness of the request at the time of the click. The message is protected no matter  
435 where or when it is linked. The technologies tend to leverage the cloud and numerous sensors  
436 throughout the install base to check these sites in real-time. They can also push down blocks of these  
437 discovered malicious sites ahead of time to inoculate the organization.

438 *Attachment Sandboxing* – Another common attack technique is to leverage attachments with embedded  
439 malware, malicious scripts, or other local execution capabilities that compromise vulnerabilities on the  
440 endpoint where the attachment is launched. These attachments bypass traditional signature-based  
441 blocks by leveraging multiple obfuscation techniques that alter the attachment content to provide a  
442 completely different signature.

443 Sandboxing technologies leverage virtual environments to open these attachments proactively and  
444 determine what behaviors occur after the attachment is opened. The protection system determines  
445 whether a file is malicious based on these behaviors, such as system calls, registry entry creation, file  
446 downloading and a slew of other checks.

447 *Automatic Response* – Another useful technique is to leverage mechanisms that automatically rescind or  
448 remove email messages that are categorized as malicious after delivery to a user’s mailbox. Leveraging  
449 analytics described earlier in this section, cybersecurity response teams will remove these messages  
450 from the user’s mailbox. This manual process requires assessing characteristics of the malicious email  
451 message, searching the mailbox environments in the organization and deleting messages that match the  
452 assessed characteristics. This time consuming process is difficult to run in a 24x7 operation and can be  
453 dangerous.

454 These technologies are capable of identifying the signature of a delivered email. When advanced threat  
455 tools determine that a previously clean message has become malicious, it can automatically delete that  
456 email message from all user mailboxes in the organization. This reduces the labor involved in manual  
457 processes and provides the consistency of automation.

## 458 **B. Digital Signatures**

459 Digital signatures allow a sender to leverage public/public key cryptography to cryptographically sign an  
460 email message. This does not encrypt the message itself. It validates that a received message is from a  
461 verified sender and hasn’t been altered in transit.

462 As long as trusted root certificates are used to create the S/MIME certificate used in digital signatures,  
463 most modern email clients will check and provide verification automatically through an icon on the  
464 message itself. This is useful when training your workforce to determine the validity of an email.

465 A word of caution: many email protection technologies change the content of an email messages (e.g.,  
466 tagging subject lines, re-writing URLs). Digital signature technology that maintains the integrity of an  
467 email will fail when these other protection techniques are deployed. Currently, there is no method to  
468 resolve this problem.

## 469 **C. Analytics Driven Education**

470 Cybersecurity departments leverage data and analytics from regular email protection platforms and  
471 advanced threat protection systems to identify the most frequently targeted users in your organization.

472 These users might not be the ones you think are highly susceptible, such as the CEO or Finance  
473 workforce. With the systems discussed in this section, SOCs can identify these targets and implement  
474 increased protections (e.g., lower thresholds for spam/malware checking, delayed processing time for  
475 attachments) as well as provide on-the-spot and targeted education. Informing these individuals of  
476 their high-risk profile instills a heightened sense of awareness and increased vigilance.

#### 477 *Threats Mitigated*

- 478 1. Email Phishing Attacks
- 479 2. Ransomware Attacks
- 480 3. Internal, Accidental or Intentional Data Loss

#### 481 *Suggested Metrics*

- 482 • Number of malicious phishing attacks prevented on a weekly basis. The goal is to  
483 ensure that systems are working. A reduction in attacks prevented indicates system  
484 misconfiguration.
- 485 • Number of malicious URLs / Attachments delivered via email discovered and prevented  
486 on a weekly basis. The goal is to measure the effectiveness of advanced tools, like click  
487 protection or attachment protection.
- 488 • Number of account resets on a weekly basis. This is based on users who accessed a  
489 malicious website. It assumes that a registered click indicates compromised credentials,  
490 so be sure to change the credential before it can be further compromised). The goal is  
491 to leverage education to keep this number as low as possible.
- 492 • Number of malicious websites visited on a weekly basis. The goal is to establish a  
493 baseline understanding, then strive for improved awareness through education  
494 activities that train employees to avoid malicious websites.
- 495 • Percentage of users in the organization who are susceptible to phishing attacks based  
496 on results of internal phishing campaigns. This provides a benchmark to measure  
497 improvements to the workforce's level of awareness. The goal is to reduce this  
498 percentage as much as possible, realizing that it's nearly impossible to stop all users  
499 from opening phishing emails. Secondary Goal: Potentially correlate to percentage of  
500 susceptible users to the number of malicious websites visited or number of malicious  
501 URLs that are opened.
- 502 • List of the top 10 targeted users each week with corresponding activity. For example,  
503 how many phishing emails are targeted to the top three users compared to the rest of  
504 the workforce? What positions do these users hold in the organization? Is there are  
505 correlation between the user, the user's position and the number of phishing emails  
506 received? What inferences can be made? What conclusions can be reached? The goal  
507 is to conduct targeted awareness training to these individuals, advising them that they  
508 are targeted more often than other users and increasing their vigilance as well as their  
509 ability to detect and report phishing attacks.
- 510 • Average Time to Detect and Time to Respond statistics for phishing attacks on a weekly  
511 basis. Time to Detect measures how long the phishing attack was in progress before the  
512 cybersecurity department was aware of it. Response times measure of how quickly the

513 cybersecurity department neutralizes the messages to end the attacks. The goal is that  
514 both of these metrics should be as low as possible – establish a baseline to understand  
515 current state and set goals to improve performance.

516 *References*

- 517 • (Configure your spam filter policies 2017)
- 518 • (Using RBL and DCC for spam protection 2007)
- 519 • (Use DMARC to validate email in Office 365 2017)
- 520 • (Ferrazzi 2015)
- 521

522

## Cybersecurity Best Practice #2: Endpoint Protection Systems

523 Endpoints are the assets  
 524 used by the workforce to  
 525 interface with an  
 526 organization’s digital  
 527 ecosystem. Generally  
 528 speaking, endpoints  
 529 include desktops, laptops,  
 530 workstations, and mobile  
 531 devices. Current cyber  
 532 attacks target endpoints  
 533 as frequently as networks.  
 534 Implementing baseline  
 535 security measures on  
 536 these assets provides a  
 537 critical layer of threat  
 538 management. As the modern workforce becomes increasingly mobile, it’s essential for these assets to  
 539 interface and function securely.

Best Practice 2: Endpoint Protection Systems	
Data that may be affected	Passwords, ePll, ePHI
Baseline Practices	A. Basic Endpoint Protection Controls
Advanced Practices	A. Automate the Provisioning of Endpoints B. Mobile Device Management C. Host Based Intrusion Detection/Prevention Systems D. Endpoint Detection Response E. Application Whitelisting F. Micro-segmentation/virtualization strategies
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Theft or Loss of Equipment or Data</li> </ul>

540 The endpoints that form the majority of our computing environment are no longer static devices that  
 541 exist in the healthcare organization’s main network. Organizations commonly leverage virtual teams,  
 542 mobility and other remote access methods to complete work. In some cases, endpoints rarely make it  
 543 to the corporate network. It’s important to build cybersecurity hygiene principles with these  
 544 characteristics in mind.

*Baseline Practice*

**A. Basic Endpoint Protection Controls** *(NIST Framework: PROTECT)*

547 Table 4 describes basic endpoint controls with practices to implement and maintain them.

Control	Description	Implementation Specification
<b>Antivirus (AV)</b>	Technology that is capable of detecting known malicious malware through the use of signatures, heuristics and other techniques.	<ul style="list-style-type: none"> <li>• Push AV packages out using endpoint management systems that interface with Windows and Apple operating systems (OS).</li> <li>• Develop metrics to monitor the status of AV engines, signature updates and health.</li> <li>• Dispatch Field Services/Desktop Support for malware that is detected and not automatically mitigated.</li> <li>• Leverage Network Access Control (NAC) to conduct a validation check prior to enabling network access.</li> </ul>

<p><b>Full Disk Encryption</b></p>	<p>Technology that is capable of encrypting an entire disk to make it unreadable for unauthorized individuals.</p>	<ul style="list-style-type: none"> <li>• Ensure encryption is enabled on new endpoints that are acquired by the organization.</li> <li>• Connect encryption management to endpoint management systems that interface with both Windows and Apple OS.</li> <li>• Develop metrics to monitor the status of encryption.</li> <li>• Dispatch Field Services/Desktop Support teams to resolve encryption errors.</li> <li>• Use anti-theft cable locks to lock down any device that cannot support environment.</li> <li>• Leverage NAC to conduct a validation check prior to enabling network access</li> </ul>
<p><b>Hardened Baseline Images</b></p>	<p>Configure the endpoint operating system in the most secure manner possible.</p>	<ul style="list-style-type: none"> <li>• Limit usage of local administrator accounts. Enable only those local administrative rights required by the user. Use a separate account dedicated to this purpose.</li> <li>• Enable local firewalls and limit inbound access to the endpoint to only those ports that are required.</li> <li>• Disable weak authentication hashes (e.g., LANMAN, NTLM Version 1.0).</li> <li>• Prevent software from auto-running/starting, especially when using thumb drives.</li> <li>• Disable unnecessary services and programs.</li> <li>• Permit usage only of known hardware encrypted thumb drives for writing data.</li> <li>• Review and consider the implementation of Security Technical Implementation Guides (STIG).</li> </ul>
<p><b>Patching</b></p>	<p>The process to ensure that endpoint operating systems and third party applications are patched regularly.</p>	<ul style="list-style-type: none"> <li>• Establish an endpoint management system and distribute operating system patches during regular maintenance windows.</li> <li>• Automatically update and distribute patches to third party applications that are known to be vulnerable, such as Internet browsers, Adobe Flash, Acrobat Reader, and Java.</li> <li>• Develop metrics to monitor patch status. Review on a weekly basis.</li> <li>• Dispatch Field Services/Desktop Support for endpoints that fail to patch.</li> </ul>

<p><b>Local Administrative Rights</b></p>	<p>The provisioning of privileged access to users for the purpose of installing or updating application and operating system software.</p>	<ul style="list-style-type: none"> <li>• Limit local administrative rights deployed to endpoints. Leverage endpoint management systems to install new programs and patch systems.</li> <li>• For users that require administrative rights, deploy a local account with administrative privileges that is separate from the general user account. Never allow a general user account to operate with administrative privileges as this increases vulnerability to malware and client-side attacks.</li> </ul>
---	--	--

548 *Table 4. Basic Endpoint Controls Mitigate Risk at Endpoints*

549 Organizations should reference *Cybersecurity Best Practice #5: IT Asset Management*, to determine if  
550 their endpoints meet IT Asset Management (ITAM) requirements. Examples include maintaining a  
551 proper inventory of endpoints, re-imaging endpoints as they are redeployed, and securely removing  
552 endpoints from circulation when decommissioned.

553 *Advanced Practice*

554 **A. Automate the Provisioning of Endpoints** **(NIST Framework: PROTECT)**

555 It is a challenge to manage thousands of endpoints consistently, especially when it is comprised of  
556 manually executed processes. Most organizations do not have the necessary resources to run such an  
557 operation without leveraging additional capabilities.

558 Value-Added Resellers (VARs) that sell endpoints through your supply chain can provide a mechanism  
559 that preconfigures the endpoint before delivering it to your enterprise. It requires the organization to  
560 build a “gold image” with a series of checklists and configuration procedures, which is provided to the  
561 VAR. This approach helps to ensure a consistent and resilient deployment.

562 In some cases, vendors provide the ability for an organization to provision devices centrally. For  
563 example, Apple provides this service for its devices. Leveraging the Device Enrollment Program (DEP)  
564 enables an organization to simplify enrollment and security management of the endpoint. This is  
565 accomplished by entering the serial number or order number of the new device within the DEP. That  
566 initiates a series of device configuration tasks that are specific to your organization’s requirements.  
567 Further information can be found within Apple’s Device Enrollment Program Guide. (DEP Guide 2015)

568 **B. Mobile Device Management** **(NIST Framework: PROTECT)**

569 Mobile devices, such as smartphones and tablets, present their own management challenges. Multiple  
570 security configuration options exists for these devices which should be configured consistently to  
571 comply with organizational security policies.

572 Mobile Device Management (MDM) technologies manage configurations of devices that are connected  
573 to these systems. In addition to configuration management, they may offer application management  
574 and containerization. All three options are important to consider, especially for organizations that  
575 leverage personal devices in business operations.

576 As most mobile devices travel on and off the organization’s network, it’s important to consider  
577 leveraging cloud-based MDM systems to enable consistent check-in. If cloud-based systems cannot be  
578 leveraged, then the on premise MDM systems must be accessible from the Internet through VPN  
579 connectivity or in the organization’s demilitarized zone (DMZ).

580 *Configuration Management* – At minimum, ensure that passcodes are leveraged and encryption is  
581 enabled. Ensure the device locks automatically after a predefined period of time (perhaps 1 minute).  
582 Implement device wipe functions after a series of unsuccessful logins (consider 10 unsuccessful logins).  
583 Limit the time that an email can reside on the mobile device (consider 30 days maximum).

584 Consider leveraging “Always on VPN” to protect the device when connecting to unsecured wireless  
585 networks. Consider prohibiting the installation of unsigned applications.

586 *Application Management* – Malicious applications reside in app stores and appear to be legitimate, such  
587 as PDF Readers or Netflix. In reality, these applications contain malicious code that provides access to  
588 data elsewhere on the mobile device. MDM solutions use whitelisting or blacklisting techniques to limit  
589 the installation of these malicious applications. Both should be considered, especially for devices that  
590 run on the Android platform – which is an open platform that accepts a wide range of applications.

591 *Containerization* – Organizations that leverage BYOD policies should consider containerization  
592 technologies. These technologies allow business data on a mobile device to be segmented and  
593 processed separately from personal data. In these models, business applications exist only in the  
594 hardened container on the mobile devices. Examples of these applications include email, calendaring  
595 and data repositories. This allows the organization to wipe the container and clear business data from  
596 the device when the workforce member leaves or changes position in the organization. It limits the  
597 ability for personally downloaded malicious applications to access business data.

598 **C. Host Based Intrusion Detection/Prevention Systems (HIDS/HIPS)**  
599 **(NIST Framework: DETECT)**

600 HIDS and HIPS technologies leverage an intrusion protection method similar to that used by Network-  
601 based Intrusion Detection and Prevention systems. These technologies can be deployed on the  
602 endpoint and designed specifically to detect attack patterns launched against the endpoint. These  
603 attacks can originate at the endpoint’s network, or through client-side attacks that occur when using  
604 email or browsing the web.

605 HIDS and HIPS technologies are usually managed through central management systems. They are  
606 deployed through central endpoint management systems used to manage endpoint software and  
607 patching. These types of systems should be configured to auto-update against their command server.  
608 The command servers should be configured to pull down fresh signatures of attack indicators regularly.

609 **D. Endpoint Detection and Response (EDR)** **(NIST Framework: DETECT)**

610 EDR technologies bridge the gap between execution and processing that occurs in an organization’s fleet  
611 of endpoints. These agent-based technologies allow cybersecurity departments to query large fleets of  
612 endpoints for suspicious running processes, file actions, and other irregular activities.

613 EDR enables a large-scale response to malware outbreaks. If malware is installed in the organization’s  
614 environment, cybersecurity professionals can ‘reach in’ and ‘remove’ the malware from thousands of  
615 devices using a single action. Finally, EDR technologies provide cybersecurity departments with forensic  
616 capabilities that supplement incident response (IR) processes.

617 **E. Application Whitelisting** **(NIST Framework: PROTECT)**

618 Application Whitelisting technologies permit only applications that are known and authorized to run,  
619 rather than identifying applications that should not be permitted to run. They are based on the  
620 assumption that it is impossible to identify and blacklist, or block, every malicious application.



621 Organizations should maintain a current inventory of all software resident on endpoints to facilitate  
622 complete and consistent maintenance and patching to protect against client-side attacks. (CIS Control 2:  
623 Inventory of Authorized and Unauthorized Software 2018).

624 Configuration of application whitelisting is complex and outside of the scope of this guide. Interested  
625 organizations should read NIST Special Publication 800-167: Guide to Application Whitelisting. (Guide  
626 to Application Whitelisting 2015)

627 **F. Micro-segmentation/Virtualization Strategies (NIST Framework: PROTECT)**

628 Technologies called “micro-virtualization” or “micro-segmentation” assume that the endpoint will  
629 function in a hostile environment. These technologies work by preventing malicious code from  
630 operating outside of its own operating environment. The concept is that every task executed on an  
631 endpoint (e.g., click on a URL, open a file) can be run in its own sandboxed environment and is  
632 prohibited from interoperating between multiple sandboxed environments.

633 Since most malware is installed by launching incremental processes after gaining an initial foothold, this  
634 strategy can be effective by eliminating that second launch. Additionally, once the malicious task has  
635 been completed, the microenvironment is torn down and reset. Further configuration advice for these  
636 technologies is specific to the technology deployed.

637 **Threats Mitigated**

- 638 1. Ransomware Attacks  
639 2. Loss or Theft of Equipment or Data

640 **Suggested Metrics**

- 641 • Percentage of endpoints encrypted based on a full fleet of known assets and measured  
642 weekly. The first goal is to achieve a high percentage of encryption, somewhere around  
643 99%. Achieving 100% encryption is nearly impossible as defects always exist. The  
644 percentage of endpoints encrypted will vary as new assets are discovered, which is why  
645 it should be measured weekly.
- 646 • Percentage of endpoints that meet all patch requirements each month. The first goal is  
647 to achieve a high percentage of success. A second goal is to ensure there are practices  
648 to patch endpoints for third party application vulnerabilities, as well as OS level  
649 applications, and have the ability to determine the effectiveness of those patches.  
650 Without the metric there might not be checks and balances in place to ensure  
651 satisfactory compliance with expectations)
- 652 • Percentage of endpoints with active threats each week. The goal is to ensure practices  
653 are in place to respond to AV alerts that aren’t automatically quarantined/protected.  
654 This indicates there could be active malicious action on an endpoint. An endpoint with  
655 an active threat should be reimaged using general IT practices and managed using a  
656 ticketing system.
- 657 • Percentage of endpoints that run non-hardened images each month. For this metric,  
658 the goal is to check assets for compliance with the full management IT practices,  
659 identifying those assets that do not comply. To do this, a key or token is placed on the  
660 asset indicating that it is managed through a corporate image. Separate practices need

661 to be implemented for those assets that are not managed this way to ensure they are  
662 properly hardened.

663 • Percentage of local user accounts that are configured with administrative access each  
664 week. The goal would be to keep this number as low as possible, granting an exception  
665 to only those local user accounts that require such access.

666 *References*

- 667 • (Security Technical Implementation Guides n.d.)
- 668 • (CIS Control 3: Secure Configurations for Hardware and Software on Mobile Devices,  
669 Laptops, Workstations and Servers 2018)
- 670 • (CIS Benchmarks 2018)
- 671 • (Guide to Application Whitelisting 2015)
- 672

673

## Cybersecurity Best Practice #3: Identity and Access Management

674 Identity and Access  
 675 Management (IAM) is a  
 676 program that encompasses the  
 677 processes, people,  
 678 technologies and practices  
 679 relating to granting, revoking  
 680 and managing access for users.  
 681 Given the complexities  
 682 associated with healthcare  
 683 environments, access  
 684 management models are  
 685 critical for limiting the security  
 686 vulnerabilities that can expose  
 687 organizations. A common  
 688 phrase used to describe these  
 689 programs is *“enabling the right  
 690 individuals to access the right  
 691 resources at the right time.”*

Best Practice 3: Identity and Access Management	
Data that may be affected	Passwords
Baseline Practices	A. Identity B. Provisioning, Transfers, and Deprovisioning Procedures C. Authentication D. Multi-Factor Authentication for Remote Access
Advanced Practices	A. Federated Identity Management B. Authorization C. Access Governance D. Single-Sign On (SSO)
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

692 Most access authentication methods rely on usernames and passwords which is proven to be a weak  
 693 model based on the success of phishing and hacking attacks.

694 Establishing IAM controls requires a distinct and dedicated program to accommodate its high level of  
 695 complexity and numerous points of integration. A toolkit for establishing an IAM program can be found  
 696 on the Educause. (Toolkit for Developing and Identity and Access Management Program, 2013)

697 This section will focus on the critical elements of an IAM program required to manage threats relevant  
 698 to the Healthcare and Public Health Sector.

699 **Baseline Practice**

700 **A. Identity** **(NIST Framework: PROTECT)**

701 As defined by NIST 800-63-3, *“...digital identity is the unique representation of a subject engaged in an  
 702 online transaction”* (Digital Identity Guidelines). A common principle to follow is "One person, One  
 703 identity, Multiple contexts." In healthcare, a person can have the context of a patient, payor, or even  
 704 employee of the health system. For clinical staff, one person can have one identity, but that person’s  
 705 context and ability to practice specialties will depend on context by country, practice area, or hospitals  
 706 where the person has a business or employee relationship.

707 Within the United States (U.S.), a person is are provided with a unique Social Security Number (SSN).  
 708 Similarly, a person who joins an organization should be given a unique identifier. By the way, that  
 709 unique identifier should not be used as a secret authenticator, the way a person’s SSN is often used.  
 710 The unique identifier is not the authenticator.

711 A person’s identity should be established through onboarding systems of record. The most common of  
 712 these systems is the ERP, or Human Resources (HR) System. When onboarding new employees in the  
 713 organization, HR business processes identify and establish the new employee in the organization. Many  
 714 processes are executed during onboarding, such as background checks, employment verification, and

715 preparation for payroll. They provide solid identity proofing activities that can be used to verify the  
716 employee's identity going forward. They are the trigger to generate a person's newly formed digital  
717 identity. These identity-proofing practices refer back to the need to understand a person's relationship  
718 and context within the organization(s).

719 It is imperative that IAM programs and functions align with HR business practices and business  
720 processes in general.

721 Identities maintain a series of attributes that describe common elements for the user. The series of  
722 attributes come from the system of record, whether that is an HR system, Contingent Workforce  
723 System, Medical Staffing Office, or other system in the organization's ecosystem. Examples of common  
724 elements include a person's name, location, telephone number, email address, job title/job code, and  
725 specialization/practice data.

726 Attributes from the system of record are transmitted to the IAM system, enriching the identity data and  
727 facilitating the flow of information to systems for sign on, access management, and other cyber security  
728 and business related functions. These attributes can be consumed by the organization and leveraged for  
729 future authorization components. In addition to common descriptive attributes, there may be other  
730 system-defined attributes. Further examples of this could be role or affiliations (general terms used to  
731 describe populations of individuals, such as clinicians, staff, staff nurse, visitor, student, etc.), attributes  
732 used to authorize eligibility for various systems (using techniques called Attribute Based Access Control),  
733 or other technical constructs.

734 Users defined under proper identity management processes will include more than your employees.  
735 These processes should account for and consider volunteers, locums, contractors, students, visiting  
736 scholars, visiting nurses, physician groups staff, billing vendors, visiting residents, special statuses (such  
737 as emeritus professors) and third party vendors that require access to provide services to your  
738 organization. Each of these identity types must have an approved channel to serve as the System of  
739 Record, where the identity proofing activities will occur.

740 All of this identity information can be stored in a single repository to be consumed for other purposes.  
741 IAM systems, by principle, are an aggregate of system of record data. IAM systems, by nature, should  
742 be a system of last resort when none exists (e.g., Contingent Workforce if HR/business does not have a  
743 solution). In the most basic context, the following principles should be followed:

- 744 • Enumerate all authorized sources of identity within the organization. This is often  
745 referred to as the Systems of Record. Examples of these sources include HR systems,  
746 vendor management systems, contingent workforce systems, medical staffing  
747 office/practice office, and student information systems.
- 748 • Ensure all users are provided with a unique identity and identifier. Smaller  
749 organizations without multiple constituents may consider using the Employee ID  
750 number from the System of Record. Larger organizations with many constituents  
751 should establish a unique identifier for each user and reconcile. Do not use a SSN as the  
752 unique identifier! An individual with multiple contexts should have one person  
753 record/one unique identifier that ties to all contexts.
- 754 • The integrity and uniqueness of digital identities should be maintained. Never reuse  
755 identities for different people. People come and go throughout the life of an  
756 organization. Their records should be maintained perpetually.

- 757 • Proper identity management enables the automation of functions such as system access  
758 and authentication. Enumerate and establish attributes that are critical to provide  
759 context to the identity and required for access and authentication controls. For  
760 complex and large organizations, this is an important principle to ensure consistent  
761 application of attributes and, subsequently, the ability to automate authentication and  
762 authorization needs, such as automated provisioning and de-provisioning.
- 763 • Store identity information in a database or directory capable of registering identity  
764 information and associated attributes. These are an aggregate of Systems of Record  
765 data. Consider specialized tools for organizations with multiple constituent types.
- 766 • Leverage a single namespace to establish user accounts within the organization. Tie  
767 these user accounts back to the identity so the individual can always be traced to their  
768 digital identity.

769 **B. Provisioning, Transfers and De-Provisioning Procedures (NIST Framework: PROTECT)**

770 Once digital identities and user accounts are established, users must be provisioned access to  
771 Information Systems prior to using them. It is important to ensure that provisioning processes follow  
772 organizational policies and principles, especially in the Healthcare environment.

773 Under HIPAA, a key principle relates to the Minimum Necessary rule. That is, organizations should take  
774 reasonable steps to limit uses, disclosures or requests of PHI to the minimum required to accomplish the  
775 intended purpose. These same principles reduce the attack surface of potentially compromised user  
776 accounts. By limiting access, you can limit the scope of a ransomware outbreak or data attack.

777 The following principles should be followed for provisioning:

- 778 • Identify common systems that all users will need to access and the most basic access  
779 rights required for each of those systems. This is generally considered to be “birthright  
780 entitlements.”
- 781 • Define these entitlements in organization policies, procedures or standards. There  
782 should be documentation that describes the access rights that all users are entitled to  
783 receive.
- 784 • Establish procedures and workflows that ensure consistent provisioning to birthright  
785 entitlements. Consider leveraging specialized tools to automate this process for  
786 accuracy and reliability. A best practice is not to automate bad or unknown workflows.
- 787 • Establish procedures and workflow that enable provisioning required in addition to  
788 birthright entitlements, such as auxiliary or ancillary systems. Pay special attention to  
789 cloud-based systems. Consider leveraging Federated Access Management tools that  
790 automatically provision access in the cloud.
- 791 • Consider a two-part process that allows a user to request access with a second  
792 individual required to approve the request prior to granting access. A common  
793 approach is to designate an employee’s supervisor as the approving party.

794 Leverage IT ticketing systems and build the workflow process into the ticketing system. This establishes  
795 consistency in the approval processes, automates the ability to gain approvals, and documents the  
796 access that was granted. It is important to ensure that access provisioning processes are auditable.

797 In addition to establishing a robust process to grant access to users, it is equally important to have a  
798 similar process to remove access at the right time. Failure to remove access promptly after an  
799 employee’s relationship with the organization is terminated may result in unauthorized or malicious  
800 access to systems.

801 The following principles should be followed for de-provisioning:

- 802 • Establish procedures to terminate access to user accounts. Ensure these procedures are  
803 executed promptly at the time of termination. Consider leveraging tools that automate  
804 this process after being informed by the SoR. The SoR is usually the HR systems  
805 although other systems may trigger the process to terminate access.
- 806 • Ensure your termination process, whether manual or automated, includes session  
807 termination steps to prevent active sessions (e.g. email on phone) from remaining active  
808 after the employee leaves the organization.
- 809 • Establish an “urgent termination” process, which flows outside of the normal  
810 termination procedures. These should be used when a sensitive termination process is  
811 being executed, such as an involuntary termination.
- 812 • Ensure that termination procedures include critical business systems as well as ancillary  
813 or auxiliary systems. Pay special attention to cloud-based systems that are accessible  
814 outside of the organization’s standard network. These assets will remain accessible to  
815 the user if the de-provisioning process isn’t completed. Consider leveraging Federated  
816 Access Management tools to de-provision access to cloud-based systems automatically.
- 817 • Build automatic timeouts for non-use in critical systems. These timeouts can catch edge  
818 cases where de-provisioning procedures are not executed, ultimately reducing the  
819 exposure to unauthorized access.

820 Removal of access should occur when a user terminates its relationship with the organization and when  
821 users transfer to new functions in the organization. For example, if a patient care service (PCS) manager  
822 transfers to the nursing department, access granted when the user was a PCS manager should be  
823 removed prior to granting access required by the user as a nurse. This helps to eliminate the  
824 accumulation of unnecessary access rights by a user.

825 **C. Authentication** **(NIST Framework: PROTECT)**

826 User accounts must leverage authentication techniques to properly assert the user’s identity in the  
827 digital ecosystem. The most common and, unfortunately, the weakest method for authentication relies  
828 on password credentials. That said, password-based authentication systems will be used for the  
829 foreseeable future and organizations should develop solid practices.

830 *Centralize Authentication* – Central authentication systems, such as Lightweight Directory Access  
831 Protocol (LDAP) directors or Active Directory, should be leveraged to the greatest extent possible. Tying  
832 authentication mechanisms back to these central systems enables enterprise management of  
833 credentials. The access rights of your user base can be managed from a single location. This is  
834 incredibly important when access needs to be de-provisioned in a timely and automated manner.

835 Passwords are the most common credential used to authenticate users. The strength and management  
836 of passwords are paramount. Password strength perspectives have been constructed to combat brute  
837 force or password guessing attacks. Assuming that you can limit the exposure to brute force and  
838 guessing attacks, NIST recommends the following techniques as part of SP 800-63 (SP 800-63B 2017):

- 839 • Limit the rate of speed at which authentication attempts can occur. Spacing out each  
840 password attempt by a second or two severely limits the ability of automated systems  
841 to brute force the password.
- 842 • Ensure the use of cryptographically strong hashing and salting for password storage.
- 843 • Use pass phrases in place of passwords. Require a minimum of 8 characters and permit  
844 up to 64 characters.
- 845 • Implement the use of dictionary-based password checking and compromised password  
846 black-lists. Prohibit users from establishing risky passwords.

847 *Privileged Account Management* – Centralized authentication should be leveraged for general user  
848 access and privileged administrative accounts. Privileged administrative accounts must be separate  
849 from the general user accounts. For example, an IT administrator should be provisioned a minimum of  
850 two accounts: one account for use completing day-to-day activities and a separate administrative  
851 account with access limited to those systems required by the IT administrator. This second step is  
852 critically important – the use of privileged accounts during the course of normal day-to-day business  
853 may expose these accounts to malware attacks giving an attacker elevated access to the organization’s  
854 environment. This exposure should be limited as much as possible. Consider the following controls for  
855 managing your privileged accounts:

- 856 • Rotate passwords regularly.
- 857 • Escrow privileged systems credentials, making them unique for each system or device.
- 858 • Link privileged access to problem, change or service tickets in the organization’s  
859 ticketing system.
- 860 • Require the use of a jump server when elevating privileges. Ensure full recording and  
861 auditing of the jump server.
- 862 • Require brokered access to a privileged account that registers the exact user using the  
863 privileged account and records all actions taken.
- 864 • Require multi-factor authentication for all privileged accounts used interactively.
- 865 • Conduct regular reviews of privileged access.
- 866 • Limit actions that privileged accounts can take through the use of access control lists.  
867 Check for the use of sensitive commands and alert accordingly.

868 For further details on how to securely configure privileged access, consider the following resources:

- 869 • Windows: (Implementing Least-Privilege Administrative Models 2017)
- 870 • Linux: (Controlling Root Access n.d.)

871 *Local Application Authentication* – There may be cases where applications do not support a centralized  
872 authentication model. Although there are fewer on premise systems that cannot bind to centralized  
873 authentication systems, these systems are still prevalent in the healthcare environment. As  
874 organizations migrate applications to the cloud, it’s easy to accidentally instantiate a cloud-based service  
875 that lacks robust authentication and focuses on local user accounts.

876 Whenever a local authentication system is used, solid access control procedures must be maintained to  
877 manage user accounts. This requires designating a responsible IT owner who will manage and regularly

878 review these accounts. Failure to do this allows users access to systems for longer than necessary and is  
879 especially risky when an employee leaves the organization and continues to have access to these  
880 systems. Consider the following extra controls:

- 881 • Designate an IT owner for each legacy/cloud-based system.
- 882 • Establish a distribution list in your organization which includes your IT owners as  
883 members. Submit terminations out to these IT owners as they occur.
- 884 • Ensure IT owners comply with standard operating procedures for the onboarding,  
885 review and, most importantly, termination of users.
- 886 • Regularly audit the practice of these manual processes. Ensure compliance with regular  
887 account review and termination procedures.

888 *Monitor Authentication Attempts* - Regular user accounts and privileged user accounts should be  
889 monitored for security and compliance purposes. These details are discussed further in *Cybersecurity*  
890 *Best Practice #8: Security Operations Center and Incident Response*. Details on methods to monitor  
891 these types of authentication logs can be found on the SANS white paper: (Keys to the Kingdom:  
892 Monitoring Privileged User Actions for Security and Compliance 2010).

893 **D. Multi-Factor Authentication (MFA) for Remote Access (NIST Framework: PROTECT)**

894 Multi-Factor Authentication (MFA) systems require the use of several authentication methods to verify a  
895 user's identity. MFA systems are commonly described as leveraging at least two of the following:  
896 something you know, something you have, and something you are. In these models, at least two of  
897 those three categories must be correctly addressed before the user's identity will be verified for access.

898 The most common MFA techniques are the use of passwords and one-time codes that are delivered to  
899 the user out-of-band from the authentication technique. For example, customer authentication to  
900 access sensitive banking information. Most banks have MFA capabilities, which require the customer to  
901 enter a password (something you know) followed by a verification code that is texted to the customer's  
902 smart phone (something you have). This is the most basic functionality of these systems.

903 MFA should be implemented on remote access technologies in the organization to limit the exposure of  
904 password credentials that could be compromised through phishing or malware attacks. This is the single  
905 most effective tool at limiting an attacker's ability to compromise the organization's environment.  
906 Consider implementing MFA on the following types of technologies:

907 *Virtual Private Networks (VPN)* – These are systems that allow remote network access to your  
908 environment. VPNs should be configured to limit access of the user based on RBAC or ABAC rules and to  
909 enable MFA.

910 *Virtual Desktop Environments* – These are environments where virtual terminal sessions can be exposed  
911 to remote access that allows your employees to work remotely. Although highly useful for workforce  
912 flexibility, these systems can be compromised easily without MFA authentication.

913 *Remote Email Access* – If your organization is going to permit remote email access, MFA should be  
914 enabled to limit the risk of compromised credential access in the email system. It is common for  
915 healthcare environments to store PHI with these systems and this exposure could result in a breach of  
916 sensitive information.



917 **Advanced Practice**

918 **A. Federated Identity Management (NIST Framework: PROTECT)**

919 Federated Identity Management is the mechanism that enables identity information to be shared  
920 between organizations in a trusted manner so that identities can be leveraged from home institutions  
921 inside of a greater ecosystem. In healthcare organizations, it is commonplace for providers, payors, and  
922 other affiliates to work together in an integrated manner. In complex, large environments, multiple  
923 organizations operate in a joint model, with different HR practices inside each of the systems.

924 Rather than creating identities in each organization involved in this joint operation, the use of federated  
925 identity management tools and processes allows identity assertions of the home institutions to be used  
926 throughout the federation.

927 Consider the following example: a clinician is part of a practice group that is credentialed within a  
928 regional hospital. From the hospital's perspective, this clinician is not an employee but must be  
929 credentialed and cleared through the medical staff office with access to the electronic medical record.  
930 From the practice group's perspective, this clinician has been on-boarded through standard HR  
931 background checks and processes. If the practice group and the hospital were operating within a  
932 federation, the clinician's "home" identity could be established from the practice group and asserted to  
933 the hospital as part of the clearance processes. If the clinician's relationship with the practice group  
934 changes, this identity information would be revoked within the hospital based upon asserts from the  
935 federation. These processes would be completely automated.

936 The same model can be leveraged when working with third party vendors who have a large workforce  
937 that provides support or staff-augmentation capabilities. In this model, the third party is the "home  
938 institution" that requires access to resources in the organization. To monitor the activities of each of  
939 those workforce members would be a highly complicated and largely manual process that is likely to be  
940 ineffective. A federation can solve this problem.

941 In complex environments such as large integrated delivery networks, federations are almost a  
942 requirement to properly manage the temporal aspects of the identities within.

943 **B. Authorization (NIST Framework: PROTECT)**

944 After authentication has occurred, the mechanism to obtain specific access in an information resource,  
945 such as an application system, is referred to as authorization. Authorization processes check the level of  
946 access that has been granted to a particular credential, and assures that the credential can access only  
947 those areas that are pre-authorized. Consider the analogy of traveling at the airport. When you pass  
948 through the security lines, your identity is authenticated and then you are authorized to access the  
949 terminals based on a ticket for a particular flight. You are not permitted to access any other flight than  
950 the one authorized on your ticket.

951 The limitation of authorization is a critical component, required by the HIPAA Privacy rule under  
952 Minimum Necessary. In addition to HIPAA compliance, Minimum Necessary is a leading practice to limit  
953 malicious use of credentials. In most cases, when hackers break into systems, they are trying to access  
954 the "keys to the kingdom" – privileged access credentials that permit access to the most sensitive  
955 resources. Don't risk unauthorized access by granting more access than necessary to your users!

956 Consider the following techniques to limit authorization to only those components required by the user:

957 *Role Based Access Control (RBAC)* – Conduct a high-level role mining exercise to map out the role types  
958 that exist within your organization and the access they require. For example, identify access

959 requirements for clinicians, support staff, unit secretaries, switchboard operators, case managers, and  
960 others. The clinician may need access to the medical record (though not necessarily the entire medical  
961 record), and the support staff cannot need access at all. By defining the unique requirements for these  
962 two roles, you have started on the path towards differentiating access models.

963 It can be difficult to provision granular-based authorization models based on a user's role. In  
964 Healthcare, two individuals might have the same job title and role, yet complete different tasks within  
965 the organization. Relying solely on a person's role to grant access will limit the ability for the other  
966 authorized responsibilities.

967 *Attribute Based Access Control (ABAC)* – Attribute based authentication models considers the attributes  
968 associated to a user's identity, the attributes of the information system being accessed, and the context  
969 associated with the access request. In this model, a user may be granted an attribute through a  
970 standard workflow process to enable the user to be granted access to a specialized function in an  
971 information system, but only during business hours or only while on premise. When the user requests  
972 this access, ABAC systems check the specific context against these factors to determine if access should  
973 be granted. (Attribute Based Access Control 2018).

974 This highly effective model limits access based on user-specific rules established in the ABAC systems  
975 that define access parameters. As an example, a request is made to grant all nurses with access to all  
976 patients on a specific floor in a specific hospital to support flexible care requirements. You might be  
977 concerned that this access is excessive since the nurse might not be part of a care team for a particular  
978 patient. To minimize this impact, you can leverage ABAC, limiting the access to the time when the nurse  
979 is present at a specific hospital and only after the nurse has been authenticated using both a password  
980 and multifactor authentication. These particular access credentials cannot be used to grant remote  
981 access to the same patients or anywhere else within the healthcare system. In this model, a hacker with  
982 access to the password and the multi-factor authentication mechanism would be unable to access the  
983 patient using those credentials.

984 **C. Access Governance** **(NIST Framework: IDENTIFY)**

985 On-boarding processes and system access request processing are the most active times during the  
986 whole establishment of access process. Once access is established for a user, it can be a challenge to  
987 determine if that access continues to be required at a given time in the future. Consider the employee  
988 who has worked for an organization for a long time, serving in multiple capacities, placed on special  
989 projects and working throughout the organization. Over time, this employee might accumulate more  
990 access than was ever intended.

991 Conducting a manual review of each employee's access to each of an organization's critical application  
992 systems would be nearly impossible. Fortunately, specialized tools are available that automate these  
993 processes, providing this capability in a self-service capacity to an organization's leadership. These  
994 processes are generally referred to as Access Governance. Below are the relevant components:

995 *Tooling* - Specialized tools bind to identity management systems and connect to critical business systems  
996 to understand the access in place for all users in these systems. These tools need the ability to connect  
997 and parse through specific aspects of the applications in question, such as electronic medical records  
998 systems, revenue cycle systems, imaging systems, lab systems, and more.

999 *Access rules* – Within the tools, specialized rules can be defined based on roles or attributes of users in  
1000 the organization. For example, it would be important in a financial system to define the difference in  
1001 roles between accounts payable and accounts receivable. No employee should be capable of access

1002 with both roles. Otherwise, a fraudulent purchase order could be generated and the invoice paid by the  
1003 same person, resulting in a fraud loss to the organization. Understanding the characteristics and  
1004 requirements of these critical roles enables you to create automated alerts that control user access.

1005 In addition to the standard segregation of duties checks, some specialized tools compare access profiles  
1006 of certain users in a role to determine if outliers exist. For example, these systems can look at the  
1007 accesses that nurses generally have across multiple systems, set a baseline of access based on the  
1008 normative manner of these accesses, and compare each user against that baseline. A specific nurse’s  
1009 profile that is determined to have excessive access can be reviewed for appropriate adjustments.

1010 *Access Review* – Through workflows established with these advanced tools, supervisors within the  
1011 organization can review the access that their employees currently have in critical environments. This  
1012 can be done on a regular cadence established by policy. In the case where an employee has retained  
1013 access that is no longer necessary, the manager can use self-service portals to identify these access  
1014 violations and flag them for removal. In some systems, once the manager flags an access for removal, it  
1015 will be automatically stripped.

1016 At the end of an access review, the manager can certify and sign off that the review is accurate. This  
1017 documentation is useful for audit practices and to demonstrate effective reviews.

1018 **D. Single-Sign On (NIST Framework: PROTECT)**

1019 Federated Single-Sign On (SSO) is an effective method to authenticate users against centralized  
1020 credential repositories. SSO techniques abstract authentication principles away from the general  
1021 Microsoft- or Linux-based methods into a generalized standard that can be implemented cross-platform.  
1022 These standards conduct authentication processes securely and pass additional identity attribute  
1023 information for authorization processes in the resources being accessed. Lastly, it has the benefit of  
1024 requiring only one login during a particular time frame while an active SSO session is enabled. Get rid of  
1025 those pesky password prompts!

1026 Several federated SSO standards exist, including OpenID, Security Assertion Markup Language (SAML),  
1027 OAuth and Active Directory Federation Services (ADFS). When implementing cloud-based systems, such  
1028 as Software-as-a-Service (SaaS) systems, the use of SSO should be a security requirement.

1029 Another SSO system model leverages a second authentication factor at a clinical workstation for easy  
1030 access within a healthcare provider space. These systems can be configured to require a user to  
1031 authenticate once per day/shift at a clinical workstation after accessing a clinical setting through use of a  
1032 password and key card. Subsequent authentications are conducted by tapping the key card to provide  
1033 secure, easy access to the clinical workstations. These systems provide multi-factor access to the clinical  
1034 environment while easing the password authentication processes.

1035 **Threats Mitigated**

- 1036 1. Ransomware Attacks  
1037 2. Internal, Accidental or Intentional Data Loss  
1038 3. Attacks Against Connected Medical Devices that can Affect Patient Safety

1039 **Suggested Metrics**

- 1040 • Number of alerts generated for excessive access to common systems. For example,  
1041 “allow any” permissions to core applications SharePoint, file systems, etc.

- 1042 • Number of users with privileged access, trended over time. The primary goal is to  
1043 establish a baseline of the normal number of privileged accounts and monitor variances  
1044 from the baseline.
- 1045 • Number of automated terminations, trended over time. The goal is to establish a  
1046 baseline for normal terminations and monitor variances from that baseline. A decrease  
1047 in the amount of terminations can indicate that the automated systems are not  
1048 terminating access properly.
- 1049 • Number of elevated privileged access requests, trended over time. The goal is to  
1050 establish a baseline to determine how much privileged access is generated over a one-  
1051 week period and monitor variances from that baseline.

1052 *References*

- 1053 • (Attribute Based Access Control 2018)
- 1054 • (Controlling Root Access n.d.)
- 1055 • (Implementing Least-Privilege Administrative Models 2017)
- 1056 • (Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance  
1057 2010)
- 1058 • (Digital Identity Guidelines n.d.)
- 1059 • (SP 800-63B 2017)
- 1060

1061 **Cybersecurity Best Practice #4: Data Protection and Loss Prevention**

1062 All organizations within the  
 1063 Healthcare and Public Health  
 1064 Sector access, process and  
 1065 transmit sensitive information,  
 1066 such as health information or  
 1067 personally identifiable  
 1068 information. The fundamental  
 1069 data used in operations is highly  
 1070 sensitive, representing a unique  
 1071 challenge to the Healthcare and  
 1072 Public Health Sector. The  
 1073 majority of the workforce in  
 1074 Healthcare must leverage these  
 1075 data to carry out their respective  
 1076 missions.

Best Practice 4: Data Protection and Loss Prevention	
Data that may be affected	Passwords, ePII, ePHI
Baseline Practices	A. Classification of Data B. Data Use Procedures C. Data Security D. Backup Strategies E. Data Loss Prevention (DLP)
Advanced Practices	A. Advanced Data Loss Prevention B. Mapping of Data Flows
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Loss of Theft of Equipment or Data</li> <li>• Accidental or Intentional Data Loss</li> </ul>

1077 With that backdrop, Healthcare faces a growing challenge of understanding where data assets exist,  
 1078 how they are used and how they are transmitted. On any given day, PHI is being discussed, processed  
 1079 and transmitted between information systems. Protecting these data requires robust policies,  
 1080 processes and technologies.

1081 As your organization starts shoring up its data protection and prevention controls, it’s best to begin by  
 1082 understanding the type of data that exist in the organization, setting a classification schema for these  
 1083 data, then determining how the data are processed. Establish a set of policies and procedures for  
 1084 normal methods of data use and then build in ‘guardrail’ systems to guide your user base towards these  
 1085 business processes.

1086 **Baseline Practice**

1087 **A. Classification of Data (NIST Framework: IDENTIFY)**

1088 There is a vast proliferation of data in Healthcare environments. They can range from the obvious  
 1089 records, including treatment information, billing information, and personally identifiable information  
 1090 (e.g., social security numbers, insurance numbers, driver’s license numbers) to research information. It  
 1091 includes the non-obvious, but still important, information such as business strategies and development  
 1092 plans, business finances, employee records, and corporate board materials.

1093 Before establishing policy describing how these varied data types should be used and disclosed, it’s best  
 1094 to classify them into high-level categories that provide a consistent framework when developing policies  
 1095 and procedures. Table 5 provides an example of a classification schema with examples of the types of  
 1096 documents that comprise the classification.

Classification	Description	Examples
<b>Highly Sensitive Data</b>	Data that could easily be used for financial fraud, or	Social security number, credit card number, mental health information,

	could cause significant reputational damage.	substance abuse information, sexually transmitted infections/disease.
<b>Sensitive Data</b>	Regulated data, or data that could cause embarrassment to patients or organizations.	Health information, clinical research data, insurance information, human/employee data, board materials.
<b>Internal Data</b>	Data that is not considered sensitive, but should not be exposed publicly.	Policies and procedures, contracts, business plans, corporate strategy and business development plans, internal business communications.
<b>Public Data</b>	All data that has been sanitized and approved for distribution to the public with no restrictions on use.	Materials published on websites, presentations, and research publications.

Table 5. Example of a Data Classification Schema

1097

1098 **B. Data Use Procedures**

(NIST Framework: IDENTIFY)

1099 After data have been classified, procedures can be written that describe how to use these data in the  
 1100 organization based on their classification. These types of procedures include the process of setting  
 1101 usage expectations and labeling the information properly.

1102 *Usage and Disclosure* – Based on the classification type, data use should be limited appropriately and  
 1103 disclosed in specific methods. Consider the procedures in Table 6:

Classification	Use	Disclosure
<b>Highly Sensitive</b>	1. Must be restricted to only those individuals who have a need to know. 2. Must use extreme caution when handling data.	Only share information internally <u>and</u> only when expressly permitted <u>and</u> when directed by the data owner.
<b>Sensitive</b>	3. Must be restricted to only those individuals who have a need to know.	Only share information internally <u>and</u> only when expressly permitted.
<b>Internal Use</b>	4. Data can be generally used, but care should be considered in its consumption.	Only shared information internally within the organization.
<b>Public</b>	5. No restrictions.	Shared freely shared with no restrictions.

1104

Table 6. Suggested Procedures for Data Disclosure

1105 Be careful when sending information through email. Ensure that sending PHI via email is consistent with  
1106 ONC guidance. Do not send unencrypted PHI through regular email or text, unless patients have  
1107 expressly requested receiving their PHI via this means.

1108 *Labeling* – It is important to label information properly to facilitate implementation of restrictions  
1109 related to its usage and disclosure. This helps keep the data secure through a few methods. First of all,  
1110 users will understand how to handle information that is properly labeled. Second, specialized security  
1111 tools, such as Data Loss Prevention systems, can be configured to discover and control information  
1112 when it is properly labeled.

1113 At minimum, the labeling process should be done so that it is readily apparent when viewing the  
1114 information or documenting its classification. Leverage techniques such as placing the classification in  
1115 the footer of the document. Collaborate with your marketing and communication departments to  
1116 create document templates based upon these sensitivity types. Leveraging organization-wide document  
1117 templates enables specialized tokens or signatures to be embedded in the documents and tracked by  
1118 Data Loss Prevention systems.

1119 **C. Data Security** **(NIST Framework: PROTECT)**

1120 Once policies and procedures have been defined, you can establish additional data security methods.  
1121 Consider the security methods described in Table 7.

Security Method	Description	Considerations
<b>Encryption Data At Rest</b>	Ensure data are encrypted when resident on file systems.	<ul style="list-style-type: none"> <li>When using Cloud, enable native encryption capabilities to prevent exposures if cloud provider is hacked.</li> <li>Ensure full disk encryption is enabled on all workstations and laptops.</li> </ul>
<b>Encryption In Transit</b>	Ensure secure transport methods are used for both internal and external movement.	<ul style="list-style-type: none"> <li>Ensure websites accessed that contain sensitive data use encrypted transport methods, such as hypertext transfer protocol secure (HTTPS).</li> <li>Enable internal encryption methods when moving data in the organization.</li> <li>Never send unencrypted sensitive data outside of the organization.</li> </ul>
<b>Data Retention and Destruction</b>	Ensure retention policies are set. Contractually bind third parties to destroy data when terminating contracts.	<ul style="list-style-type: none"> <li>Use standard destruction forms and require vendors to attest data has been destroyed pursuant to those forms.</li> <li>Set retention policies and quote limits on email systems to reduce the amount of data</li> </ul>

		<p>that can be exposed. Ensure that legal retention requirements are met.</p> <ul style="list-style-type: none"> <li>• Establish a purge strategy that includes purge mechanisms.</li> </ul>
<b>Scrub production data from Test and Development environments</b>	<p>Ensure that identifiable information is removed when replicating production environments for testing.</p>	<ul style="list-style-type: none"> <li>• Leverage specialized tools to de-identify data elements within large systems (such as EMRs).</li> <li>• Regularly audit data elements within test and production environments to ensure they are clean.</li> </ul>
<b>Mask Sensitive Data within Applications</b>	<p>Restrict users from accessing highly sensitive information, such as SSNs, by masking it unless authorized.</p>	<ul style="list-style-type: none"> <li>• Permit SSN access only to those members who require it (e.g., registration desks, admitting desks, payor processing).</li> </ul>
<b>Limit ability to print / save / export data based on function</b>	<p>Restrict the workforce's ability to export data out of systems that contain sensitive data without proper authorization.</p>	<ul style="list-style-type: none"> <li>• Encourage users to work within applications. Minimize data exporting by providing the required capabilities to manipulate data within the application.</li> <li>• Implement restrictions on data exports, especially in reporting or database systems that can query and return large datasets.</li> <li>• Potentially remove the ability to print and copy/paste EMR applications or web mail accessed from home.</li> </ul>

1122

*Table 7. Security Methods to Protect Data*

1123

**D. Backup Strategies (NIST Framework: PROTECT)**

1124

A robust backup strategy for enterprise assets is critically important to daily IT operations. It is equally important to have such a backup strategy in the event of cybersecurity incidents. There will be events that cause an asset, or multiple assets, to be thoroughly compromised. During these events, these routine backups can be the only way to ensure proper execution of the Recovery phase of your IR process. A full decommission and restore to a time before the compromise occurred is the best method to neutralize the compromise.

1130

At minimum, each mission critical asset in your environment should have a backup plan. Backups can be executed using a variety of methods, the most common being disk-to-tape, disk-to-disk, or disk-to-cloud

1131



1132 backups. The integrity of these backups is paramount: these copies are your last line of defense and  
1133 you want to make sure they are complete and accurate when you need them.

1134 *Disk-to-Tape* – This method makes backups by accessing designated systems and files and writing all the  
1135 content to a tape drive, or a tape library. Specialized software, hardware and inventory controls are  
1136 required. To conduct backups efficiently, you will need the appropriate tape robots and a tape library  
1137 that is based on the number and size of systems being backed up. These backups can be very large.  
1138 You'll want to configure a Write Once and Read Many (WORM) option with the tapes. It is of utmost  
1139 criticality that encryption is enabled in the writing to these tapes. If a tape is lost or stolen, you do not  
1140 want to have a breach of sensitive data.

1141 There are great advantages to maintaining offline backups. You can rely on these copies to be available  
1142 when you need them, and attacks against the backup medium itself are as they are offline.

1143 *Disk-to-Disk* - This method involves taking backup copies from a disk and replicating them to a separate  
1144 disk storage array that is dedicated to maintaining backup copies. This option is generally lower cost  
1145 than the other tape strategies discussed in this section. Disk-to-disk backups generally executes more  
1146 quickly than disk-to-tape. It is important to execute encryption strategies on the backup file, in case the  
1147 file is copied outside of the organization.

1148 It's important to consider access control of the disk storage system as part of a disk-to-disk approach.  
1149 With cyberattacks like ransomware, attackers intent to disrupt production and backup files. Attackers  
1150 that launch ransomware attacks are aware that an organization's first response will be to contain the  
1151 ransomware and then restore the uncorrupted files from a backup source. If they can compromise the  
1152 backup and production files, there is a much higher likelihood that the organization will pay a ransom to  
1153 get their files back. Access control mechanisms should limit access from the system being backed up to  
1154 the disk array to only those access channels. Do not permit other access to the array from other  
1155 accounts, including administrative accounts. Remember, everyone can be a potential target of a  
1156 ransomware attack, especially administrators.

1157 *Disk-to-Cloud* – This method is very similar to the disk-to-disk backup. Cloud backup offers multiple  
1158 added values, however. With a disk-to-cloud backup, you automatically get the resiliency and flexibility  
1159 of the cloud environment as well as the benefits from investments made by the cloud providers to  
1160 maintain 100% data availability. Rather than a single-point-of-failure model in backup plans like a disk-  
1161 to-disk or even disk-to-tape, cloud providers replicate data backups leveraging a cloud infrastructure  
1162 with multi-fault tolerant capabilities.

1163 As with the disk-to-disk model, it's important to limit access to the cloud backup storage to only the  
1164 systems and disks that are backed up and the data repository. Never implement a drive that maps to  
1165 the backup repository. That mapped drive could be the vehicle that delivers the ransomware  
1166 encryption. Always encrypt backup files to protect your organization if the cloud provider is breached.

1167 Lastly, whatever method of backup is used, it's important to test the recovery of these backups on a  
1168 periodic basis to ensure data availability. As mentioned previously, your backup process is the last line  
1169 of defense and must be demonstrated to be trustworthy in a time of need.

1170 **E. Data Loss Prevention (DLP) (NIST Framework: PROTECT)**

1171 Once standard data policies and procedures are established and the workforce is trained to use them,  
1172 Data Loss Prevention (DLP) systems should be implemented to ensure that sensitive data are used in  
1173 compliance with these policies.

1174 Multiple DLP solutions exist and can be applicable depending on the types of data access channels that  
 1175 need to be monitored. Traditionally, DLP systems monitor channels that include email, file storage,  
 1176 endpoint usage, web usage, and network transmission. All these channels should be considered.

1177 A challenge with DLP systems is to determine which methods will be used to positively identify sensitive  
 1178 information. Within a healthcare environment, that can be tricky. Generally, there are two approaches  
 1179 and both have limitations:

- 1180 • Identify sensitive data based on dictionary words that may trigger the inclusion of  
 1181 sensitive data. These dictionaries include robust language repositories that identify  
 1182 health information. The challenge with this technique is related to the terminology.  
 1183 Medical terms are used in the regular course of business without being attributed to any  
 1184 particular sensitive information. This can lead to a high rate of false positives, forcing  
 1185 the workforce to apply prevention practices that are not necessary.
- 1186 • Identify sensitive data based up identifiers that are known to be sensitive. This may  
 1187 include leveraging tokens that are embedded in documents classified as sensitive and  
 1188 the actual identifiers used for patients. When leveraging document identifiers, the  
 1189 number of false positive rates will be drastically reduced. However, the workforce must  
 1190 be trained on the proper classification. When leveraging actual identifiers used for  
 1191 patients, the false positive rates will be lower as it is positive confirmation. This requires  
 1192 extracting information from the EMR in a regular cadence to load these identifiers into  
 1193 the system. Extra precautions must be taken so that these large data sets are not  
 1194 exposed.

1195 Once your identification methodology is established, DLP systems can be configured to monitor data  
 1196 access channels of interest and make policy decisions based on the data types and the access channel.  
 1197 It's best to provide direct feedback to the user when the data policy has been violated to avoid  
 1198 recurrence. This real-time feedback will help users to adjust their data usage behaviors. Data channels  
 1199 are presented in Table 8 for your consideration.

Data Channel	Implementation Specification	Considerations
<b>Email</b>	Implement inline through SMTP routing for email messages being delivered outside of the organization.	<ul style="list-style-type: none"> <li>• Define thresholds of risky behavior. Implement a DLP block for these thresholds (e.g., over 100 records of PHI in the email).</li> <li>• Define thresholds of risky behavior. Implement a DLP encrypt action for these thresholds, forcing the message to be encrypted before delivered.</li> </ul>
<b>Endpoint</b>	Install DLP agents on managed endpoints that can apply data policies.	<ul style="list-style-type: none"> <li>• Standardize and deploy encrypted thumb drives to users that require mobile storage options.</li> <li>• Prevent the copying of data to unencrypted thumb drives, or force encryption when copying data.</li> </ul>

		<ul style="list-style-type: none"> <li>Control the use of non-controlled peripherals and/or storage devices (e.g., backup of iPhones on devices). Permit only when specifically authorized.</li> <li>Conduct data discovery scans of data resident on endpoints – exposing data on the endpoint so the user can make data destruction decisions.</li> </ul>
<b>Network</b>	Implement through Switched Port Analyzer (SPAN) ports from egress network points or through Internet Content Application Protocol (ICAP) on web proxies.	<ul style="list-style-type: none"> <li>If online, prevent the leakage of identified unencrypted sensitive data based upon thresholds defined (e.g., files that contain 100 records of PHI).</li> <li>If out of band, activate IR procedures to contain data leakages that occur through the network.</li> </ul>

Table 8. Data Channels Enforce Data Policies

1200

1201

1202 **Advanced Practice**

1203 **A. Advanced Data Loss Prevention**

(NIST Framework: PROTECT)

1204 After implementing basic DLP controls, you should consider expanding your DLP capabilities to monitor  
 1205 other common data access channels. Table 9 recommends methods for your consideration.

Data Channel	Implementation Specification	Considerations
<b>Cloud Storage</b>	Leverage cloud access security broker (CASB) systems to monitor data flows into cloud systems.	<ul style="list-style-type: none"> <li>Label data identified as sensitive. Implement digital rights and encryption to limit access to sensitive data.</li> <li>Ensure that cloud storage file systems and shares do not expose sensitive data in an “open sharing” construct without authentication (i.e., do not permit the use of sharing data through a simple URL link).</li> </ul>
<b>On Premise File Storage</b>	Point discovery scanning systems at known file servers or other large data repositories.	<ul style="list-style-type: none"> <li>Conduct regular DLP scans against the file systems to scan and identify sensitive data.</li> <li>Leverage tools to query security access permissions for each file that contains sensitive data. Define thresholds for excessive access and set alerts if these are crossed. Forward alerts to the SOC for response as described in <i>Cybersecurity Best Practice #8: Security Operations Center and Incident Response</i>.</li> </ul>

		<ul style="list-style-type: none"> <li>• Determine staleness of records with sensitive data. Consider executing data destruction practices for records that have not been opened or viewed for an extended period of time.</li> <li>• Determine data ownership of sensitive files identified in file storage systems, leveraging automated tools. Establish workflow options that allow the data owner to provide input into access permission reviews of their sensitive files.</li> </ul>
<b>Web Based Scanning</b>	Configure DLP systems to crawl known public websites for sensitive information.	<ul style="list-style-type: none"> <li>• Conduct a “spearing” exercise, similar to methods deployed by search engines. Compare files and results posted on websites against DLP matching policies and respond quickly to any sensitive data that is exposed.</li> <li>• Conduct manual searching activities on a periodic basis over exposed websites. Look for files that may contain large amounts of sensitive data (e.g., XLS(X), CSV, TXT and PDF).</li> </ul>

1206 *Table 9. Expanded DLP for Other Data Channels*

1207 **B. Mapping of Data Flows** **(NIST Framework: IDENTIFY)**

1208 After data business practices are defined, it’s advisable to describe these processes in a data map. Data  
 1209 maps should include the following components: applications that house sensitive data, standard  
 1210 direction movement of data, users of applications and data, and methods used to store and transmit  
 1211 data.

1212 Conducting this type of mapping and potentially adding to a larger Enterprise Architecture (EA)  
 1213 reference architecture enables an organization to identify data protection and monitoring requirements.

1214 **Threats Mitigated**

- 1215 1. Ransomware Attacks
- 1216 2. Loss or Theft of Equipment or Data
- 1217 3. Internal, Accidental or Intentional Data Loss

1218 **Suggested Metrics**

- 1219 • Number of encrypted email messages, trended by week. The goal is to establish a  
 1220 baseline of encrypted messages sent. Be on the lookout for spikes of encryption (which  
 1221 could indicate data exfiltration) and no encryption (which could indicate that encryption  
 1222 is not working properly).
- 1223 • Number of blocked email messages, trended by week. The goal is to detect large  
 1224 numbers of blocked messages which could indicate potential malicious data exfiltration  
 1225 or user education training.

1226  
1227  
1228

- Number of files with excessive access on the file systems, trended by week. The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets and deliver to access management

1229  
1230

- Number of unencrypted devices with access attempts, trended by week. The goal is to use this information to educate the workforce on the risks of removable media.

1231 *References*

1232  
1233

- (SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) 2010)

1234

1235

## Cybersecurity Best Practice #5: IT Asset Management

1236 The process by which  
 1237 organizations manage IT assets  
 1238 is generally referred to as IT  
 1239 Asset Management (ITAM).  
 1240 ITAM is critically important to  
 1241 understand and ensure that  
 1242 proper cyber hygiene controls  
 1243 are in place across all assets in  
 1244 the organization. These  
 1245 processes increase the visibility  
 1246 of cybersecurity professionals  
 1247 in the organization and reduce  
 1248 the unknowns.

1249 ITAM processes should be  
 1250 implemented for endpoints,  
 1251 servers and networking equipment. The best practices in this section assist and support every other  
 1252 best practice identified in this publication. ITAM best practices can be difficult to implement and  
 1253 sustain. They should be baked into every life cycle stage of IT operations to establish and sustain data  
 1254 accuracy and integrity. For each asset, this includes procurement, deployment, maintenance, and  
 1255 decommissioning. Though each type of asset deploys different methods during its life cycle, the life  
 1256 cycle itself is consistent.

1257 The Financial Sector, as part of its public-private partnership with NIST National Cybersecurity Center of  
 1258 Excellence (NCCOE), has written a detailed ITAM best practice guide. Though specific to the Financial  
 1259 Sector, the methodologies discussed in the guide are easily applied to the Healthcare and Public Health  
 1260 Sector. *NIST Special Publication 1800-5b: IT Asset Management 2015*

Best Practice 5: IT Asset Management	
Data that may be affected	Passwords, ePII, ePHI
Baseline Practices	E. Inventory of Endpoints and Servers A. Procurement B. Secure Storage for Inactive Devices C. Decommissioning Assets
Advanced Practices	D. Asset Pre-Configuration E. Automated Discovery and Maintenance A. Integration with Network Access Control
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Loss of Theft of Equipment or Data</li> <li>• Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

1261 **Baseline Practice**

1262 **A. Inventory of Endpoints and Servers (NIST Framework: IDENTIFY)**

1263 The first ITAM component that should be implemented is a build out of the inventory repository. This  
 1264 critical technology component provides a normalized, consistent approach that organizations can use to  
 1265 store inventory data.

1266 Important data elements should be captured for each asset in the ITAM, including the following:

- 1267 • AssetID (primary key)
- 1268 • Hostname
- 1269 • Purchase Order
- 1270 • Operating System
- 1271 • MAC Address
- 1272 • IP Address
- 1273 • Deployed to (User)

- 1274 • Last Logged on User
- 1275 • Purchase Date
- 1276 • Cost
- 1277 • Physical Location

1278 The build out of a robust ITAM becomes your single source of truth for all IT assets in your organization.  
1279 This repository will be maintained and trusted to be highly accurate and actionable.

1280 Special consideration should be given to the differences between ITAM systems and device  
1281 management systems. Device management systems, which connect to IT devices such as endpoints and  
1282 servers, can automate the management and maintenance of these assets. They are highly effective at  
1283 executing tasks such as software discovery, patch management and monitoring performance. Device  
1284 management systems cannot account for the addition and removal of IT assets or answer the inevitable  
1285 question, “where did that laptop go?” They manage an organization’s devices at a single point in time  
1286 and are not workflow driven.

1287 IT Service Management tools (e.g., ticketing systems) can be integrated with IT General Controls to  
1288 ensure accuracy and precision of assets through standard performance management activities. (CIS  
1289 Control 1: Inventory of Authorized and Unauthorized Devices 2018)

1290 **C. Procurement** **(NIST Framework: IDENTIFY)**

1291 Once the ITAM system is implemented and configured, it is important to tie normal supply chain  
1292 processes with the ITAM processes. The goal is to leverage supply chain processes to proactively  
1293 register each technology asset, endpoint, server or networking equipment into the ITAM system as it is  
1294 acquired.

1295 To achieve this, IT organizations must work with Supply Chain departments to streamline technology  
1296 acquisition channels. When technology acquisitions are specifically categorized, a trigger can be  
1297 established to capture details of each technology purchase. At a minimum, this can be the generation of  
1298 a ticket in the IT ticketing systems that prompts a designated IT professional to manually capture details  
1299 for the new asset when it is acquired. This can be accomplished physically at a shipping dock, or  
1300 virtually for virtual technology purchases.

1301 In more advanced organizations, the procurement process may be automated to capture salient details  
1302 for an asset. This reduces the manual labor required and exposure to human error collecting the data.

1303 As the asset is acquired, it is critical to tag it with an asset tag. These tags can be physical or logical. The  
1304 most important aspect of the tagging process is ensure that the asset has a unique ID that will be used  
1305 to identify it in the ITAM system. Using other fields (e.g., hostname, IP address, MAC address) as the  
1306 unique ID may cause complications as these fields may change, potentially creating a duplicate record.

1307 **D. Secure Storage for Inactive Devices** **(NIST Framework: IDENTIFY)**

1308 Assets that are not in circulation should be returned to the appropriate IT department for secure  
1309 storage. Storage areas (e.g., lockers, cages, rooms) should be secured with physical access controls.  
1310 Access should be limited to those who require it. Physical access controls may include badge readers,  
1311 video camera surveillance, and door alarms.

1312 If an asset is identified for redeployment, it should be securely imaged to deploy a “fresh” computer  
1313 system for the new user. This ensures that old sensitive data is removed and the asset has a clean bill of  
1314 health.

1315 When an asset is sent to storage for redeployment or processing, the ITAM system should be updated to  
1316 reflect a change of ownership and new physical location (i.e., storage) for the asset. If the asset is  
1317 redeployed or decommissioned, the ITAM system should be updated again to reflect its new status.

1318 **E. Decommissioning Assets** **(NIST Framework: PROTECT)**

1319 It is critically important to properly dispose of retired assets. These assets may contain sensitive  
1320 information. When executing destruction and certification procedures, update the ITAM to indicate that  
1321 the device has been decommissioned. This establishes a permanent record in your asset management  
1322 source of truth, the ITAM. The following procedures should be completed when decommissioning an IT  
1323 asset.

1324 *Central Collection* – IT assets should be collected and stored in centralized, physically locked areas prior  
1325 to decommissioning. Your workforce must be trained to turn in any asset that they no longer use.

1326 *Central Destruction/Wipe* – Assets that are collected for decommission must complete a secure process  
1327 to destroy or electronically wipe the storage media. This ensures that devices are properly sanitized  
1328 before leaving the organization’s possession for destruction. Permanent removal of storage media may  
1329 be completed by your IT organization or an external service provider. It is a good practice to obtain and  
1330 archive a certificate of destruction for audit purposes.

1331 *Record Keeping* – Once the IT asset has been cleared for removal from the organization, the ITAM record  
1332 of the asset information should be registered for destruction or decommissioning. The certificate of  
1333 destruction can be stored in the ITAM record for easy access. It’s highly advisable not to delete the  
1334 asset record. Instead, update the asset’s status in the ITAM system to reflect that it is decommissioned  
1335 and no longer owned by the organization. You may need to refer to the asset record in the future.

1336 **Advanced Practice**

1337 **A. Asset Pre-Configuration** **(NIST Framework: PROTECT)**

1338 Most large Value Added Resellers (VARs) can preconfigure an asset being purchased by the organization  
1339 before shipping it to the organization. This is most commonly used for user workstations and laptops,  
1340 but may be completed with server-based software.

1341 In this method, IT organizations build a “gold-image” for the asset. This image is a fully configured  
1342 template that includes IT and cybersecurity baselines. A series of tasks are identified that are normally  
1343 completed by the IT department, such as establishment of encryption, installation of antivirus, and  
1344 registration of the asset in the ITAM.

1345 Providing these standard tasks to the VAR enables an organization to outsource this common work to  
1346 third party providers who are contractually bound to complete it accurately and consistently. This  
1347 provides a higher level of assurance that assets acquired by the organization are properly configured  
1348 and secured.

1349 **B. Automated Discovery and Maintenance** **(NIST Framework: IDENTIFY)**

1350 Once your ITAM system is in place and your procurement processes are registered, the challenge is to  
1351 maintain these records. A fictitious example describes a common IT asset in a large organization with  
1352 the following characteristics:



- 1353 • Number of endpoints: 10,000
- 1354 • Number of servers: 1,000
- 1355 • Number of data elements managed per asset: 11
- 1356 • Total number of data elements required to maintain accurate details: 121,000

1357 It is very difficult to manually maintain 121,000 data elements. After an asset is acquired by an  
 1358 organization, it is often deployed throughout its lifecycle in unforeseen ways. For example, a new  
 1359 laptop may be issued to a user. That user may leave the organization, turning in the laptop to a  
 1360 supervisor. The supervisor may assign the laptop to the new employee who fills the open position.  
 1361 Unless IT is informed and ITAM is updated, the asset record for the laptop, now assigned to a different  
 1362 user, will be wrong.

1363 Another classic example relates to an upgrade or hardware change to an existing asset. This asset might  
 1364 change operating system or patch levels. Maintaining that information manually in the ITAM is nearly  
 1365 impossible.

1366 Automated discovery systems can maintain these records and account for both scenarios described  
 1367 above. In the case where an asset changes hands to a new user, discovery tools can register login  
 1368 occurrences for the “assigned user” and for the “actual logged in user.” If a threshold is triggered  
 1369 indicating that the assigned user no longer logs in and a different user continually logs in, that may  
 1370 prompt a change in ownership workflow. This workflow may be automated without requiring  
 1371 intervention or manually completed by generating a ticket to validate the change of ownership. In the  
 1372 case of OS and patching levels, automated discovery systems can provide snapshot views of current  
 1373 patching levels for assets. When these snapshots are compared by cybersecurity vulnerability  
 1374 management systems, vulnerabilities due to obsolete software versions will be identified across the  
 1375 fleet.

1376 **C. Integration with Network Access Control (NIST Framework: PROTECT)**

1377 The practices outlined so far assume normal processes for acquisitions. There are times, however, when  
 1378 IT assets are integrated in the organization by means other than standard supply chain channels.  
 1379 Examples include personal devices (referred to as Bring-Your-Own-Device, or BYOD) and assets that are  
 1380 donated or provided free-of-charge as part of a third party contract.

1381 Without an oversight function, it is difficult to detect and track these assets. These outliers can be  
 1382 controlled by integrating your Network Access Control and ITAM systems. Further details can be found  
 1383 in *Cybersecurity Best Practice #6: Network Management*.

1384 **Threats Mitigated**

- 1385 1. Ransomware Attacks
- 1386 2. Loss or Theft of Equipment or Data
- 1387 3. Internal, Accidental or Intentional Data Loss
- 1388 4. Attacks Against Connected Medical Devices that May Affect Patient Safety

1389

*Suggested Metrics*

1390

1391

1392

- Percentage of devices added to asset management system through procurement channels, trended over time. The goal is to establish a baseline and achieve a higher percentage over time.

1393

1394

1395

- Number of devices added to the ITAM as a result of NAC, trended over time. The goal is to analyze spikes that occur after initial deployment and may indicate a problem capturing or maintaining asset records.

1396

1397

1398

1399

- Number of devices properly removed from asset management system using proper decommissioning channels, trended over time. The goal is to ensure devices are properly decommissioned. Lack of execution of these processes over a period of time may indicate a compliance issue.

1400

*References*

1401

1402

1403

1404

1405

- (NIST SPECIAL PUBLICATION 1800-5b: IT ASSET MANAGEMENT 2015)
- (CIS Control 1: Inventory of Authorized and Unauthorized Devices 2018)
- (FIPS 199: Standards for Security Categorization of Federal Information and Information Systems 2004)

1406

## Cybersecurity Best Practice #6: Network Management

1407 Organizations leverage IT  
1408 networks as a core  
1409 infrastructure to conduct  
1410 business operations. Without  
1411 networks, there would be no  
1412 interoperability capability. It is  
1413 equally critical to deploy  
1414 networks securely to limit  
1415 exposure to and potential  
1416 impacts of cyber attacks.

Best Practice 6: Network Management	
Data that may be affected	-
Baseline Practices	A. Network Profiles and Firewalls B. Network Segmentation C. Intrusion Prevention Systems D. Web Proxy Protection E. Physical Security of Network Devices
Advanced Practices	A. Additional Network Segmentation B. Command and Control Monitoring of Perimeter C. Anomalous Network Monitoring and Analytics D. Network Based Sandboxing/Malware Execution E. Network Access Control (NAC)
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Loss of Theft of Equipment or Data</li> <li>• Accidental or Intentional Data Loss</li> <li>• Medical Devices and Patient Safety</li> </ul>

1417

1418

1419

1420

1421

1422

1423

1424

### Baseline Practice

#### A. Network Profiles and Firewalls

(NIST Framework: PROTECT)

1427 An effective network management strategy includes the deployment of firewalls to enable proper  
1428 access inside and outside of the organization. Firewall technology is far more advanced than standard  
1429 router based access lists, and is a critical component of modern network management. Organizations  
1430 should deploy firewall capabilities throughout the following areas: on WAN pipes to the Internet and  
1431 perimeter, across data centers, in building distribution switches, in front of partner WAN/VPN  
1432 connections and over wireless networks.

1433 There should be clear boundaries that determine how traffic is permitted to move throughout the  
1434 organization, leveraging a default-deny rule set whenever possible. At the perimeter, inbound and  
1435 outbound rules must be configured with a default-deny rule set to limit accidental network exposures.  
1436 This often complicated process can be achieved by establishing security zones through network  
1437 segmentation.

1438 Consider limiting the outbound connections permitted by assets in your organization. This can be a  
1439 challenge to implement across the board. However, for particular zones of high sensitivity, egress  
1440 limiting can prevent malicious callbacks or data exfiltration. The SOC should monitor these egress logs.

1441 Firewall rules may change when technology is added or removed. A robust change management  
1442 process should include reviewing every firewall to identify necessary changes. These change requests  
1443 should comply with standard IT Operations Change Management processes and be approved by  
1444 cybersecurity departments before any firewall is modified.

1445 As part of standard rule management for firewalls, it's important to periodically review firewalls to  
1446 ensure they are properly structured as required by cybersecurity teams. Consider a monthly or  
1447 quarterly review of the highest risk rule sets.

1448 **B. Network Segmentation** **(NIST Framework: PROTECT)**

1449 A fundamental method to limit cyberattacks is the practice of partitioning networks into security zones.  
1450 These zones can be based on sensitivity of assets within the network (e.g., clinical workstations, general  
1451 user access, guest networks, medical device networks, building management systems, IOT networks) or  
1452 standard perimeter segmentations (e.g., DMZ, middleware, application servers, database servers,  
1453 vendor systems). Examples of standard network zones are:

1454 *Perimeter Defenses* – Most organizations host services that are accessed through the Internet. A robust  
1455 defense strategy should be deployed to monitor these “front doors” (CIS Control 12: Boundary Defense  
1456 2018).

1457 Best practices for perimeter defenses include:

- 1458 • Implement highly restrictive rules on inbound and outbound ports and protocols.  
1459 Leverage default-deny rules in firewalls and enable access only when clearly  
1460 understood.
- 1461 • Restrict DMZ from Middleware, Application and Database servers. DMZ controls are  
1462 critical as these servers are exposed to the Internet and have a large threat footprint.
- 1463 • Restrict the ability for DMZ servers to log in directly to servers on the inside network,  
1464 specifically using remote desktop protocol (RDP), server message block (SMB), secure  
1465 shell (SSH) or other remote access ports (tcp/3389, tcp/445, tcp/139, tcp/22).
- 1466 • Ensure that local administrator passwords are unique to each DMZ server and do not  
1467 use these passwords for any other server in the organization.
- 1468 • Ensure that DMZ servers cannot connect directly to the Internet. Instead, these servers  
1469 should access the Internet through outbound proxy services. Outbound proxy rules  
1470 should limit the sites, URLs, IPs and ports that a DMZ server can access to only those  
1471 whitelisted sites required for updates or application functionality. Be cautious of  
1472 whitelisting hosting organizations like AWS: they may be used by malicious actors to  
1473 download malware to a compromised server.
- 1474 • Consider this type of posture for partner WAN links or site-to-site VPN connections. Do  
1475 not permit access to systems/applications that are not required by the user.

1476 *Data Center Networks* – Servers in the data center should be segmented into appropriate zones. Several  
1477 different layers of segmentation may occur within the Data Center networks, including

- 1478 • Database servers;
- 1479 • Application Servers; and
- 1480 • Middleware.

1481 *Critical IoT Assets* – It is important to restrict access to assets that have a potentially high impact to the  
1482 business or patients if compromised. A common factor of these devices is that management and  
1483 patching of security vulnerabilities may be limited. Examples include medical devices, security cameras,  
1484 badge readers, temperature sensors, and building management systems. Generally speaking, these

1485 assets exist outside of the data centers. Without proper segmentation, they may infiltrate general  
1486 access networks. To achieve segmentation in the physical buildings, leverage multiprotocol label  
1487 switching (MPLS) to build out virtual networks and place these restrictions behind core firewalls.

1488 *Vendor Access* – Vendor access should be limited based on need. It should be temporary and provided  
1489 only to access required information. Some assets are managed exclusively or accessed by third party  
1490 vendors. These vendors may need continual access to the organization’s network. It’s important to  
1491 segment this vendor access from other networks and limit the vendor’s ability to access other parts of  
1492 your corporate network. Whether these networks exist inside or outside of the data center, the  
1493 principles are the same. In 2015, Target was the victim of a cyberattack leveraging these exact channels  
1494 (Anatomy of the Target data breach: Missed opportunities and lessons learned 2015). Common  
1495 examples include building management systems, security systems, physical access controls, and  
1496 persistent tunnels required to enable cloud functionality.

1497 *General Access Networks* – The vast majority of your workforce will operate on general access networks.  
1498 These are “edge” networks that provide connectivity back to the services offered in data centers, the  
1499 Internet, or other assets. These networks require a sense of openness when communicating with  
1500 services that are hosted by the organization. However, restrictions should be implemented that prohibit  
1501 the assets in one general access network from communicating with the assets in another general access  
1502 network. This critical control that can help stop the outbreak and spread of malware and ransomware  
1503 attacks.

1504 *Guest Networks* – It is common for most organizations to provide guest access to the Internet. This is  
1505 especially important in provider organizations visited by patients and their friends and families. Access  
1506 to the Internet is a core value of provider organizations. However, it must be restricted and controlled  
1507 appropriately. These restrictions should exist on wireless networks, where it is most common, as well as  
1508 wired networks often located in public spaces or conference rooms. Explicitly prohibit access to the  
1509 internal network: guest users should access the organization through the same front door as the rest of  
1510 the Internet. Lastly, as much as possible, limit the ability of your workforce to access guest networks.

1511 **C. Intrusion Prevention Systems (NIST Framework: PROTECT)**

1512 An Intrusion Prevention System (IPS) is important for your network perimeter, data center and partner  
1513 connections. These systems are capable of reading network traffic to detect and potentially prevent  
1514 known attacks.

1515 Today, the effectiveness of these signature-based systems is not as prevalent as they used to be.  
1516 However, they do serve as vital input to an organization’s SOC that provide context to the types of  
1517 attacks that occur. Though they might not identify every single attack, they provide information you’re  
1518 your IR team to conduct forensic capabilities.

1519 **D. Web Proxy Protection (NIST Framework: PROTECT)**

1520 Web proxy systems provide incredibly important protections against modern phishing and malware  
1521 attacks. These systems are implemented at the perimeter of the network or in the Cloud to provide  
1522 protections for your mobile workforce. As most of these attacks are web-based, web proxy systems  
1523 provide users with friendly error pages explaining that the user has been restricted from accessing a  
1524 known malicious website. This is great feedback for users. When configured properly, web proxy  
1525 systems leverage the following methods to limit client-side attacks:

1526 *Reputation Blocking* – Many blackhole lists are available publicly or through ISACs/ISAOs that prevent  
1527 users from accessing malicious websites. These are usually fed into proxy systems through automated  
1528 list and feeds.

1529 *Organizational Block Lists* – As part of an organization’s IR, malicious websites and other sites can be  
1530 identified based on actual attacks against the organization. Web proxy systems are critical shut-off  
1531 points to limit access to websites quickly.

1532 *Category Blocking* – Most modern and commercial web proxy technologies will pre-categorize websites  
1533 on behalf of the organization. Considering the millions of websites that exist, this is an incredibly useful  
1534 service. Consider blocking categories that contain malicious, suspicious, or illegal websites.

1535 **E. Physical Security of Network Devices (NIST Framework: PROTECT)**

1536 Network devices are deployed throughout an organization’s facilities. Inside the general user space,  
1537 physical data closets that contain network devices must be secured. Additionally, it is useful to limit  
1538 network ports on switches. Consider the following controls:

- 1539 • Data and network closets should be locked always. Consider using badge readers instead of  
1540 traditional key locks to monitor access.
- 1541 • Disable network ports that are not in use. Ensure that procedures are in place to maintain ports  
1542 in shutdown mode until an activation request is submitted and approved.
- 1543 • Establish guest networks in conference rooms that are configured to access only these  
1544 networks.

1545 **Advanced Practice**

1546 This section includes methods to detect and potentially prevent cyberattacks against an organization’s  
1547 network. These methods should be engineered into network management practices. Once established,  
1548 cybersecurity departments can follow *Cybersecurity Best Practice #8: Security Operations Center and*  
1549 *Incident Response* to monitor and respond to attacks on the network.

1550 **A. Additional Network Segmentation (NIST Framework: PROTECT)**

1551 As your network expands, other strategies can be deployed to maintain secure segmentation. Consider  
1552 the following:

1553 *Required VPN Access for Data Center* – Consider leveraging a VPN, or bastion hosts, that must be  
1554 enabled before access is granted to privileged servers in the data center. These VPN or bastion hosts  
1555 should have Multi-Factor Authentication. Only authorized IT administrators should be granted access.  
1556 Logs should be routed to the SOC for monitoring.

1557 **B. Command and Control Monitoring of Perimeter (NIST Framework: DETECT)**

1558 Layered command and control (C2) traffic is a common mechanism used by hackers to maintain access  
1559 to compromised computers. These are beacons, typically outbound from the computer, that check back  
1560 in to a central server. This control can detect where an attacker has maintained persistence. There are  
1561 many methods to look for C2 traffic. These include:

1562 *Direct to compromised server via Internet Protocol (IP) or Internet Control Message Protocol (ICMP)* – In  
1563 this method, traffic runs over the network using outbound ports or protocols that are generally open  
1564 (e.g., HTTP, HTTPS or ICMP protocols). C2 traffic can be encrypted or cleartext, depending on the  
1565 attacker’s level of sophistication. The attacker must have compromised a series of servers or stood up

1566 virtual servers that are accessible. This method tends to be less effective than others as it is easy to shut  
1567 down offending systems once the compromise has been detected. When shut down occurs, the  
1568 attacker loses persistence control.

1569 *DNS queries* – In this method, the attacker establishes control using a DNS query embedded in malware  
1570 that is downloaded to a computer. As long as the DNS record is maintained, the servers that maintain  
1571 C2 communications can switch out and flex as they are discovered. Generally speaking, this method is  
1572 also fairly easy to detect and resolve. When the DNS name has been identified, the organization can  
1573 implement a DNS Sinkhole. This Sinkhole can be an entry on the local cache in the organization’s DNS  
1574 resolvers to remove a non-existent IP address, such as 127.0.0.1. Once the Fully Qualified Domain Name  
1575 is identified, these DNS registrations can be taken down through Abuse reporting to DNS hosting  
1576 services.

1577 *Fast flux DNS queries* – In this method, the hacker leverages DNS to maintain persistence, knowing that  
1578 the DNS registrations will likely be taken down at some point. When this occurs, malware downloaded  
1579 to the local client and C2 services runs an algorithm that checks the first several bytes of well-known  
1580 sites (e.g., cnn.com, nbc.com) to create and register fake DNS names on the organization’s DNS  
1581 resolvers. These domains tend to live for 24 hours or less. Using the same algorithm, the clients switch  
1582 to the next domain until command is re-established. These methods are fairly successful. Defense  
1583 mechanisms for Fast Flux DNS queries require analytics that relate to local DNS lookups and discover  
1584 “gibberish” domain names. “Oiewr921ai.evil.com” is an example of a gibberish domain name.

1585 **C. Anomalous Network Monitoring and Analytics (NIST Framework: DETECT)**

1586 A variation on C2 monitoring is to analyze network traffic, rather than focus on a particular vector or  
1587 attack style. This requires specialized technologies that can profile inbound and outbound network  
1588 traffic. Some versions of these tools provide “Deep Inspection,” which allows the full contents of a  
1589 packet to be analyzed, categorized and built into massive databases of network-based metadata.

1590 Once metadata is gathered on the network traffic profile, analytics can be conducted to look for outliers,  
1591 anomalous traffic, and other highly sophisticated methods of discovery. These tools are not  
1592 preventative in nature. They are intended to widely increase the SOC’s visibility, facilitating detection,  
1593 confirmation or validation of suspicious actions. These tools are highly useful in replaying events that  
1594 occurred as part of an attack to support network forensic activities.

1595 **D. Network Based Sandboxing / Malware Execution (NIST Framework: DETECT)**

1596 By monitoring common protocols that allow downloading of binaries and files, organizations can check a  
1597 download prior to permitting it to run on the organization’s devices. These binaries, executables, or  
1598 even data files (e.g., docx, xlsx) are run in a virtual environment that looks for malicious activities when  
1599 the file executes.

1600 Common methods include:

- 1601 • Watching what registry keys are queries, amended, added, or deleted;
- 1602 • Monitoring for outbound network connections;
- 1603 • Launching processes in memory; and
- 1604 • Conducting anomalous system calls.

1605 Tools that facilitate automated sandboxing look for suspicious outputs or actions rather than attempting  
1606 to base actions on a particular signature of a particular configuration.

1607 To be effective, these technologies monitor network flows. This can occur passively or actively. Passive  
1608 systems monitor network traffic at the stream level, not residing in line with the communication flows.  
1609 Active systems insert themselves inline to the communication flows and conduct checks on the fly,  
1610 denying access to downloaded files until they are cleared.

1611 These systems provide protection against malicious files. However, they do not provide protection  
1612 against active attacks inside your network.

1613 **E. Network Access Control (NAC) (NIST Framework: PROTECT)**

1614 NAC systems are engineered to automatically profile new IT assets that connect to network resources,  
1615 such as wireless networks, wired networks or VPN. They help ensure that the controls discussed in  
1616 *Cybersecurity Best Practice #2: Endpoint Protection* are in place on each asset. NAC systems execute  
1617 these controls on a real-time basis when the asset connects to the network.

1618 NAC systems are highly effective at discovering personal devices leveraged on the network (BYOD).  
1619 They can be configured to permit authorized BYOD devices to access the network or prohibit them  
1620 entirely.

1621 When basic NAC controls are implemented and you can monitor the security of endpoints that connect  
1622 to your network, there are other interesting and advanced techniques that can be leveraged to provide  
1623 checks and balances for general IT controls.

1624 One example is to integrate your NAC solution with your ITAM repository. As discussed in *Cybersecurity*  
1625 *Best Practice #5: IT Asset Management*, ITAM repositories should be populated using your organization's  
1626 standard procurement processes. That said, not all processes run perfectly and there are other ways  
1627 that assets are integrated into an organization's environment. This often occurs due to human error or  
1628 sidebar procurement channels that are not leveraged consistently.

1629 Configuring your NAC solution to check against your ITAM enables assets to be profiled spontaneously,  
1630 providing self-directed work streams to users. This can be achieved by doing the following:

- 1631 • Set up application programming interfaces (API) between the NAC solution and the  
1632 ITAM solution that enable read and write options.
- 1633 • Query the ITAM database when an asset connects to the network. If the asset does not  
1634 exist, present the user with a splash page.
- 1635 • Determine if the asset is organizationally owned (purchased with organizational funds)  
1636 or personally owned (purchased by the user).
- 1637 • Register the selection, conduct the NAC security scan, and publish the results in the  
1638 ITAM.
- 1639 • Execute IT general controls that reconcile assets that are out of compliance with  
1640 standard Asset Management procedures. This can include:
  - 1641 ○ Ensuring that appropriate monitoring controls are in place;
  - 1642 ○ Registering the asset with the right identifiers (Asset IDs); and,
  - 1643 ○ Updating asset ownership based on actual human interaction.

1644 These highly effective mechanisms provide visibility into the actual devices being used on the network,  
1645 increasing ITAM accuracy and consistency.



1646 **Threats Mitigated**

- 1647 1. Ransomware Attacks
- 1648 2. Loss or Theft of Equipment or Data
- 1649 3. Internal, Accidental or Intentional Loss of Sensitive Data
- 1650 4. Attacks Against Connected Medical Devices that May Affect Patient Safety

1651 **Suggested Metrics**

- 1652 • Number of assets on the network that have not been categorized, trended over time.  
1653 The goal is to establish a process to register and understand all assets on the network.  
1654 After the baseline is complete, minimize the number of uncategorized assets.
- 1655 • Number of organizationally owned assets discovered using NAC that were not  
1656 previously categorized through Asset Management procedures, trended by month. The  
1657 goal is to monitor this lagging metric that measures effectiveness of the supply chain  
1658 and IT operations processes. Increases in the number of organizationally owned assets  
1659 that were not previously categorized indicates that standard processes are not being  
1660 executed properly. Implement continuous improvement processes for IT operations.
- 1661 • Percentage of assets that comply with security policies, trended by week. The goal is to  
1662 establish a baseline, then set stepwise goals to improve compliance over time.  
1663 Ultimately, compliance percentage should range from 95% to 99%.
- 1664 • Number of malicious files captured/secured with advanced networking tools  
1665 (sandboxing), trended by week. The goal is to capture all malicious files. An extended  
1666 trend of no detected malicious files may indicate that sandboxing solutions are not  
1667 working.
- 1668 • Number of malicious C2 connections discovered and removed, trended by week. The  
1669 goal is a weekly report that shows all detected C2 connections are mitigated  
1670 successfully.
- 1671 • Number of approved servers/hosts in the DMZ compared to hosts in the DMZ, trended  
1672 by week. The goal is for zero servers/hosts in the DMZ that are not understood. IT  
1673 Operations practices should be reviewed if servers are added that were not previously  
1674 authorized.

1675 **References**

- 1676 • (CIS Control 12: Boundary Defense 2018)
- 1677
- 1678

1679

## Cybersecurity Best Practice #7: Vulnerability Management

1680 Vulnerability management is  
 1681 used by organizations to  
 1682 proactively conduct  
 1683 vulnerability discovery  
 1684 processes. These processes  
 1685 enable the organization to  
 1686 classify, evaluate, prioritize,  
 1687 remediate, and mitigate the  
 1688 technical vulnerability  
 1689 footprint from the perspective  
 1690 of an attacker. The ability to  
 1691 mitigate vulnerabilities before  
 1692 a hacker discovers them gives  
 1693 a competitive edge to the  
 1694 organization along with time to address these vulnerabilities in a prioritized fashion.

Best Practice 7: Vulnerability Management	
Data that may be affected	-
Baseline Practices	A. Host/Server Based Scanning B. Web Application Scanning C. System Placement and Data Classification D. Patch Management, Configuration Management, Change Management
Advanced Practices	A. Remediation Planning
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Ransomware Attacks</li> <li>• Insider, Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices</li> </ul>

1695 Vulnerability scanning comes in multiple flavors. Generally speaking, the most well-known methods are  
 1696 scans against servers (or hosts) and against web applications. Both scan types focus on different  
 1697 considerations.

1698 **Baseline Practice**

1699 **A. Host/Server Based Scanning (NIST Framework: DETECT)**

1700 In this model, vulnerability scanners are leveraged to identify weaknesses in an operating systems or  
 1701 third party application that resides on a server. There are two types of scan options: unauthenticated  
 1702 and authenticated.

1703 In the unauthenticated model, the scanner has no extra sets of server privileges and queries the server  
 1704 based on ports that are active and present for network connectivity. Depending on the level of  
 1705 sophistication of the software scanner, each server is queried and checked for vulnerabilities. Scan  
 1706 results provide the perspective of an attacker who lacks server access. Vulnerabilities that rate high in  
 1707 this space should be mitigated first, as they are the most likely entry points to the server for a hacker.

1708 Authenticated scans are conducted by letting the vulnerability scanner log in to the server and query all  
 1709 running software with all running versions. The vulnerability lists are usually compared against a  
 1710 database (maintained by the scanner’s vendor) and vulnerabilities are enumerated based on known  
 1711 disclosed issues from the known software version. While this type of scanning provides a much higher  
 1712 degree of accuracy of the enumeration of the vulnerability, it doesn’t necessarily provide context that  
 1713 describes how the vulnerability may be exploited. The other advantage of this type of scan is that it will  
 1714 identify client-side vulnerabilities that may exist on the server and otherwise be difficult to discover,  
 1715 such as vulnerable versions of Java.

1716 Most scanning systems can categorize vulnerabilities against the MITRE Common Vulnerability Scoring  
 1717 System (CVSS). The CVSS system helps organizations to prioritize identified vulnerabilities which enables  
 1718 development of a prioritized response. Version 3 of the system considers the following three factors:  
 1719 Base Score, Temporal Score, and Environmental Score. These factors along with sub-factors are used to

1720 calculate vulnerabilities on a scale ranging from one to ten. For more information, refer to (Common  
1721 Vulnerability Scoring System SIG n.d.).

1722 **B. Web Application Scanning** (NIST Framework: DETECT)

1723 In this model, specialized vulnerability scanners are leveraged that interrogate a running web  
1724 application to check for vulnerabilities in the application design. Most web applications run dynamic  
1725 code, run atop of a web server, interact with middleware, and connect to databases. If the web  
1726 application is not coded securely, this architecture may enable access to data or systems in ways that  
1727 are unanticipated.

1728 Common and popular attack types of web applications include structure query language (SQL) Injection,  
1729 Cross-Site Scripting, and Security Misconfigurations. In these cases, attackers can:

- 1730 • Bypass web application security controls and pull data directly from the database;
- 1731 • Steal an already authenticated cookie on a vulnerable website to get access; or
- 1732 • Leverage misconfigurations that can permit properly formatted commands or scripts to  
1733 execute privileged content on the webserver itself.

1734 More information can be found on the Open Web Application Security Project (OWASP) Top 10 Website  
1735 (OWASP Top 10 - 2017: Ten Most Critical Web Application Security Risks 2017).

1736 In all cases, vulnerabilities to web applications with sensitive information represent a high risk to the  
1737 organization. It is important to understand these vulnerabilities to conduct appropriate and prioritized  
1738 remediation.

1739 **C. System Placement and Data Classification** (NIST Framework: IDENTIFY)

1740 Organizations should leverage *Cybersecurity Best Practice #4: Data Protection and Loss Prevention* and  
1741 *Cybersecurity Best Practice #5: IT Asset Management* to understand IT assets and asset classifications.  
1742 These best practices answer the question, “How bad would it be if this asset was breached?”

1743 It is important to understand the exposure of each system in your environment. Organizations should  
1744 leverage *Cybersecurity Best Practice #6: Network Management* to determine the likelihood that each  
1745 this system can be compromised.

1746 The level of risk related to vulnerabilities in your systems is directly related to the exposure of these  
1747 systems and the types of data they contain.

1748 **D. Patch Management, Configuration Management, and Change Management**  
1749 (NIST Framework: PROTECT)

1750 All organizations should have a routine activity to patch security flaws in their servers, applications  
1751 (including web applications), and third party software. Although the patching process may vary, large  
1752 organizations should leverage centralized systems to interrogate servers and determine which software  
1753 updates should be implemented.

1754 At least monthly, organizations should implement patches that are produced by the vendor community.  
1755 IT Operations should collect these patches, conduct appropriate regression tests to ensure each patch  
1756 does not negatively impact the business, and schedule patch implementation during routine change  
1757 windows. This process should be executed and measured using standard IT Operations activities.

1758 Not all vulnerabilities are created equal. Some are easier to exploit than others. The National  
1759 Vulnerability Database (NVD) has produced the CVSS. The CVSS is a standard measurement across all  
1760 industries that normalizes and ranks the severity of a particular vulnerability. (NVD NIST 2018)

1761 Generally speaking, the more a particular vulnerability is exposed, the higher priority an organization  
1762 will assign to mitigate it. Exposure may be more critical than the actual impact to an asset considering  
1763 that hackers attempt to gain a foothold on organizational assets before conducting additional internal  
1764 attacks. Another factor to consider is the level of active exploitability in the wild. A lower criticality  
1765 vulnerability may have an active threat against it. In these cases, organizations might want to consider  
1766 proactively executing IR processes, organizing the response team and quickly patching systems. The  
1767 WannaCry exploit of 2017 was a classic example of organizations identifying an active threat and quickly  
1768 implementing patches that were previously neglected.

1769 If your systems are running end of life OS or software, associated vulnerabilities should be identified and  
1770 steps taken to bring these systems back to a supported state. This may include decommissioning  
1771 application systems that run on unsupported OS, which may require additional investments by the  
1772 organization. Once systems are unsupported, it is generally impossible to apply security patches. This  
1773 may increase the organizations risk posture.

1774 Table 10 provides general guidelines to plan remediation efforts based on criticalities.

Vulnerability Criticality	Days to Mitigate in DMZ	Days to Mitigate in Data Center
<b>Critical</b>	< 14 days	< 30 days
<b>High</b>	< 30 days	< 90 days
<b>Medium</b>	< 90 day	< 180 days
<b>Low</b>	< 180 days	At your discretion

1775 *Table 10. Vulnerability Criticalities Drive Mitigation Timeframes*

1776 The vulnerability scanning process is a quality check on the effectiveness of an organization’s patch  
1777 management practice, otherwise referred to as a “lagging metric.” Organizations with a robust patch  
1778 management practice are better positioned to mitigate residual vulnerabilities.

1779 In addition to conducting routine patch management activities, organizations should ensure that proper  
1780 security configuration management activities are in place. Common vulnerabilities can be introduced in  
1781 systems with insecure configurations. Examples of insecure configuration includes permitting an FTP  
1782 server to allow anonymous login, making that login accessible to the Internet, or failing to change  
1783 default account passwords on applications. Organizations that follow *Cybersecurity Best Practice #2:*  
1784 *Endpoint Protection Systems* and expand those practices to their servers will be positioned to minimize  
1785 these issues.

1786 Lastly, consideration needs to be given to changes made to systems, servers, and networks along with  
1787 the vulnerabilities that may be exposed as a result. A testing plan should be part of the change  
1788 management process. It should include a vulnerability scan of new network connectivity (such as a  
1789 firewall change) or a new system function or service. This scan should be conducted during the test

1790 phase of the change process, before the change is implemented into the production environment. This  
1791 enables the identification and mitigation of security exposures.

1792 **Advanced Practice**

1793 **A. Remediation Planning (NIST Framework: PROTECT)**

1794 It is important to better classify and prioritize vulnerabilities that remain after completion of standard  
1795 patch management practices. These are issues that generally cannot be mitigated with a patch. They  
1796 may require system configuration changes, code updates, or perhaps even a full-blown version upgrade.  
1797 The process of resolving these vulnerabilities tends to be more time-consuming and complex.

1798 Similar to risk management activities, remediation efforts should be prioritized to resolve identified  
1799 vulnerabilities. The most common practice is to first patch identified vulnerabilities and rescan the  
1800 system to validate the vulnerability is closed. Most vulnerability scanning systems have the ability to  
1801 track the opening, closure, and reopening of vulnerabilities over time. It is highly encouraged to  
1802 leverage these metrics for institutional tracking.

1803 Mitigation of some vulnerabilities requires far more effort than a simple patch. In these cases, it is best  
1804 to develop structured remediation plans that include the following elements:

1805 *Remediation Owner* – The single individual accountable for ensuring the vulnerability, or vulnerabilities,  
1806 are addressed. It is important to assign a single owner on remediation plans otherwise they are likely to  
1807 stall due to a lack of leadership.

1808 *Plan* – A full description of the remediation plan to be completed. This plan should be developed by the  
1809 remediation plan owner and security office. Once the plan is approved, execution tasks can be started.

1810 *Stakeholders* – The individual stakeholders who are responsible for completing tasks in the remediation  
1811 plan, or organizing other individuals who will complete these tasks. This may include individuals who  
1812 need to be informed of remediation activities as well as individuals who actually complete the work.

1813 *Dates* – Major milestone dates and remediation plan due dates must be captured on the remediation  
1814 plan. This is an incredibly important commitment that must be made by the Remediation Owner.

1815 *Status* – Periodically, the plan should be updated to remain current. This generally occurs between once  
1816 a week to once a month. The Remediation Owner may be accountable for providing status updates.

1817 After a remediation plan is completed, a monitoring process should be implemented by the  
1818 organization’s information security office. This monitoring process may include all remediation plans in  
1819 progress and current activities. The security office may provide support to those activities that are  
1820 behind schedule. Consider operating such a monitoring process once a week to keep good traction.

1821 **Threats Mitigated**

- 1822 1. Ransomware Attacks  
1823 2. Internal, Accidental or Intentional Data Loss  
1824 3. Attacks Against Connected Medical Devices that May Affect Patient Safety

1825 **Suggested Metrics**

- 1826 • Stacked aggregate of vulnerabilities in DMZ trended by month, with vulnerabilities  
1827 categorized using CVSS categories (Critical, High, Medium, Low, None) and plotted as a  
1828 simple stacked bar. The goal is to mitigate the most severe vulnerabilities first through

1829 patching and configuration management. Of the remaining vulnerabilities, the most  
1830 critical should be mitigated within 30 days. The total number of vulnerabilities should  
1831 be reduced over time.

1832 • Stacked aggregate of vulnerabilities in data center trended by month, with  
1833 vulnerabilities categorized using CVSS scores and plotted as a simple stacked bar. The  
1834 goal is to mitigate the most severe vulnerabilities first through patching and  
1835 configuration management. The total number of vulnerabilities should be reduced over  
1836 time.

1837 • Number of unmitigated new vulnerabilities introduced into the environment trended by  
1838 week. The goal is to keep the number of new vulnerabilities as low as possible, defined  
1839 by your organization's level of risk tolerance.

1840 *References*

- 1841 • (CIS Control 4: Continuous Vulnerability Assessment and Remediation 2018)
- 1842 • (OWASP Top 10 - 2017: Ten Most Critical Web Application Security Risks 2017)
- 1843 • (NVD NIST 2018)
- 1844 • (Common Vulnerability Scoring System SIG n.d.)

1845  
1846  
  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864

## Cybersecurity Best Practice #8: Security Operations Center and Incident Response

Most cybersecurity programs begin by implementing controls designed to prevent cyber attacks against an organization’s IT infrastructure and data. This is a good place to start and there is a lot of value in basic cyber hygiene, leveraging the best practices that are discussed in this volume. However, in the modern age of cyber threats, not all attacks can be prevented with these basic controls. It is equally important to invest in and develop capabilities to detect successful attacks and respond quickly to mitigate the effects of these attacks.

Best Practice 8: Security Operations Center and Incident Response	
Data that may be affected	-
Baseline Practices	A. Security Operations Center B. Incident Response C. Information Sharing and ISACs/ISAOs
Advanced Practices	A. Advanced Security Operations Center B. Advanced Information Sharing C. Incident Response Orchestration D. Baseline Network Traffic E. User Behavior Analytics F. Deception Technologies
Key Mitigated Risks	<ul style="list-style-type: none"> <li>• Phishing Attacks</li> <li>• Ransomware Attacks</li> <li>• Loss or Theft of Equipment</li> <li>• Insider, Accidental or Intentional Data Loss</li> <li>• Attacks Against Connected Medical Devices</li> </ul>

A good example is the threat of phishing attacks. Even if organizations followed every best practice discussed in *Cybersecurity Practice #1: Email Protection*, they will still be susceptible to phishing attacks. It is incredibly important to detect in near real-time a phishing attack that successfully infiltrates your environment and to neutralize its effects before widespread theft of credentials or malware installation occurs. This is a classic example of shoring up your detection capabilities (detecting the phishing attack that gets past your basic controls) and response capabilities (neutralizing the effects before serious damage to the organization occurs).

Maintaining these capabilities requires the establishment of an IR program and a SOC to manage the IR along with security engineering that enhances an organization’s ability to detect and response to cyberattacks.

### *Baseline Practice*

#### **A. Security Operations Center (NIST Framework: DETECT)**

A SOC is an organizational structure that leverages cybersecurity frameworks, people, tools, and processes to provide dedicated cybersecurity operations for an organization. Generally speaking, SOCs are the areas within an organization that dedicate 100% of their time to cybersecurity prevention, detection or response capabilities, providing the execution arm of cybersecurity IR.

A SOC is generally segmented into four main functions, depending on the organization’s level of maturity. These functions are:

*Engineering* – Security Engineering is the process of building new cybersecurity capabilities into the existing toolsets in an environment. Examples include building new alerts within a Security Incident and Event Management (SIEM), establishing new log sources for log management systems, establishing new

1886 analytics patterns for detection, or simply implementing new cybersecurity systems to add capabilities  
 1887 into the environment.

1888 *Operations* – Security Operations is the process of managing and maintaining the cybersecurity tools  
 1889 within the SOC. This is sometimes referred to as “Keeping the Lights On.” This generally means  
 1890 monitoring critical cybersecurity systems to ensure they operate at agreed upon performance levels.

1891 *Threat Intelligence* – A specific type of function that focuses entirely on how to discover cybersecurity  
 1892 threats that may be relevant to the organization along with the means and methods these threats may  
 1893 use to infiltrate the organization. This function focuses on the threat actors themselves, the tools they  
 1894 leverage, and the digital signatures they leave in the process of conducting their activities. Once these  
 1895 digital footprints are established, sometimes called an Indicator of Compromise (IOC), engineering  
 1896 teams can implement these patterns into the systems and establish IR plays to execute when activated.

1897 *Incident Response* – IR is the process of conducting a structured and consistent response to any IR plays  
 1898 that have been created. The goal of this function is to:

- 1899 • Validate an IR play that has been triggered;
- 1900 • Contain any successful cybersecurity attacks to the organization;
- 1901 • Eliminate the threat from the environment;
- 1902 • Recover systems or data that might have been affected by the attack; and,
- 1903 • Ensure that any attack vectors that were exploited are well understood and fed back to  
 1904 the Security Engineering teams for future prevention or enhanced detection capabilities  
 1905 to further minimize the impacts of those vectors.

1906 It is critically important to instill a continuous feedback loop between your IR and Engineering teams so  
 1907 the organization continues to learn and grow based on the actual success of threats and threat actors.

1908 As SOCs are implemented, a core concept is to ensure that IR teams and handlers apply consistent  
 1909 methods to execute response practices. SOCs and IR teams should establish a Playbook, also known as a  
 1910 Runbook that describes existing detection mechanisms and the procedures to be followed if the  
 1911 detection mechanism is triggered. This may be referred to as a “Play,” similar to Plays that football  
 1912 teams maintain in their Playbooks.

1913 Examples of Plays that might be found in a Playbook are provided in Table 11.

Play Category	Play	Description	Source Data
Reconnaissance	Vulnerability scanning sweep of DMZ.	Large number of vulnerabilities being scanned across the DMZ spectrum. May be a single server being scanned over multiple ports or multiple servers being scanned on a single port.	<ul style="list-style-type: none"> <li>• Server list in DMZ.</li> <li>• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) logs configured to detect vulnerability scanning.</li> <li>• Firewall logs.</li> <li>• Netflow data.</li> </ul>



<b>Reconnaissance</b>	Vulnerability scan from known malicious IPs.	Vulnerability scans of the DMZ or other servers/endpoints exposed to the Internet over channels that are shared and known to be malicious (Indicator of Compromise).	<ul style="list-style-type: none"> <li>• IOC list from threat sharing sources (e.g., ISACs).</li> <li>• IDS/IPS Logs.</li> <li>• Firewall logs.</li> <li>• Netflow data.</li> </ul>
<b>Reconnaissance</b>	Successful access from known malicious Ips.	Successful authentications from known malicious IP addresses. Authentications through standard remote access channels, such as VPN, virtual terminals, jump boxes, or other mechanisms.	<ul style="list-style-type: none"> <li>• Authentication Logs.</li> <li>• Firewall Logs.</li> <li>• IOC list from threat sharing sources (e.g., ISACs).</li> </ul>
<b>Reconnaissance</b>	Internal attacks from third party VPNs.	Detection of attacks coming through partnering third party VPN connections, such as organizations that provide building automation services.	<ul style="list-style-type: none"> <li>• Firewall Logs (from segmented networks).</li> <li>• IDS/IPS Logs.</li> <li>• Authentication Log.</li> </ul>
<b>Persistence</b>	Creation of local user accounts on static systems.	Detection of a local user account being created on an asset, such as a Windows *nix server, where local user account creations normally do not occur. This may indicate malicious activity.	<ul style="list-style-type: none"> <li>• Logs from local servers.</li> </ul>
<b>Persistence</b>	After exploit persistence hold.	Detection of malicious users attempting to maintain permanent access. Look for launch or changing of scheduled tasks, script downloads, and new process creation.	<ul style="list-style-type: none"> <li>• Critical server lists.</li> <li>• Known process baselines.</li> <li>• Logs from server task or scheduled job management.</li> <li>• URL Filtering logs by server.</li> </ul>

<b>Privilege Escalation</b>	Privileged Account brute force success.	Large numbers of invalid login attempts followed by a successful login to a known privileged account.	<ul style="list-style-type: none"> <li>Privileged Account List.</li> <li>Authentication Logs (e.g. Active Directory, Servers).</li> </ul>
<b>Privilege Escalation</b>	Default Account password guessing.	Large number of invalid login attempts followed by a successful login to a known default user account.	<ul style="list-style-type: none"> <li>Default account list.</li> <li>Authentication Logs (e.g. Active Directory, Servers).</li> </ul>
<b>Privilege Escalation</b>	Interactive login to Service Accounts.	Detection of a service account being used as an interactive login (a user logging in to a terminal session). Service accounts should only be used for applications or services.	<ul style="list-style-type: none"> <li>Service account list.</li> <li>Authentication Logs (Active Directory, servers).</li> </ul>
<b>Data Exfiltration</b>	Data Transfer.	Detection of data transfers occurring outside of the organization from servers that normally do not conduct such activities. Must normalize/baseline server network behavior and detect anomalous activities off baseline.	<ul style="list-style-type: none"> <li>Netflow data, or Firewall traffic profile data.</li> <li>List of permitted remote storage sites (e.g. Box).</li> </ul>

1914

*Table 11. IR Plays Describe Responses to Cyberattacks*

1915

In each of these cases, the source data provided will include events or log information that is critical to detect the play being constructed. Specialized security systems can ingest these logs and apply pattern matching, rules matching, and analytics matching capabilities to specific events in the logs to call out potential incidents of interest. These specialized systems are referred to as SIEM systems.

1916

1917

1918

1919

This section provides details for the high level play, what it seeks to accomplish, and the types of source data that must be collected to successfully detect it. The list below will not discuss specific technical log event data that is required. Information on how to configure this information can be found in multiple publications, such as (Swift 2010) and (The 6 Categories of Critical Log Information 2013).

1920

1921

1922

1923

**B. Incident Response**

**(NIST Framework: RESPOND, RECOVER)**

1924

One of the most basic, and most important, functions in a cybersecurity organization is the IR process.

1925

This process provides the organization with standardized procedures to respond to cyberattacks. The

1926 attack may be as simple as an attempted phishing attack against users or a highly sophisticated  
 1927 extortion attack that shuts down digital operations. In both cases, from minimal to significant impact,  
 1928 the organized manner of an IR is critical to manage these threats.

1929 The following procedure is a summary of (SP 800-61r2: Computer Security Incident Handling Guide  
 1930 2012). Generally, a structured IR process is segmented into the following steps:

1931 *Preparation* – Before you respond to a cybersecurity incident, it’s important to have policies, processes,  
 1932 and procedures in place. This includes the following components:

- 1933 • *IR Policy* – a policy that defines the categorization and severity of incidents, the  
 1934 stakeholders involved in IR, the roles and responsibilities of each person, the entry  
 1935 criteria when a security incident occurs and the person who is in charge of IR plays.  
 1936 Stakeholders may range from the standard blocking and tackling personnel in IT  
 1937 Operations to legal, marketing and public affairs personnel for high impact incidents. A  
 1938 template IR policy is provided as **Appendix I in the main document**.
- 1939 • *Cybersecurity Incident Response Team (CIRT)* – The CIRT is a pre-formed and “on the  
 1940 ready” group that knows how to navigate issues when Critical or High severity security  
 1941 incidents arise. This team develops and manages your organizational response. Most  
 1942 commonly, CIRTs formed in the HPH Sector when potential data breaches occur and the  
 1943 organization must manage the potential breach in compliance with HITECH. It is  
 1944 important to identify the Incident Commander, the most senior official who will be in  
 1945 charge of managing cybersecurity incidents. The Incident Commander is usually the  
 1946 CISO or equivalent in an organization. It’s important to note that the Incident  
 1947 Commander should not dive into the technical weeds of the incident, but keep the  
 1948 various teams organized and focus on their objectives. For example, Table 12 describes  
 1949 that teams that may be involved in resolving a critical security incident and potential  
 1950 breach.

Team	Description
<b>Executive/Senior Leadership</b>	This is an organization’s C-Suite or most senior executives. They provide overall direction and approvals required to resolve significant cybersecurity breaches. These individuals should be kept informed throughout the life cycle of a significant cybersecurity incident.
<b>Cybersecurity Teams</b>	These teams are comprised of people with cybersecurity expertise who understand attacks, vulnerabilities and the methods by which threat vectors are exploited. They provide technical depth and detail to technical teams and execute procedures in the Playbook.
<b>Technical Teams</b>	These teams are comprised of subject matter experts (SME) for the technologies that have been compromised and are engaged in developing and implementing the response. These SMEs may be system owners, system administrators, or other individuals with specialized IT expertise. They take instruction from the cybersecurity teams as part of the Playbook execution.

<b>Legal Teams</b>	These teams are comprised of attorneys in your general counsel (internal or external) that help manage the incident under privilege as well as consult on regulatory expectations.
<b>Public Affairs/Marketing and Communications</b>	These people manage external communications to deliver a consistent voice and message in the event of a high visibility cybersecurity incident. It is critically important to manage the reputation of the organization.
<b>HIPAA Privacy Teams</b>	These teams are responsible for understanding the full extent of a cybersecurity incident that involves PHI. This includes conducting a breach analysis process in compliance with HITECH and providing consult for any patient-facing communications that should occur.

Table 12. Roles and Responsibilities to Respond to a Critical Cybersecurity Incident

1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978

- Playbook and/or Runbook** – An organization’s Playbook contains sets of standard operating procedures to respond to different types of cyberattacks. Procedures to respond to a phishing attack are different from those required to respond to a system intrusion or a ransomware attack. Each of these three types of attack is a distinct “Play” in an organization’s cybersecurity “Playbook.” For each Play, it’s important to describe the steps that will be followed to mitigate the attack so that your response is not “made up on the fly.” Though each particular attack has its own unique characteristics and nuances, your procedural processes should follow the steps provided in your Playbook for that type of attack. A template playbook is provided in **Appendix I in the main document.**
  - Tools and Technologies** – Once you establish your policies, CIRT and Playbook, the next level of improvement is to configure your tools and technologies to streamline the execution of your plays. This connects your IR processes back to your Security Engineering processes to create a continual feedback loop that is essential to becoming a resilient organization.
- Identification** – The first response to any cyberattack is to understand the scope and extent of the attack. The identification phase of an attack sets in motion the process of categorizing and classifying components of the attack based on your policies and procedures. Critical and sophisticated attacks warrant a well-organized and effective response.
- For example, a general phishing attack against a small user set that is easily identified as malicious may be assigned a lower level of concern than a targeted phishing attack against a select user base leveraging the nomenclature of your organization. These highly specialized attacks are known to be very successful and can easily compromise a user’s credentials or introduce remote access malware into your environment.
- An example of the identification exercise in a phishing process may be as simple as the following:
- Receive notification from your user base or through your own detection systems of a phishing attack or campaign.

- 1979                   • Profile and understand the extent and scope of the phishing attack. Determining its  
1980                   level of sophistication and intent.
- 1981                   • Conduct a basic investigation to determine if links were clicked or malware was  
1982                   delivered.
- 1983                   *Containment* – After the extent and scope of the attack is understood, the next step is to contain the  
1984                   attack before it penetrates further into your organization. This phase is critical and must not be  
1985                   overlooked – less mature organizations may start fixing the vulnerability that was exploited before they  
1986                   stop the attack. Your Playbook should include containment procedures for each of the plays that are  
1987                   addressed. In some cases, this may require shutting down information systems to prevent them from  
1988                   being compromised if they are vulnerable to the attack.
- 1989                   An example of a containment exercise in the phishing process may be as simple as the following:
- 1990                   • Shun any remote access C2 traffic that might be established as part of the attack.
- 1991                   • Change credentials proactively for users who clicked to open a credential theft phishing  
1992                   campaign.
- 1993                   *Eradication* – This phase of your response focuses your IR effort on eliminating all traces of the attack  
1994                   including the attack foothold. This includes:
- 1995                   • Identification of all emails that were delivered to your user base.
- 1996                   • Removal of these emails from mailboxes of the same user base.
- 1997                   • Reimaging of endpoints where malicious binaries or malware were downloaded to  
1998                   ensure no foothold exists.
- 1999                   *Recovery* – After the threat is neutralized and all malicious activity is removed from the organization’s  
2000                   systems, you must determine whether or not to reactivate the compromised technology. In most cases,  
2001                   the answer to this question will be “of course,” since these technologies fulfill a larger purpose in your  
2002                   organization. In cases where legacy technologies were compromised, however, it might not be worth  
2003                   the effort and investment to bring them back online.
- 2004                   In either case, the process to restore the technical capability in the organization is equally important as  
2005                   the process to remove the threats and malicious activities in your systems. As you restore functionality,  
2006                   shut down the vectors that made the attack successful. This may be done by patching an exploited  
2007                   vulnerability or rebuilding an entire system to leverage hardening processes such as those identified in  
2008                   *Cybersecurity Best Practice #2: Endpoint Protection Systems*.
- 2009                   *Lessons Learned/After Action Report* – Arguably the most important stage of your IR process is a full  
2010                   debrief with your IR teams after the attack is mitigated and systems are returned to full functionality.  
2011                   This debrief should profile the successful attack vectors and identify short term adjustments to  
2012                   introduce enhanced prevention, detection or response capabilities as well as long term strategic  
2013                   elements that require more detailed planning.
- 2014                   For example, if your organization falls prey to a sophisticated phishing attack that results in the theft of  
2015                   multiple credentials followed by the installation of remote access tools and elimination of an advanced  
2016                   persistent threat in your systems, a multifaceted set of mechanisms may be considered for short term  
2017                   and long term improvement. Examples may include:

- 2018 • Refine a particular play within the Playbook that didn't execute as efficiently as possible.
- 2019 Timeliness is one of the most critical aspects of any response – taking too long to ramp
- 2020 up your IR Playbook increases your exposure to a successful attack.
- 2021 • Refine and expand logging capabilities to detect threats more quickly. Implementing
- 2022 these capabilities into your SIEMs. Delve into the specific patterns of the attack as much
- 2023 as possible for lessons learned.
- 2024 • Share attack details and information with participating ISACs and ISAOs. This helps
- 2025 other organizations to prevent validated and vetted threats. It provides greater
- 2026 credence to the intelligence and increases resiliency of the sector as a whole.
- 2027 • Leverage advanced analytics-based phishing protection tools such as “click protection”
- 2028 or “attachment sandboxing.” This usually requires investment and budget allocation by
- 2029 the organization.
- 2030 • Refocus and prioritize resources to build out greater capabilities to identify and respond
- 2031 to phishing attacks. From a strategic perspective, it's important to refocus your
- 2032 resources in response to a threat that is ramping up against your organization.

2033 A feedback loop from your IR processes back into engineering and operations is paramount to become a  
 2034 resilient organization. This type of feedback loop enhances an organization's cybersecurity capabilities  
 2035 overtime and organically while increasing flexibility and agility in IR response processes.

2036 To read an example case of a “mock attack,” consider “A Practical Example of Incident Response to a  
 2037 Network Based Attack” from the SANS Reading Room (Fraser 2017)

2038 Further details associated with an IR Playbook can be found in the SANS Reading Room, “Incident  
 2039 Handler's Handbook” (Kral 2011).

**C. Information Sharing and ISACs/ISAOs (NIST Framework: DETECT)**

2041 Security engineering and operations activities tend to be centered towards preventing cyberattacks and  
 2042 building out systems that enable streamlined execution of IR functions. That said, not all attacks are  
 2043 equal. They range from simple “script kiddies” that attempt to gain entry to any target to advanced  
 2044 persistent threats backed by substantial resources and a strong desire to gain entry to your organization.  
 2045 The means to differentiate these types of attacks falls under the discipline of Threat Intelligence.

2046 The next level of sophistication is realized through involvement with and participation in Information  
 2047 Sharing and Analysis Centers (ISAC) and Information Sharing and Analysis Organizations (ISAO). There  
 2048 are many ISACs and ISAOs and they tend to focus on a specific vertical (such as NH-ISAC within  
 2049 Healthcare) or community (such as the Population Health ISAO). In all cases, these are associations  
 2050 whose sole function is to bring together like communities for the purposes of sharing cyber intelligence  
 2051 to protect their constituents. The means to share this intelligence vary in sophistication, although most  
 2052 mature ISACs leverage common standards and formats, such as Structure Threat Information eXpression  
 2053 (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), as well as flash reports that  
 2054 profile current attacks. Participation in an ISAC or ISAO offers incredible value to an organization. It  
 2055 connects your cybersecurity professionals with the greater cybersecurity community. At a minimum,  
 2056 your organization should be a member of an ISAC or ISAO.

2057 As with all disciplines, there are multiple levels of maturity within the Threat Intelligence discipline. The  
 2058 most basic sharing of threat intelligence involves consuming lists of “vetted bad IP addresses” or “feeds”  
 2059 from commodity sources. These sources have been well curated to identify where the loudest and most

2060 obvious attack space resides. Organizations can use multiple means to consume these feeds, but it  
2061 usually originates by subscribing to a daily download of IOCs.

2062 **Advanced Practice**

2063 **A. Advanced Security Operations Centers (NIST Framework: DETECT)**

2064 In addition to the practices discussed for SOCs, an organization’s move to more advanced realms of  
2065 security management should include expanding its SOC to a 24x7x365 model. In this model, the SOC is  
2066 staffed and monitored 24 hours a day, 7 days a week, 365 days a year.

2067 There are multiple methods to achieve this model, all of which include benefits and constraints. Some  
2068 of these methods are described below:

2069 *Fully Outsourced* – In the fully outsourced model, all SOC and threat actions are sourced to a third party  
2070 provide who has the required infrastructure, staff, and capabilities. These models generally tend to  
2071 leverage sensors provided by the third party that are installed on your networks and used to collect  
2072 necessary log information that enriches detection and response activities. In these models, SOC analysts  
2073 actively look for threats and provide your internal IR personnel with specific actions to take once the  
2074 threats is identified.

2075 This model has the advantage of scale and capability. It is difficult to hire and retain qualified security  
2076 analysts to provide this dedicated function. Additionally, organizations benefit from the shared  
2077 intelligence discovered by other clients of the service provider. The main disadvantage is that these  
2078 analysts tend not to fully complete response actions, requiring engagement from your internal teams.  
2079 Additionally, investments made by your organization in cybersecurity tools might not be fully leveraged  
2080 as the service providers are likely to use their own tools.

2081 *Fully Insourced* – In the fully insourced model, all SOC and threat actions are handled with internal staff  
2082 and infrastructure. This model requires the build out of a dedicated physical space with the IT  
2083 infrastructure and tools necessary to support your IR personnel. It requires a combination of skills from  
2084 security engineers, incident handlers, and threat hunters.

2085 This model has the advantage of situational awareness and an in-depth understanding of the  
2086 organization’s business requirements and nuances. Internal staff are accustomed to the specific needs  
2087 of the organization. Additionally, internal staff understand the context of an organization’s various  
2088 systems far more intrinsically than an outside service provider. The main disadvantages of this model  
2089 relate to cost, workforce retention, and threat intelligence. Building out an internal SOC can be a costly  
2090 proposition if the organization doesn’t have existing facilities to support it. Moving to a 24x7 operation  
2091 requires hiring new employees and supervisors to ensure effective management and coverage during  
2092 holidays and time off. Lastly, in this model, the organization does not necessarily get current  
2093 information about threat actions occurring in other organizations.

2094 *Hybrid* – In the hybrid model, the SOC and incident handling functionalities attempt to leverage  
2095 strengths of the Fully Outsourced and the Fully Insourced models while minimizing the disadvantages.  
2096 In this model, organizations contract with a service provider to provides 24x7x365 monitoring and  
2097 response by remotely accessing the organization’s existing security technologies (e.g., SIEMs, IPS,  
2098 firewalls). The service provider provides facilities and staff for monitoring and response actions and the  
2099 organization provides the tools and escalation processes.

2100 This model tends to offer flexibility and scaling of existing investments made in cybersecurity  
2101 technologies, processes, and people. However, it requires a specific and scripted procedural playbooks

2102 to be effective. The organization is required to drive these procedural playbooks and ensure the service  
2103 provider complies with them. Lastly, in this model, organizations lose some of the situational awareness  
2104 normally provided by internal handlers. Generally speaking, precise roles and responsibilities must be  
2105 established to achieve the desired outcome.

2106 **B. Advanced Information Sharing (NIST Framework: DETECT)**

2107 Leveraging threat intelligence can be challenging. The organization must establish a threat model,  
2108 ingest data according to the model, and automate the collection and response. Generally speaking, this  
2109 requires dedicated human and technology resources to be successful.

2110 MITRE has developed a model to manage these threats. “Adversarial Tactics, Techniques, and Common  
2111 Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior. It  
2112 addresses the phases of an adversary’s lifecycle and the platforms that are targeted. ATT&CK is useful  
2113 for understanding security risks from known adversary behavior, planning security improvements, and  
2114 verifying defenses work as expected (Adversarial Tactics, Techniques & Common Knowledge n.d.). It is  
2115 recommended that organizations consider this model in addition to STIX and TAXII automation methods  
2116 to build out a robust threat intelligence program.

2117 Beyond ISACs and ISAOs, there are individual intelligence gathering organizations or departments within  
2118 organizations that have a vested interest in getting “deep intelligence” directly from the attacker  
2119 community. This capability requires substantial investments and specialized talent (think intelligence  
2120 officers). Generally speaking, this level of maturity is not achievable in most large organizations.  
2121 However, with proper vetting, the fruits of their labor can assist the HPH Sector immensely.

2122 **C. Incident Response Orchestration (NIST Framework: RESPOND)**

2123 It can be incredibly difficult to manage a response and leverage intelligence from the many specialized  
2124 tools that may exist to provide cybersecurity in an organization. Examples of these tools include SIEMs,  
2125 User Behavior analytics, deception technologies, email protection platforms, and Endpoint Detection  
2126 and Response technologies. Though tools like SIEMs are designed to ingest information from multiple  
2127 sources and provide context, this capability is dependent on the extensibility of log data generated by  
2128 these systems as well as the workflow and process capabilities of the SIEM technology. Generally  
2129 speaking, SIEMs are fantastic at developing alerts and notifying security resources of emergent issues,  
2130 but, generally not as robust in the process of executing IR playbooks.

2131 This is where IR Orchestration tools come in handy. Once playbooks have been scripted and vetted,  
2132 these tools ensure that playbook execution is consistent throughout the process. Without these types  
2133 of tools, IR consistency must be managed by cybersecurity personnel. These tools enable cybersecurity  
2134 personnel to focus on the incident rather than the consistent execution and documentation of an  
2135 incident.

2136 In addition to the workflow components of IR Orchestration, these tools can pull data from system  
2137 security stacks and present it to the incident responder in a centralized dashboard. Examples of data  
2138 that may be pulled into this dashboard include: SIEM, Log Data, Dynamic Host Configuration Protocol  
2139 (DHCP) logs, asset inventories, anti-malware consoles, vulnerability management data, threat  
2140 intelligence information, identity management systems, and endpoint security technologies. Each of  
2141 these systems provides a perspective on the particular type of threat that your organization is  
2142 experiencing.



2143 **D. Baseline Network Traffic** **(NIST Framework: DETECT)**

2144 A useful technique to deploy is to baseline your network traffic and implement capabilities to alert upon  
2145 anomalous changes to the baseline. This can be accomplished by leveraging netflow data and systems  
2146 that can ingest netflow data. Each system that operates in the ecosystem will have a standard 'digital  
2147 footprint' for its network communications, and generally will operate within those parameters. By  
2148 conducting a baseline operation on each of the major and core systems you can compare what is  
2149 'expected' to what is actually occurring. This process can be done manually or you can invest in  
2150 technologies that can automate this process for you.

2151 **E. User Behavior Analytics** **(NIST Framework: DETECT)**

2152 User Behavior Analytics (UBA) is a technique that may be considered as the "SIEM for Users." In most  
2153 modern threats, the threat actors attempt to leverage access that already exists in the user space.  
2154 Although attackers can generate new accounts for access attempts, they are well aware that most  
2155 organizations monitor systems for new accounts, especially those with privileged access. The  
2156 exploitation of existing accounts, however, might go unnoticed.

2157 UBA systems provide analytics context from a user perspective. Similar to conducting a baseline activity  
2158 over network access, UBAs baseline user activity and actions throughout the organization's digital  
2159 ecosystem. The tool ingests the most relevant user activity logs from these systems as well as existing  
2160 authentication and authorization systems. Deviations are discovered after the user has been profiled,  
2161 enabling IR actions to be executed according to the proper playbooks.

2162 One note of importance: UBA protects against external as well as internal threat actors.

2163 **F. Deception Technologies** **(NIST Framework: DETECT)**

2164 Deception technologies expand on the honeypot and honeynet techniques of old, delivering it at scale  
2165 to the enterprise. These techniques place "fake systems" or "fake breadcrumbs" throughout the digital  
2166 ecosystem and wait for them to be "tripped." They work on the principle that communications should  
2167 not occur in a system that serves no purpose in the organization. If such a communication occurs, it  
2168 should be brought to the attention of the IR teams for further investigation.

2169 Deception technologies discover attackers who have placed a foothold on your organization's network  
2170 and are attempting to pivot to find targets of interest. These targets may be simple (e.g., file storage  
2171 systems, email systems) or they may be complicated (e.g., EMR or Imaging systems). In all cases, the  
2172 goal of the attacker is to leverage access already obtained to pilfer data or conduct an extortion attack  
2173 (i.e., ransomware). The attacker's approach is to generate hundreds or thousands of these "fake  
2174 systems" so that it is difficult to differentiate them from real assets.

2175 Your IR teams can profile the threat actor by watching their behavior on these fake systems. For  
2176 example, technologies exist to create a complete fake file system that interacts and responds like a real  
2177 file storage system, even generating files that appear legitimate. By watching the threat actor  
2178 enumerate the file system, your IR teams can develop a high level of certainty of the malicious intent  
2179 and identify the foothold held by the threat actor on the organization's network.

2180 **Threats Mitigated**

- 2181 1. Phishing Attacks
- 2182 2. Ransomware Attacks
- 2183 3. Loss or Theft of Equipment

2184 4. Internal, Accidental or Intentional Data Loss

2185 5. Attacks against Connected Medical Devices that May Affect Patient Safety

2186 *Suggested Metrics*

- 2187 • Time to detect and respond in aggregate, trended by week. The goal is that an IR  
2188 response should kick off within X hours after detection of an incident and the incident  
2189 should be mitigated within X hours after response. Lag time between occurrence and  
2190 detection of a security incident should be fewer than X days.
- 2191 • Number of true positive incidents executed by incident category on a weekly basis.  
2192 Though there is no goal set for this metric, it's important to monitor trends in incidents  
2193 that occur in your organization. This will inform the larger security strategy over time  
2194 based on actual threats in your organization.
- 2195 • Number of backup failures by week. The goal is to minimize the number of backup jobs  
2196 that fail and to provide continual assurance that backup jobs are executing as intended.
- 2197 • Number of notable (or critical/high rated) security incidents per week, providing a  
2198 profiled enumeration of each incident. Each notable security incident should be  
2199 executed consistently and thoroughly. Each incident should have an After Action  
2200 Report. The goal is to demonstrate that After Action Reports and incident reports are  
2201 written for each notable security incident. This will help with the development and  
2202 implementation of continual improvement processes.

2203 *References*

- 2204 • (Fraser 2017)
- 2205 • (Kral 2011)
- 2206 • (Swift 2010)
- 2207 • (The 6 Categories of Critical Log Information 2013)
- 2208 • (SP 800-61r2: Computer Security Incident Handling Guide 2012)
- 2209 • (Adversarial Tactics, Techniques & Common Knowledge n.d.)
- 2210

2211

## Cybersecurity Best Practice #9: Medical Device Security

2212 Healthcare systems leverage  
 2213 many diagnostic and  
 2214 therapeutic methods for  
 2215 patient treatments. These  
 2216 may be technological  
 2217 systems that render and  
 2218 provide detailed images of CT  
 2219 scans, or they may be devices  
 2220 that connect directly to the  
 2221 patient for a diagnostic or  
 2222 therapeutic purpose. These  
 2223 types of devices may have  
 2224 straightforward  
 2225 implementations, such as  
 2226 bedside monitors that

Best Practice 9: Medical Device Security	
Data that may be affected	ePHI
Baseline Practices	A. Medical Device Management B. Endpoint Protections C. Identity and Access Management D. Asset Management E. Network Management
Advanced Practices	A. Vulnerability Management B. Security Operations and Incident Response C. Procurement and Security Evaluations D. Contacting the FDA
Key Mitigated Risks	<ul style="list-style-type: none"> <li>Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

2227 monitor the vital signs of a patient during an inpatient stay, or it may have a complicated  
 2228 implementation such as an infusion pump that delivers specialized therapies, such as chemotherapy to a  
 2229 cancer patient, and requires continual updates to its drug libraries. These complex and interconnected  
 2230 devices impact patient safety and well-being, and should be robustly designed and properly secured.

2231 This section focuses entirely upon the methods that Health Delivery Organizations (HDO) can employ to  
 2232 protect connected medical devices. Specifically, it will focus on the actions that HDOs are permitted to  
 2233 take and how to best work with device manufacturers and the U.S. Food and Drug Administration (FDA).

2234 Any device that connects directly to the patient for the purpose of diagnostic or therapies must undergo  
 2235 extensive quality control processes to ensure they are safe for use. Rigorous stipulations are in place for  
 2236 the development and release of such systems. These stipulations are managed by the FDA. The  
 2237 organizations that produce these devices must comply with these regulations, and generally are referred  
 2238 to as device manufacturers. Organizations that purchase these devices and use them for the treatment  
 2239 of patients are the clinical providers. In the context of this relationship, they are referred to as HDOs.

2240 Given the highly regulated nature of these devices and the specialized skills required to make  
 2241 modifications, it is ill-advised for HDOs to make configuration changes without the support of the device  
 2242 manufacturer. Doing so may put the HDO at risk for voiding warranties, result in legal liabilities, and, at  
 2243 worst, harm the patient. Traditional methods used by security programs to secure these assets cannot  
 2244 necessarily be deployed. For example, one cannot simply apply a patch to a vulnerable component of  
 2245 the OS that runs a medical device.

2246 For a practical example of full life cycle management, risk analysis, management, best practices, and  
 2247 detailed configuration specifications to secure wireless pumps (one type of medical devices), consider  
 2248 the information released by NIST and the National Cybersecurity Center of Excellence (NCCOE), *NIST SP*  
 2249 *1800-8: Securing Wireless Infusion Pumps In Healthcare Delivery Organizations 2017*.

2250 **Baseline Practice**

2251 **A. Medical Device Management (NIST Framework: IDENTIFY)**

2252 Medical devices are a specialized type of “Internet of Things” (IOT), leveraged for clinical diagnostic or  
2253 treatment purposes within HDOs.

2254 That said, cybersecurity for medical devices follows many of the best practices already discussed in this  
2255 document, including:

- 2256 • Cybersecurity Best Practice #2: Endpoint Protections
- 2257 • Cybersecurity Best Practice #3: Identity and Access Management
- 2258 • Cybersecurity Best Practice #5: Asset Management
- 2259 • Cybersecurity Best Practice #6: Network Management
- 2260 • Cybersecurity Best Practice #7: Vulnerability Management
- 2261 • Cybersecurity Best Practice #8: Security Operations and Incident Response

2262 Rather than recreating these best practices, HDOs are encouraged to extend the relevant best practice  
2263 from each section, implementing it appropriately for medical device management.

2264 **B. Endpoint Protections (NIST Framework: PROTECT)**

2265 As much as feasible, medical devices should have following controls enabled:

2266 *Antivirus software* – Usually the medical device manufacturer must directly support this software or it  
2267 must be cleared for operation by the manufacturer. Ensure that a compliant AV technology is enabled.  
2268 If AV cannot be implemented, compensating controls should enforce an AV scan whenever the device is  
2269 serviced prior to reconnecting to the device network.

2270 *Local firewalls enabled* – Medical devices should be configured to communicate only with required  
2271 systems. Unused services and ports should be disabled as long as they are supported by the  
2272 manufacturer.

2273 *Encryption* – If supported by the manufacturer, medical devices should have local encryption enabled in  
2274 the case the device is stolen.

2275 *Default Password Changes* – If supported by the manufacturer, default passwords, especially those  
2276 enabling privileged access, should be changed to a credential used only for the medical device. Do not  
2277 tie this unique credential to any general systems management credential as you do not want any  
2278 compromise of those credentials to impact the medical device.

2279 *Routine Patching* – As part of preventative maintenance cycles, medical devices should be patched with  
2280 supported cybersecurity patches that are released by the device manufacturers. Given the special  
2281 sensitivity to the configuration and management of these devices, it is emphasized that patching must  
2282 not take place on these devices unless cleared by the manufacturer.

2283 **C. Identity and Access Management (NIST Framework: PROTECT)**

2284 As much as feasible, medical devices should have following controls enabled on them:

2285 *Authentication* – If supported by the manufacturer, the device should bind its authentication capabilities  
2286 with systems enterprise authentication domains. This automates termination of access to the device  
2287 upon termination of employment for the user.

2288 *Vendor Support Passwords* – Passwords should not be shared among the vendor team. A unique logon  
2289 credential should be established for each vendor employee. Ensure the manufacturer does not use the  
2290 same account and password to manage medical devices in your organization and others.

2291 *Remote Access* – If remote access is required to manage medical devices, MFA capabilities should be  
2292 deployed. Depending on the deployment scenario, the device manufacturer may be required to support  
2293 these capabilities. Otherwise, these capabilities should be deployed on a separate component of your  
2294 existing MFA system to limit exposure in the event that the MFA system is compromised.

2295 **D. Asset Management** **(NIST Framework: IDENTIFY)**

2296 As much as feasible, medical devices should have following controls enabled on them:

2297 *Inventory* – All medical devices should be added to an inventory that is capable of understanding the  
2298 core components of the medical device itself. This may be your general IT Asset Management inventory  
2299 as described in *Cybersecurity Best Practice #5: IT Asset Management*. You may have to leverage  
2300 specialized tools designed specifically for tracking the lifecycle of medical devices. Such systems can be  
2301 useful for maintaining preventative maintenance schedules.

2302 *Wiping* – When a medical device is slated for decommissioning, it is critical to ensure that all data  
2303 resident on the device is wiped. These devices typically are returned to the vendor and potentially  
2304 resold or delivered to other organization for destruction. You do not want your organization’s data to  
2305 be accessed by these other parties.

2306 **E. Network Management** **(NIST Framework: PROTECT)**

2307 As much as feasible, medical devices should have following controls enabled on them:

2308 *Segmentation* – Given the critical nature of these devices and the general inability to configure them to  
2309 reduce vulnerabilities, it is critically important to segment these devices separately from general access  
2310 or data center networks. The ability to restrict access to the device is essential to its safe operation.

2311 Dedicated networks should be set up that are highly restricted. The only traffic allowed on these  
2312 networks should be profiled based on required operation of the devices connected to that network.  
2313 Access to the device management systems should be heavily restricted to limit exposure of the  
2314 management system to being compromised. Lastly, it’s important to ensure that these networks are  
2315 segmented such that any vulnerability scanning systems are not permitted access in a clinical setting.  
2316 Given the delicate nature of medical devices, execution of a rogue vulnerability scan could disrupt the  
2317 devices.

2318 As part of the segmentation strategy, review data flows and interfaces between the medical devices and  
2319 their connected systems. Be sure not to limit the essential functionality of the medical device including  
2320 the ability for it to be patched remotely if that is required.

2321 Device manufacturers may require installation of their own physical networks in the organization. In  
2322 these cases, access to the manufacturer’s physical network should be limited with the same restrictions  
2323 as if the HDO were implementing its own segmentation strategy.

2324 **Advanced Practice**

2325 **A. Vulnerability Management (NIST Framework: DETECT)**

2326 As much as feasible, medical devices should have following controls enabled on them:

2327 *Vulnerability and Risk Categorization* – In 2016, the FDA issued the Postmarket Management of  
 2328 Cybersecurity in Medical Devices guidance. (Postmarket Management of Cybersecurity in Medical  
 2329 Devices 2016) This guidance document presents components for the proper management of medical  
 2330 devices once they have been deployed in an HDO. Focusing on the risk to patient safety, this guidance  
 2331 stipulates that manufacturers should implement vulnerability and risk management practices to  
 2332 categorize risks according to the device effectiveness and the potential to cause harm to the patient.

2333 HDOs should work with device manufacturers to enable a common understanding of the framework for  
 2334 the risk categorizations. Upon disclosure of a high risk, HDOs should take an escalated action to secure  
 2335 the device.

2336 *Vulnerability Disclosure Programs* – Each device manufacturer should have a program that informs HDOs  
 2337 of vulnerabilities that exist in their devices. These programs should have a communication channel to  
 2338 report information and inform parties. HDOs should work with the manufacturers so all parties  
 2339 understand the respective points of contacts in the manufacturer and the HDO.

2340 In addition to these communication channels, other channels exist for the disclosure of medical device  
 2341 vulnerabilities. These include the Industrial Control Systems – Computer Emergency Response Team  
 2342 (ICS-CERT), which the manufacturers can included as part of their vulnerability releases, or the  
 2343 respective ISACs or ISAOs with which the manufacturers participate.

2344 The HDO must have a program in place to accept inbound vulnerability disclosures, evaluate the HDO’s  
 2345 exposure to these vulnerabilities, and stand up response actions with the manufacturers to remediate or  
 2346 mitigate each vulnerability according to its level of risk.

2347 Table 13 provides a general rule of thumb for the response (including interim compensating controls)  
 2348 timeframes of medical device vulnerabilities that is in line with expectations in the Postmarket  
 2349 Management of Cybersecurity for Medical Devices guidance.

Vulnerability Criticality	Days
<b>Uncontrolled Risk</b>	
Communicate to Customer	< 30 days
Remediate Risk	< 60 days
<b>Controlled Risk</b>	As defined by routine patching and preventative maintenance

2350 *Table 13. Response Timeframes to Resolve Medical Device Vulnerabilities*

2351 *Software Bill of Materials (SBOM) and Vulnerability Lookups* – By leveraging the SBOM registered in the  
 2352 organization’s ITAM, the HDO can compare data from the National Vulnerability Database (NVD) against  
 2353 data in the organization’s software libraries. This comparison provides the HDO with information on  
 2354 current potential vulnerability postures in the medical device space.

2355 A simple search of the NVD can be conducted by using the web interface located at  
2356 <https://nvd.nist.gov/vuln/search>. This search allows HDOs to look up vulnerabilities based upon  
2357 products that they currently have. It does not require SBOM material to be pre-registered.

2358 *Vulnerability Scanning*

2359 **WARNING: THIS ACTION MUST BE TAKEN WITH EXTREME CAUTION DUE TO THE POTENTIAL IMPACTS**  
2360 **ON MEDICAL DEVICES WITHIN THE PRODUCTION ENVIRONMENT. HDOS SHOULD NOT ATTEMPT TO**  
2361 **CONDUCT THIS ACTION UNLESS THEY ARE ABSOLUTELY CERTAIN THE MEDICAL DEVICE IS NOT IN**  
2362 **PRODUCTION, IS NOT CURRENTLY IMPLEMENTED IN A CLINICAL SETTING, AND IS NOT CONNECTED TO**  
2363 **PATIENT.**

2364 The final action that an HDO can take to understand its vulnerability posture is to conduct vulnerability  
2365 scans against the medical devices. There are two opportune times to conduct vulnerability scans against  
2366 medical devices:

- 2367 • When the device is first procured and tested before deployment in the production  
2368 environment; and,
- 2369 • When a device is taken offline for preventative maintenance and routine patching.

2370 In both scenarios, it is important for the device to be in a highly controlled setting while not connected  
2371 to a patient. A vulnerability scan can be configured to profile the device and determine if potential  
2372 vulnerabilities exist, or confirm that vulnerabilities have been mitigated as part of a remediation or  
2373 patching plan.

2374 To conduct such an exercise, it is best for the cybersecurity team to work with the clinical engineering  
2375 teams and establish a profiled scan template in the vulnerability management software. This template  
2376 should allow the scan to be executed only against a specific non-production network and only by specific  
2377 individuals. To provide further assurance that the vulnerability scan cannot cause harm to the medical  
2378 devices, IP addresses of the scanners should be blocked as part of the segmentation strategy noted  
2379 above.

2380 When these preparations are complete, the clinical engineering teams can be granted access to the  
2381 scanning software in a restricted manner that allows the scan to be run only against the network used  
2382 for preventative maintenance. Vulnerabilities discovered can be shared with the information security  
2383 office to determine the relative risks. Upon classification of these risks, the teams should contact the  
2384 device manufacturer and work together to develop and implement a remediation plan.

2385 ***B. Security Operations and Incident Response***  
2386 ***(NIST Framework: PROTECT, RESPOND, RECOVER)***

2387 Expanding on the SOC and IR processes found in *Cybersecurity Best Practice #8: Security Operation*  
2388 *Center and Incident Response*, HDOs can provide better monitoring, detection and response activities  
2389 around their medical device ecosystem. To provide visibility into the daily operations of the medical  
2390 device systems, the following sources should be configured to send logs to the HDO's log management  
2391 systems, SIEM, or both:

- 2392 • Firewalls providing segmentation to the medical device network segment;
- 2393 • Information systems that control the operation of the medical devices;
- 2394 • Netflow data from the medical device network segment;

- 2395 • Intrusion prevention systems in front of the medical device network segment; and,
  - 2396 • Logs from any deception technology deployed in the medical device network segment.
- 2397 With the source of these logs, plays can be enumerated and added into the standard Incident Response  
 2398 playbooks, as described in Table 14.

Play Category	Play	Description	Source Data
<b>Reconnaissance</b>	Vulnerability scanning sweep of Medical Device Segment.	Large number of vulnerabilities being scanned across the medical device network. May be caused by a single server being scanned over multiple ports, or multiple servers being scanned over a single port.	<ul style="list-style-type: none"> <li>• Medical device management system.</li> <li>• IDS/IPS logs in front of the medical device network, configured to detect vulnerability scanning.</li> <li>• Firewall logs in front of the medical device network.</li> <li>• Netflow data from within the medical device network.</li> </ul>
<b>Lateral Movement</b>	Detection of unknown source clients accessing medical device remote access ports.	Detect attacks coming from sources outside of known management sources attempting to gain access to remote access ports (e.g., ftp, ssh).	<ul style="list-style-type: none"> <li>• Firewall logs in front of the medical device network.</li> <li>• Network data from within medical device network.</li> </ul>
<b>Lateral Movement</b>	Triggered decoy within medical device network.	Respond to triggers of decoys being communicated from within or across the medical device network segment. These communications should not occur and indicate malicious or broken processes.	<ul style="list-style-type: none"> <li>• Deception technology logs from within the medical device network.</li> <li>• Firewall logs in front of the medical device network.</li> <li>• Network data from within the medical device network.</li> </ul>

2399 *Table 14. IR Plays to Combat Cyberattacks Against Medical Devices*

2400 **C. Procurement and Security Evaluations (NIST Framework: IDENTIFY)**

2401 First and foremost, HDOs must establish a set of cybersecurity requirements during the acquisition of  
 2402 new medical devices. These requirements should be embedded in your contracting processes and



2403 shared with your supply chain and procurement offices. Ideally, these cybersecurity requirements are  
2404 included in a Request for Information (RFI) or Request for Proposal (RFP) process.

2405 Secondly, technology acquisitions including medical devices require a security evaluation as part of the  
2406 supply chain process. Though important for the acquisition of medical devices, this is true for any  
2407 integration of technology into the HDO. Allowing cybersecurity evaluation processes to occur as part of  
2408 the supply chain process provides an opportunity for cyber risks to be understood, evaluated, and  
2409 mitigated prior to deployment.

2410 The first process that should be kicked off as part of the medical device acquisition process is a security  
2411 evaluation of the devices. This evaluation should uncover any risks or flaws in the current design of the  
2412 medical device and allow transparent communications between the supply chain process, clinical  
2413 engineering and the manufacturers. To shepherd the process along, the HDO should insist on receiving  
2414 a Manufacturer Disclosure Statement for Medical Device Security (MDS2). The MDS2 is a standardized  
2415 form leveraged by most manufacturers and developed by HIMSS and the American College of Clinical  
2416 Engineering (ACCE). It provides a list of comprehensive cybersecurity questions for medical devices with  
2417 responses from the manufacturer of the device in question. Questions in the MDS2 include:

- 2418 • “Can this device display, transmit, or maintain private data (including electronic  
2419 Protected Health Information)?”
- 2420 • “Can the medical device create an audit trail?”
- 2421 • “Can users be assigned different privileged levels within an application based on ‘roles’  
2422 (e.g. guests, regular users, power users, administrators)”; and,
- 2423 • “Can the device owner/operator reconfigure product security capabilities?”

2424 A copy of the latest MDS2 can be found on the Association of Electrical Equipment and Medical Imaging  
2425 Manufacturers (NEMA) website (The Association of Electrical Equipment and Medical Imaging  
2426 Manufacturers 2013). Answers to these questions assist the HDO to complete a meaningful evaluation  
2427 of the medical device.

2428 After the security evaluation is complete, the cybersecurity program should review and provide input  
2429 and review into the contract with the manufacturer. This stage should occur in tandem with the supply  
2430 chain and legal negotiations and leverage a template of security terms of interest from the HDO. These  
2431 terms should reference the FDA Postmarket Management of Cybersecurity for Medical Devices guidance  
2432 document, referencing components of the guidance that are critical for the safe operation of the  
2433 devices.

2434 Armed with the results of the cybersecurity evaluation, scenarios to resolve any unmitigated risks should  
2435 be included in the contracting process to limit the HDO’s liability, especially with constraints around the  
2436 HDO’s ability to alter the medical devices.

2437 *Software Bill of Materials* – The HDO should request a SBOM as part of the procurement process. The  
2438 SBOM is a list of software components that comprise the medical device. Think of it as the software  
2439 library, or the ingredients of the recipe, that make up the device. Understanding the software libraries  
2440 that make up the device facilitates the HDO’s ability to understand the impact of vulnerabilities  
2441 announced by the NVD.

2442 **D. Contacting the FDA** **(NIST Framework: DETECT)**

2443 If HDO is stuck managing high risk cybersecurity vulnerability and cannot get support from the medical  
2444 device manufacturer to mitigate this risk, the HDO’s final recourse is to contact the FDA directly to  
2445 express concern about the vulnerability. Contacts to the FDA should be limited to critical or high risk  
2446 scenarios, especially those with the potential to cause harm to patients.

2447 The CDRH emergency contact information is provided below:

- 2448 • Email: [AskCyberMed@fda.hhs.gov](mailto:AskCyberMed@fda.hhs.gov)
- 2449 • Phone: 301-796-7436

2450 **Threats Mitigated**

- 2451 1. Attacks Against Connected Medical Devices and Patient Safety

2452 **Suggested Metrics**

- 2453 • Number of medical devices not currently segmented on wireless or wired networks,  
2454 trended over time. The goal is to limit medical devices on the general access network,  
2455 data center network, or other location that does not meet the requirements of specific  
2456 network segmentation strategies.
- 2457 • Number of unmitigated, high risk vulnerabilities on connected medical devices, trended  
2458 over time. The goal is to reduce the number of unmitigated risks as close to zero as  
2459 possible. Each high risk vulnerability should have a remediation action plan, as defined  
2460 in *Cybersecurity Best Practice #7: Vulnerability Management*.
- 2461 • Number of medical devices procured that did not receive security evaluation, trended  
2462 over time. The goal is to reduce the number of procurement actions without security  
2463 evaluation to as near as zero as possible. Leverage this metric to work with your supply  
2464 chain and clinical engineering departments to ensure the process is executing as  
2465 intended.
- 2466 • Number of medical devices that do not conform to basic endpoint protection best  
2467 practices, trended over time. The goal is to reduce the number of medical devices that  
2468 do not meet the basic hygiene management practices or to implement practices for  
2469 these devices. It is not always possible to reduce this number to zero. Mitigating  
2470 factors should be leveraged to keep it as low as possible.
- 2471 • Number of devices that have unknown risks due to lack of manufacturer disclosure  
2472 information, trended over time. The goal is to ensure device manufacturers have  
2473 vulnerability disclosure programs and that your organization is tied into these processes.

2474 **References**

- 2475 • (Postmarket Management of Cybersecurity in Medical Devices 2016)
- 2476 • (NIST SP 1800-8: Securing Wireless Infusion Pumps In Healthcare Delivery Organizations  
2477 2017)

2478  
2479

2480

## Cybersecurity Best Practice #10: Cybersecurity Policies

2481 Cybersecurity policies must be  
 2482 established for the workforce  
 2483 to understand their expected  
 2484 behaviors within the  
 2485 organization as they relate to  
 2486 cybersecurity. These policies  
 2487 should be written for the  
 2488 various user audiences that  
 2489 exist in the organization. There  
 2490 are differences between the  
 2491 general workforce user, IT user,  
 2492 and high profile/risk users (e.g.,  
 2493 Finance, HR, or Health  
 2494 Information Management).

Best Practice 10: Cybersecurity Policies	
Data that may be affected	-
Baseline Practices	A. Policies
Advanced Practices	-
Key Mitigated Risks	<ul style="list-style-type: none"> <li>Email Phishing Attacks</li> <li>Ransomware Attacks</li> <li>Loss or Theft of Equipment or Data with Sensitive Information</li> <li>Accidental or Intentional Data Loss</li> <li>Attacks Against Connected Medical Devices and Patient Safety</li> </ul>

2495 New cybersecurity hygiene  
 2496 controls should be supported by institutional policy to set the proper expectations. Without these  
 2497 policies, it may be unclear to the workforce what level of adherence is required and what activities put  
 2498 the organization at risk for the threat types discussed in this document.

2499 **A number of policy templates have been provided in the Appendices.**

2500 **A. Policies** **(NIST Framework: IDENTIFY)**

2501 There is only one general safeguard for this section and that is a listing of policies that organizations can  
 2502 consider, described in Table 15.

Policy Name	Description	User Base
<b>Roles and Responsibilities</b>	Define all cybersecurity roles and responsibilities throughout the organization. This includes who will establish policy as well as implement and conduct security practices.	All users.
<b>Education and Awareness</b>	Define the mechanisms that will be used to train the workforce on cybersecurity practices, threats and mitigations.	All users.  Cybersecurity Department.
<b>Acceptable Use / Email Use</b>	Describe actions that users are permitted and not permitted to take. Explicitly define how email is to be used and leveraged.	All users.
<b>Data Classification</b>	Define how data are to be classified with usage parameters around those classifications.	All users.

<b>Personal Devices</b>	Define the organization’s position on the usage of personal devices (i.e., BYOD). If these are permitted, establish expectations for how the devices will be managed.	All users.
<b>Laptop, Portable Device, and Remote Use</b>	Define policies for the security of mobile devices and how they are to be used in a remote setting.	All users. IT Department.
<b>Incident Reporting and Checklist</b>	Define user requirements to report suspicious activities within the organization. Define responsibilities of the cybersecurity department for managing incidents.	All Users. Cybersecurity Department.
<b>Disaster Recovery Plan</b>	Define the practices deployed to recover IT assets in the case of a disaster, including backup plans.	IT Department.
<b>IT Controls Policies</b>	Describe the requirements for IT security controls in a series of policies or a single long policy. Examples include Access Control, Identity Management, Configuration Management, Vulnerability Management, and Data Center management.	IT Department.
<b>IT Acquisition Policy</b>	Define the criteria that must be implemented to ensure proper identification and protection of all IT assets purchased by the organization.	Supply Chain / Procurement Users. IT Department.

2503 *Table 15. Cybersecurity Policies to Be Considered*

2504 **Threats Mitigated**

- 2505 1. Email Phishing Attacks
- 2506 2. Ransomware Attacks
- 2507 3. Loss or Theft of Equipment or Data
- 2508 4. Internal, Accidental or Intentional Data Loss
- 2509 5. Attacks Against Connected Medical Devices that can Affect Patient Safety

2510 **Suggested Metrics**

- 2511 • Number of policies reviewed over a specified timeframe. The goal is to establish a
- 2512 standard practice to review policies and monitor compliance with this standard.
- 2513 • Number of workforce members review and sign off after reading policies over a
- 2514 specified timeframe. The goal is to establish a standard practice for workforce members

2515  
2516  
2517  
2518

to review applicable policies and attest that this review has been completed, and for the organization to monitor compliance with this standard.

2519

## Appendix A: Acronyms and Abbreviations

2520

Acronym/Abbreviation	Definition
<b>ABAC</b>	Attribute Based Access Control
<b>ACCE</b>	American College of Clinical Engineering
<b>ADFS</b>	Active Directory Federation Services
<b>AHIP</b>	America’s Health Insurance Plans
<b>API</b>	Application Programming Interface
<b>ASL</b>	Assistant Secretary for Legislation
<b>ASPR</b>	Assistant Secretary for Preparedness and Response
<b>ATT&amp;CK</b>	Adversarial Tactics, Techniques & Common Knowledge
<b>AV</b>	Anti-Virus
<b>BYOD</b>	Bring Your Own Device
<b>C2</b>	Command and Control
<b>CASB</b>	Cloud Access Security Broker
<b>CEO</b>	Chief Executive Officer
<b>CHIO</b>	Chief Health Information Officer
<b>CHIP</b>	Children’s Health Insurance Program
<b>CIO</b>	Chief Information Officer
<b>CIRT</b>	Cybersecurity Incident Response Team
<b>CISO</b>	Chief Information Security Officer
<b>CISSP</b>	Certified Information Security Systems Professional
<b>CMS</b>	Centers for Medicare and Medicaid
<b>CNSSI</b>	Committee on National Security Systems Instruction

<b>COO</b>	Chief Operations Officer
<b>CSA</b>	Cybersecurity Act
<b>CVSS</b>	Common Vulnerability Scoring System
<b>DCC</b>	Distributed Checksum Clearinghouse
<b>DEP</b>	Device Enrollment Program
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DHS</b>	Department of Homeland Security
<b>DKIM</b>	Domain Key Identified Mail
<b>DLP</b>	Data Loss Prevention
<b>DMARC</b>	Domain-based Message Authentication Reporting and Conformance
<b>DMZ</b>	Demilitarized Zone
<b>DNS</b>	Domain Name System
<b>DNSRBL</b>	Domain Name System Real-time Blackhole List
<b>DoD</b>	Department of Defense
<b>DOS</b>	Denial of Service
<b>DRP</b>	Disaster Recovery Plan
<b>DSM</b>	Direct Secure Messaging
<b>EA</b>	Enterprise Architecture
<b>EDR</b>	Endpoint Detection and Response
<b>EHR</b>	Electronic Health Record
<b>EMR</b>	Electronic Medical Record
<b>EPHI</b>	Electronic Private Health Information
<b>ERP</b>	Enterprise Resource Planning
<b>FDA</b>	Food and Drug Administration

<b>FERPA</b>	Family Educational Rights and Privacy Act
<b>FIPS</b>	Federal Information Processing Standards
<b>FISMA</b>	Federal Information Security Modernization Act
<b>GDPR</b>	General Data Protection Regulation
<b>GINA</b>	Genetic Information Nondiscrimination Act
<b>HCIC</b>	Health Care Industry Cybersecurity
<b>HDO</b>	Health Delivery Organization
<b>HHS</b>	Department of Health and Human Services
<b>HIDS</b>	Host Based Intrusion Detection Systems
<b>HIMSS</b>	Health Information Management and Systems Society
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>HIPS</b>	Host Based Prevention Systems
<b>HIT</b>	Health Information Technology
<b>HITECH</b>	Health Information Technology Economic and Clinical Health Act
<b>HMO</b>	Health Maintenance Organization
<b>HPH</b>	Healthcare and Public Health
<b>HR</b>	Human Resources
<b>HRSA</b>	Health Resources and Services Administration
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>IA</b>	Information Assurance
<b>IAM</b>	Identity and Access Management
<b>IBM</b>	International Business Machines
<b>ICAP</b>	Internet Content Adaptation Protocol



<b>ICMP</b>	Internet Control Message Protocol
<b>ICS-CERT</b>	Industrial Control Systems – Computer Emergency Response Teams
<b>ICU</b>	Intensive Care Unit
<b>IDS</b>	Intrusion Detection System
<b>INFOSEC</b>	Information Security
<b>IOC</b>	Indicator of Compromise
<b>IoT</b>	Internet of Things
<b>IP</b>	Intellectual Property or Internet Protocol
<b>IPS</b>	Intrusion Prevention System or Internet Partner Services
<b>ISAC</b>	Information Sharing and Analysis Center
<b>ISAO</b>	Information Sharing and Analysis Organization
<b>IT</b>	Information Technology
<b>ITAM</b>	Information Technology Asset Management
<b>LAN</b>	Local Area Network
<b>LANMAN</b>	Local Area Network Manager
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LLC</b>	Limited Liability Corporation
<b>MAC</b>	Media Access Control
<b>MACRA</b>	Medicare access and the Children’s Health Insurance Program Reauthorization Act
<b>MARS</b>	Minimum Acceptable Risk Standards
<b>MDM</b>	Mobile Device Management
<b>MDS2</b>	Manufacturer Disclosure Statement for Medical Device Security

<b>MFA</b>	Multi-Factor Authentication
<b>MITRE</b>	The MITRE Corporation
<b>MPLS</b>	Multiprotocol Label Switching
<b>NAC</b>	Network Access Control
<b>NCCIC</b>	National Cybersecurity and Communications Integration Center
<b>NCI</b>	National Cancer Institute
<b>NEMA</b>	Association of Electrical Equipment and Medical Imaging Manufacturers
<b>NH-ISAC</b>	National Healthcare – Information Sharing and Analysis Centers
<b>NIH</b>	National Institutes of Health
<b>NIST</b>	National Institute of Standards and Technology
<b>NNCOE</b>	NIST National Cybersecurity Center of Excellence
<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>OS</b>	Operating System
<b>OWASP</b>	Open Web Application Security Project
<b>PACS</b>	Pictures Archiving and Communication Systems
<b>PCI-DSS</b>	Payment Card Industry Data Security Standard
<b>PCS</b>	Patient Care Service
<b>PHI</b>	Personal Health Information
<b>PII</b>	Personal Identifiable Information

<b>RBAC</b>	Rule Based Access Control
<b>RBL</b>	Real-time Blackhole List
<b>RDP</b>	Remote Desktop Protocol
<b>RFI</b>	Request for Information
<b>RFP</b>	Request for Proposal
<b>ROM</b>	Read Only Memory
<b>SaaS</b>	Software as a Service
<b>SAMHSA</b>	Substance Abuse and Mental Health Services Administration
<b>SAML</b>	Security Assertion Markup Language
<b>SBOM</b>	Software Bill of Materials
<b>SIEM</b>	Security Incident and Event Management
<b>SMB</b>	Server Message Block
<b>SME</b>	Subject Matter Expert
<b>S/MIME</b>	Secure Multi-Purpose Internet Mail Extensions
<b>SMS</b>	Short Message Service
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SOC/IR</b>	Security Operations Center / Incident Response
<b>SPAN</b>	Switched Port Analyzer
<b>SPF</b>	Sender Policy Framework
<b>SQL</b>	Structured Query Language
<b>SSH</b>	Secure Shell
<b>SSN</b>	Social Security Number
<b>SSO</b>	Single Sign On
<b>STIG</b>	Security Technical Implementation Guide

<b>STIX</b>	Structure Threat Information eXpression
<b>SVP</b>	Senior Vice President
<b>TAXII</b>	Trusted Automated eXchange of Indicator Information
<b>TLS</b>	Transport Layer Security
<b>TXT</b>	Text
<b>UBA</b>	User Behavior Analytics
<b>URL</b>	Uniform Resource Locator
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USB</b>	Universal Serial Bus
<b>VAR</b>	Value Added Reseller
<b>VP</b>	Vice President
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide Area Network
<b>WORM</b>	Write Once Read Many

2521  
2522  
2523  
2524  
2525