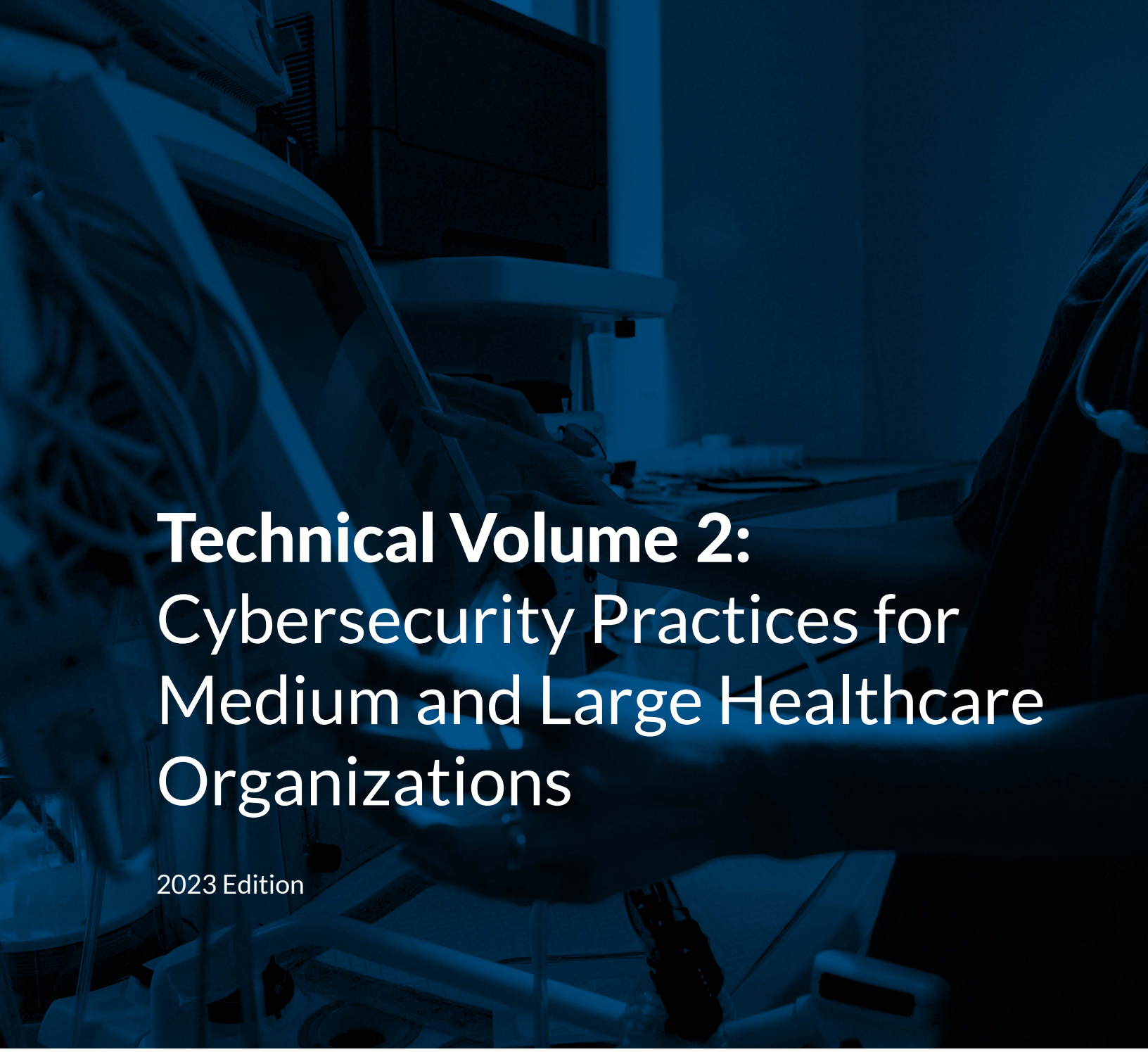


Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations

2023 Edition

Healthcare & Public Health Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Table of Contents

List of Tables

Introduction

This volume will help answer the question, "How do I mitigate the five threats outlined in the Main Document?"

Technical Volume 2 outlines healthcare cybersecurity best practices for medium-sized and large healthcare organizations. Medium-sized and large organizations generally have dedicated information technology (IT) departments, and very likely have dedicated cybersecurity staff. Organizational personnel typically have an awareness of the cybersecurity threats faced to patients and their organization.

This volume is for the technical practitioner and contains technical details for implementing cybersecurity practices. It provides an overview of cybersecurity practices that have been outlined by the industry as highly effective at mitigating risks to the healthcare industry.

This volume is an index of existing industry practices, with guidance on how to start your journey implementing these practices. Details and explanations of the cybersecurity practices are included for additional context where needed.

To determine the size of your organization, please refer to Main Document, Table 1. Examples of medium-sized organizations are community hospitals, critical access hospitals with more than 50 beds, or larger medical groups. Examples of larger organizations include large health systems with multiple hospitals, integrated delivery networks, or clinical groups with multiple geographically dispersed locations.

Please consider these simple instructions when reading this volume:

1. If you are a medium-sized organization, start with the sub-practices with the heading "Sub- Practices for Medium-Sized Organizations." Feel free to consider the additional sub-practices as well.
2. If you are a large organization, consider implementing all the sub-practices listed in the document, including both those under the heading "Sub-Practices for Medium-Sized Organizations" **as well as** those labeled "Sub-Practices for Large Organizations."

Cybersecurity Practices at Medium-Sized Healthcare Organizations

Medium-sized healthcare organizations perform critical functions for the healthcare and public health (HPH) sector. These organizations include critical access hospitals in rural areas, practice management organizations that support physician practices, revenue cycle or billing organizations, mid-sized device manufacturers, and group practices. Medium-sized healthcare organizations generally employ hundreds of personnel, maintain between hundreds and a few thousand IT assets, and may be primary partners with and liaisons between small and large healthcare organizations. It is typical for a medium-sized organization to have several critical systems that are interconnected to enable work activities in support of its mission.

These organizations tend to have a diverse inventory of assets that support multiple revenue streams. They also tend to have narrow profit margins, limited resources, and limited flexibility to implement robust cybersecurity practices. For example, it is rare for a medium-sized organization to have its own dedicated 24x7x365 security operations center (SOC).

Medium-sized organizations typically focus on preventing cybersecurity events and implementing restrictive security policies with few exceptions permitted. These restrictive policies are often due to insufficient resources to support more open and flexible cybersecurity models, such as those larger organizations can often afford. Medium-sized organizations usually struggle to obtain cybersecurity funding that is distinct from their standard IT budgets. The top security professionals in an organization of this size might often feel overwhelmed by compliance and cybersecurity duties, wear multiple hats, and experience constraints around execution plans.

Medium-sized organizations operate in complex legal and regulatory environments that include, but are not limited to, the following:

- The Office of the National Coordinator for Health Information Technology (ONC) regulations prohibiting information blocking and promoting the interoperability of Certified Electronic Health Information Technology[1]
- The Medicare Access and Children's Health Insurance Program Reauthorization Act of 2015 (MACRA)/Meaningful Use[2]
- Multiple enforcement obligations under the Food and Drug Administration (FDA)[3]
- The Joint Commission or DNV accreditation processes[4]
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH) requirements[5]

1 ONC Cures Act Final Rule, https://www.healthit.gov/curesrule/.
2 "MACRA," Centers for Medicare and Medicaid Services (CMS), https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/MACRA-MIPS-and-APMs/MACRA-MIPS-and-APMs#:~:text=The%20Medicare%20Access%20and%20CHIP,clinicians%20for%20value%20over%20volume.
3 "Cybersecurity," FDA, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.
4 "Learn the Process," The Joint Commission, https://www.jointcommission.org/accreditation-and-certification/become-accredited/learn-the-process/.
5 "The HIPAA Privacy Rule," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. "HITECH Act Enforcement Interim Final Rule," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

- The Payment Card Industry Data Security Standard (PCI-DSS1)[6]
- Substance Abuse and Mental Health Services Administration (SAMHSA) requirements (42 CFR part 2)[7]
- The Gramm-Leach-Bliley Act for financial processing[8]
- The Family Educational Rights and Privacy Act (FERPA) for those institutions participating within Higher Education[9]
- The Genetic Information Nondiscrimination Act (GINA)[10]
- The General Data Protection Regulation (GDPR) in the European Union[11]
- State laws setting standards for privacy and security such as the California Consumer Privacy Act (CCPA)[12]

Changes to the Stark Law Physician self-referral regulations and the related anti-kickback statute took effect in January 2021. These protect the donation of cybersecurity technology and services that are "necessary and used predominantly to implement, maintain, reestablish effective cybersecurity."[13]

IT Assets Used by Medium-Sized Organizations

Medium-sized organizations may have up to a few thousand IT assets. All assets may have cybersecurity vulnerabilities and are therefore susceptible to cyber threats. There are three important factors in securing assets: (1) understanding their relationship within your organization's IT ecosystem; (2) understanding how the workforce leverages and uses the assets; and (3) understanding the data that are generated, stored, and processed within those assets.

Not all assets are equally important; some are mission critical and must be fully operational due to patient safety, while others are less critical, and might even be offline for days or weeks without harming your organization's mission. Some assets are critical for patient care, such as bedside monitors, whereas others have large repositories of sensitive data that represent significant risk but are not as critical to the enterprise's business. In all cases, your organization uses IT assets for business reasons and should protect those assets with proper cyber hygiene controls.

Examples of assets found in medium-sized organizations include, but are not limited to, the following:

- Static devices used by the workforce, such as shared workstations and clinical workstations used strictly for patient care with select mobile devices, such as laptops and smartphones. Due to budget restrictions, medium-sized organizations may not maintain many mobile devices.

6 "PCI DSS v4.0 Resource Hub," PCI Security Standards Council, https://www.pcisecuritystandards.org/.
7 "Registration Requirements," SAMHSA, https://www.samhsa.gov/grants/applying/registration-requirements.
8 "Gramm-Leach-Bliley Act," FTC, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.
9 "Family Educational Rights and Privacy Act (FERPA)," US Department of Education, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
10 "Genetic Information," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html.
11 "General Data Protection Regulation: GDPR," Intersoft Consulting, https://gdpr-info.eu/.
12 "California Consumer Privacy Act (CCPA)," State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.
13 The Stark Law, 42 C.F.R. § 411.357(bb)(1) and the Anti-Kickback Statute, 42 C.F.R. § 1001.952(jj) are the result of the CMS Final Rule at 85 Fed. Reg. 77,492 (December 2, 2020).

- Internet of things (IoT) devices, such as smart televisions, medical devices, thermometers, printers, copiers, and security cameras.
- Data that includes sensitive health information stored and processed on devices, servers, applications, and the cloud. These data include names, medical record numbers, birth dates, Social Security numbers (SSNs), diagnostic conditions, prescriptions, mental health issues, substance abuse, or sexually transmitted disease information. Individually identifiable health information (IIHI) about a patient that is created or maintained by a HIPAA covered entity is protected health information (PHI) and must be safeguarded against unauthorized use or disclosure.
- Assets related to the IT infrastructure, such as firewalls, network switches and routers, Wi-Fi networks (both corporate and guest), servers supporting IT management systems, and file storage systems (cloud-based or onsite).
- Applications or information systems that support the business processes. These may include human resource (HR) or enterprise resource planning (ERP) systems, pathology lab systems, blood bank systems, medical imaging systems, pharmacy systems, revenue cycle systems, supply chain or materials management systems, specialized oncology therapy systems, radiation oncology treatment systems, and data warehouses (e.g., clinical, financial).

Personal devices, often referred to as "bring your own device" (BYOD), are often not permitted in medium-sized organizations due to its inability to implement dedicated security controls required to secure such devices.

Cybersecurity Practices

At a minimum, medium-sized organizations should consider implementing the *Sub-Practices for Medium-Sized Organizations* discussed in each cybersecurity practice presented in this volume. However, medium-sized organizations may additionally adopt the cybersecurity practices used by large organizations.

Organizations should consider adopting any cybersecurity practice determined to be relevant.

Cybersecurity Practices at Large Healthcare Organizations

Large healthcare organizations perform a range of different functions. These organizations may be integrated with other healthcare delivery organizations, academic medical centers, insurers that provide healthcare coverage, clearinghouses, pharmaceuticals, or medical device manufacturers. In most cases, large organizations employ thousands of employees, maintain tens of thousands to hundreds of thousands of IT assets, and have intricate and complex digital ecosystems. Whereas smaller organizations operate using only a few critical systems, large organizations can have hundreds or thousands of interconnected systems with complex functionality.

The missions of large organizations are diverse and varied. They include providing standard general practice care, providing specialty or subspecialty care for complicated medical cases, conducting innovative medical research, providing insurance coverage to large populations of patients, supporting the healthcare delivery ecosystem, and supplying and researching new therapeutic treatments (such as drugs or medical devices).

Large organizations have missions that are broad in scope, and large volumes of assets may be necessary to fulfill such missions. They often struggle to obtain funding to maintain security programs and control their assets (potentially resulting in shadow IT, rogue devices, and unmanaged/unpatched devices). Therefore, it is essential for large organizations to understand how sensitive data flow in and out of their organization, and to understand the boundaries and segments that determine where one entity's responsibilities end, and another's start.

Large organizations operate in a legal and regulatory environment that is as complicated as their digital ecosystems. This environment includes, but is not limited to, the following references:

- The Office of the National Coordinator for Health Information Technology (ONC) regulations prohibiting information blocking and promoting the interoperability of Certified Electronic Health Information Technology[14]
- The Medicare Access and Children's Health Insurance Program Reauthorization Act of 2015 (MACRA)/Meaningful Use [15]
- Multiple enforcement obligations under the Food and Drug Administration (FDA)[16]
- The Joint Commission or DNV accreditation processes[17]
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH) requirements[18]

14 ONC Cures Act Final Rule, https://www.healthit.gov/curesrule/.
15 "MACRA," Centers for Medicare and Medicaid Services (CMS), https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/MACRA-MIPS-and-APMs/MACRA-MIPS-and-APMs#:~:text=The%20Medicare%20Access%20and%20CHIP,clinicians%20for%20value%20over%20volume.
16 "Cybersecurity," FDA, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.
17 "Learn the Process," The Joint Commission, https://www.jointcommission.org/accreditation-and-certification/become-accredited/learn-the-process/.
18 "The HIPAA Privacy Rule," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. "HITECH Act Enforcement Interim Final Rule," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

- The Payment Card Industry Data Security Standard (PCI-DSS1)[19]
- Substance Abuse and Mental Health Services Administration (SAMHSA) requirements (42 CFR part 2)[20]
- The Gramm-Leach-Bliley Act for financial processing[21]
- The Stark Law as it relates to providing services to affiliated organizations[22]
- The Family Educational Rights and Privacy Act (FERPA) for those institutions participating within Higher Education[23]
- The Genetic Information Nondiscrimination Act (GINA)[24]
- The General Data Protection Regulation (GDPR) in the European Union[25]
- State laws setting standards for privacy and security such as the California Consumer Privacy Act (CCPA)[26]
- Minimum Acceptable Risk Standards for exchangers[27]
- Federal Information Security Modernization Act (FISMA) requirements as incorporated into federal contracts and research grants through agencies such as the National Institutes of Health (NIH)[28]

Changes to the Stark Law physician self-referral regulations and the related anti-kickback statute took effect in January 2021. These protect the donation of cybersecurity technology and services that are "necessary and used predominantly to implement, maintain, reestablish effective cybersecurity."[29]

IT Assets Used by Large Organizations

Large organizations support their operations with complicated ecosystems of IT assets. All assets may have cybersecurity vulnerabilities and are susceptible to cyber threats. There are three important factors in securing assets: (1) understanding their relationship within your organization's IT ecosystem, (2) understanding how the workforce leverages and uses the assets, and (3) understanding the data generated, stored, and processed within those assets.

19 "PCI DSS v4.0 Resource Hub," PCI Security Standards Council, https://www.pcisecuritystandards.org/.
20 "Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule," SAMHSA, https://www.samhsa.gov/newsroom/press-announcements/202007131330.
21 "Gramm-Leach-Bliley Act," FTC, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.
22 "Fraud & Abuse Laws," HHS Office of Inspector General, https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/#:~:text=The%20Physician%20Self%2DReferral%20Law%2C%20commonly%20referred%20to%20as%20the,relationship%2C%20unless%20an%20exception%20applies.
23 "Family Educational Rights and Privacy Act (FERPA)," US Department of Education, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
24 "Genetic Information," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html.
25 "General Data Protection Regulation: GDPR," Intersoft Consulting, https://gdpr-info.eu/.
26 "California Consumer Privacy Act (CCPA)," State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.
27 "Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0," HHS Guidance Portal, https://www.hhs.gov/guidance/document/minimum-acceptable-risk-standards-exchanges-mars-e-20.
28 "4.1.9 Federal Information Security Management Act," NIH, https://grants.nih.gov/grants/policy/nihgps/html5/section_4/4.1.9_federal_information_security_management_act.htm.
29 The Stark Law, 42 C.F.R. § 411.357(bb)(1) and the Anti-Kickback Statute, 42 C.F.R. § 1001.952(jj) are the result of the CMS Final Rule at 85 Fed. Reg. 77,492 (December 2, 2020).

Not all assets are equally important. Some are mission critical and must always be fully operational, while others are less critical, and might even be offline for days or weeks without harming your organization's mission or causing impact to patient safety. Some assets have large repositories of sensitive data that represent significant risk that are not necessarily critical to the enterprise's business. In all cases, organizations use IT assets for business reasons and should protect those assets with proper cyber hygiene controls.

Examples of assets found in large organizations include, but are not limited to, the following:

- Devices used by the workforce that enable internet connectivity, such as mobile phones, tablets, voice recorders, and laptop computers for dictation.
- Personal devices creating or maintaining sensitive data, often referred to as BYOD.
- Large deployments of IoT assets, including smart televisions, networked medical devices, printers, copiers, security cameras, refrigeration sensors, blood bank monitoring systems, building management sensors, and more.
- Data that includes IIHI stored and processed on devices, servers, applications, and the cloud. This data could include names, medical record numbers, birth dates, SSNs, diagnostic conditions, prescriptions, and mental health, substance abuse, or sexually transmitted disease information. IIHI about a patient that is created or maintained by a HIPAA covered entity is PHI that must be safeguarded against unauthorized use or disclosure.
- Assets related to the IT infrastructure, such as firewalls, network switches and routers, Wi-Fi networks (corporate and guest), servers supporting IT management systems, and file storage systems (cloud-based or onsite).
- Applications or information systems that support business processes. These can include ERPs, pathology lab systems, blood bank systems, medical imaging systems, pharmacy systems (retail and specialized), revenue cycle systems, supply chain or materials management systems, specialized oncology therapy systems, radiation oncology treatment systems, data warehouses (clinical, financial, research), vendor management systems, and more.

Document Guide: Cybersecurity Practices

This volume provides medium-sized and large organizations with a series of cybersecurity practices to prevent, react to, and recover from the five cybersecurity threats identified in Table 1 below and discussed in the Main Document (See the Main Document for detailed definitions and descriptions of each threat).

Table 1. Five Prevailing Cybersecurity Threats to Healthcare Organizations

Threat	Potential Impact of Attack
Social engineering	Malware delivery or credential attacks. Both attacks further compromise your organization.
Ransomware attack	Information system assets locked and held for payment of ransom (extortion). Disrupts normal healthcare operations. Prevents business functions like electronic billing for treatment services. May lead to a breach of sensitive information and patient identify theft, as bad actors have started exporting data and publishing it as part of the extortion strategy.
Loss or theft of equipment or data	Breach of sensitive information. May lead to patient identity theft.
Insider, accidental or malicious data loss	Removal of data from your organization (intentionally or unintentionally). May lead to a breach of sensitive information. May also lead to patient identify theft.
Attacks against network connected medical devices	Undermined patient safety, delay or disruption of treatment, and well-being.

Each cybersecurity practice responding to the threats listed above is broken up into three core segments: **Sub-Practices for Medium-Sized Organizations** (or *medium sub-practices)*, **Sub-Practices for Large Organizations** (or *large sub-practices*) and the **Threats Mitigated** by the practice. Each practice also contains a series of suggested metrics to measure the effectiveness of the cybersecurity practice.

Medium sub-practices apply to *both* medium-sized and large organizations. Large sub-practices are designed for application by large organizations. These large sub-practices could also benefit an organization of any size that has an interest in adopting them.

The following tables present summaries of each of the cybersecurity practices described herein.

Cybersecurity Practice 1: Email Protection Systems	
Assets Affected	Sensitive Data, System Integrity
Medium Sub-Practices	**1.M.A** Basic Email Protection Controls **1.M.B** Multi-Factor Authentication for Remote Access **1.M.C** Email Encryption **1.M.D** Workforce Education
Large Sub-Practices	**1.L.A** Advanced and Next-Generation Tooling **1.L.B** Digital Signatures **1.L.C** Analytics Driven Education
Key Mitigated Risks	• Social engineering • Ransomware attacks • Insider, accidental or malicious data loss

Cybersecurity Practice 2: Endpoint Protection Systems	
Assets Affected	Sensitive Data, System Integrity, System Availability
Medium Sub-Practices	**2.M.A** Basic Endpoint Controls **2.M.B** Mobile Device Management
Large Sub-Practices	**2.L.A** Automate the Provisioning of Endpoints **2.L.B** Host Based Intrusion Detection/Prevention Systems **2.L.C** Endpoint Detention Response **2.L.D** Application Allowlisting **2.L.E** Micro-Segmentation/Virtualization Strategies
Key Mitigated Risks	• Ransomware attacks • Loss or theft of equipment or data

Cybersecurity Practice 3: Identity and Access Management	
Assets Affected	Sensitive Data Information Systems
Medium Sub-Practices	**3.M.A** Identity **3.M.B** Provisioning, Transfers, and Deprovisioning Procedures **3.M.C** Authentication **3.M.D** Multi-Factor Authentication for Remote Access
Large Sub-Practices	**3.L.A** Federated Identity Management **3.L.B** Authorization **3.L.C** Access Governance **3.L.D** Single Sign-On
Key Mitigated Risks	• Ransomware attacks • Insider, accidental or malicious data loss • Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice 4: Data Protection and Loss Prevention	
Assets Affected	Passwords, PHI
Medium Sub-Practices	**4.M.A** Classification of Data **4.M.B** Data Use Procedures **4.M.C** Data Security **4.M.D** Backup Strategies **4.M.E** Data Loss Prevention
Large Sub-Practices	**4.L.A** Advanced Data Loss Prevention **4.L.B** Mapping of Data Flows
Key Mitigated Risks	• Ransomware attacks • Loss or theft of equipment or data • Insider, accidental or malicious data loss

Cybersecurity Practice 5: IT Asset Management	
Assets Affected	Passwords, PHI
Medium Sub-Practices	**5.M.A** Inventory of Endpoints and Servers **5.M.B** Procurement **5.M.C** Secure Storage for Inactive Devices **5.M.D** Decommissioning Assets
Large Sub-Practices	**5.L.A** Automated Discovery and Maintenance **5.L.B** Integration with Network Access Control
Key Mitigated Risks	• Ransomware attacks • Loss or theft of equipment or data • Insider, accidental or malicious data loss • Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice 6: Network Management	
Assets Affected	PHI
Medium Sub-Practices	**6.M.A** Network Profiles and Firewalls **6.M.B** Network Segmentation **6.M.C** Intrusion Prevention Systems **6.M.D** Web Proxy Protection **6.M.E** Physical Security of Network Devices
Large Sub-Practices	**6.L.A** Additional Network Segmentation **6.L.B** Network Analytics and Blocking **6.L.C** Network Access Control

Cybersecurity Practice 6: Network Management	
Key Mitigated Risks	• Ransomware attacks • Loss or theft of equipment or data • Insider, accidental or malicious data loss • Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice 7: Vulnerability Management	
Assets Affected	PHI
Medium Sub-Practices	**7.M.A** Host/Server Based Scanning **7.M.B** Web Application Scanning **7.M.C** System Placement and Data Classification **7.M.D** Patch Management, Configuration Management **7.M.E** Change Management
Large Sub-Practices	**7.L.A** Penetration Testing **7.L.B** Vulnerability Remediation Planning **7.L.C** Attack Simulation
Key Mitigated Risks	• Ransomware attacks • Insider, accidental or malicious data loss • Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice 8: Security Operations Center and Incident Response	
Assets Affected	PHI
Medium Sub-Practices	**8.M.A** Security Operations Center **8.M.B** Incident Response **8.M.C** Information Sharing and ISACs/ISAOs
Large Sub-Practices	**8.L.A** Advanced Security Operations Center **8.L.B** Advanced Information Sharing **8.L.C** Incident Response Orchestration **8.L.D** Baseline Network Traffic **8.L.E** User Behavior Analytics **8.L.F** Deception Technologies
Key Mitigated Risks	• Social engineering • Ransomware attacks • Loss or theft of equipment or data • Insider, accidental or malicious data loss • Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice 9: Network Connected Medical Devices	
Assets Affected	PHI
Medium Sub Practices	**9.M.A** Medical Device Management **9.M.B** Endpoint Protections **9.M.C** Identity and Access Management **9.M.D** Asset Management **9.M.E** Vulnerability Management **9.M.F** Contacting the FDA
Large Sub-Practices	**9.L.B** Security Operations and Incident Response **9.L.C** Procurement and Security Evaluations
Key Mitigated Risks	• Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice 10: Cybersecurity Oversight and Governance	
Assets Affected	N/A
Medium Sub-Practices	**10.M.A** Policies **10.M.B** Cybersecurity Risk Assessment and Management **10.M.C** Security Awareness and Training
Large Sub-Practices	**10.L.A** Cyber Insurance
Key Mitigated Risks	• Social engineering • Ransomware attacks • Loss or theft of equipment or data • Insider, accidental or malicious data loss • Attacks against network connected medical devices that may affect patient safety

Cybersecurity Practice #1: Email Protection Systems

Areas of Impact
Sensitive Data, System Integrity

Medium Sub-Practices
- **1.M.A** Basic Email Protection Controls
- **1.M.B** Multi-factor Authentication for Remote Access
- **1.M.C** Email Encryption
- **1.M.D** Workforce Education

Large Sub-Practices
- **1.L.A** Advanced and Next-Generation Tooling
- **1.L.B** Digital Signatures
- **1.L.C** Analytics Driven Education

Key Threats Addressed
- Social engineering
- Ransomware attacks
- Insider, accidental, or malicious data loss

405(d) Resources
- Prescription Poster: Email Protection Systems
- Five Threats Flyers:
  - Social Engineering
  - Ransomware Attacks
  - Insider, Accidental or Malicious Data Loss

According to the 2021 Verizon Data Breach Investigations Report, phishing was "present in 36% of breaches (up from 25% last year)." Additionally, 23% of malware was delivered through email.[30] Phishing isn't the only social engineering threat to be concerned with. There has also been a rise in Business Email Compromise (BEC) attacks, whereby scammers attempt to trick business and individuals to perform fraudulent wire transfer payments.[31] Though other areas of significant threat exist (including in the web application space), the effectiveness of phishing attacks allows attackers to bypass most perimeter detections by "piggy backing" on legitimate workforce users. If an attacker obtains an employee's password through any type of social engineering attack, and if that employee has remote access to your organization's IT assets, the attacker has made significant progress toward penetrating your organization.

The two most common phishing methods are credential theft (leveraging email to conduct a credential harvesting attack on your organization) and malware dropper attacks (email delivery of malware that can compromise endpoints). An organization's cybersecurity practices must address these two attack vectors. Because both attack types leverage email, email systems should be the focus for additional security controls.

Sub-Practices for Medium-Sized Organizations

1.M.A: Basic Email Protection Controls

NIST Framework Ref: ID.RA-2, PR.AC-4, PR.AC-1, PR.AC-7, PR.DS-2, PR.PT-3, DE.CM-4

Standard phishing detection, antispam, and antivirus (AV) filtering controls are basic protections that should be implemented in any email system. They are implemented directly on the email platform. These controls assess inbound and outbound emails from known malicious senders or patterns of malicious content. **Table 2** below provides a list of suggested security implementations for email protection controls.

30 "2021 Data Breach Investigations Report," Verizon (2021), 56, https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.
31 "2021 Data Breach Investigations Report," Verizon (2021), 25, https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.

Table 2. Email Protection Controls

Control	Description
Real-time deny list[32]	Community-based lists of IP addresses and host names of known or potential spam originators. Consider lists provided by Spamhaus, Spamcop, DNSRBL, or by your email vendor.
Distributed Checksum Clearinghouse (DCC)	The DCC is a distributed database that contains a checksum of messages. Email messages go 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.
Removal of open relays	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 you must configure it to allow messages only from trusted sources. Failure to do this may permit a spammer or hacker to exploit the "trust" of your mail server to transmit malicious content.
Spam/virus check on outbound messages	Spam/virus checks on outbound emails can detect malicious content, revealing compromised accounts and potential security incidents. Review email spam/virus rules as part of **Cybersecurity Practice #8: Security Operations Center and Incident Response**.
AV check	Scan all email content against an AV engine with up-to-date signatures. If possible, this control should unpack compressed files (such as zip files) to check for embedded malware.
Restrict the "Send as" permission for distribution lists	Limit distribution lists to essential members. Distribution lists can enable attackers to disseminate malicious content from a compromised account. Therefore, they and should not be accessible to large numbers of users.
Implement sender policy framework (SPF) records	A Sender Policy Framework (SPF) record identifies which mail servers' policy framework (SPF) may send email on behalf of your domain. This enables the receiving mail records server to verify the authenticity of the sending mail server. This should be configured as part of a Domain-based Message Authentication Reporting and Conformance (DMARC) record.
Implement domain key identified mail (DKIM)	DKIM is a method of email authentication that uses cryptography to ensure that email messages come from authorized email servers. A public key is stored within your organization's domain name system (DNS) as a text (txt) record. All messages sent from that domain are digitally signed with a DKIM signature that can be validated through the DNS public key txt record. This should be configured as part of a DMARC record.

32 Murthy Raju, "Using RBL and DCC for Spam Protection," Linux.com (Last modified June 14, 2007), https://www.linux.com/news/using-rbl-and-dcc-spam-protection.

Control	Description
Implement domain-based message authentication reporting and conformance (DMARC)[33]	DMARC is an authentication technology that leverages both SPF and DKIM based message to validate an email's From: address (i.e., the sender). DMARC enables the receiving mail system to check SPF and DKIM records, ensuring conformance reporting to the sending host as well as the "From:" address. It instills trust that the sending party's email address is not spoofed; spoofing is a common attack type used to trick users into opening malicious emails.

In most cases, email protection controls do not operate alone. When combined to evaluate an organization's emails, they contribute information that provides a more complete assessment of each message. Modern systems score email content on each pass through the protection controls.

Organizations should implement this scoring technique and set at least three thresholds: OK for Delivery, Quarantine, or Block/Drop. Each email should be scored to determine which of the three thresholds applies. Based on that threshold, automated actions should be executed. Emails cleared for delivery automatically pass through for additional processing. The email protection system discards Block/Drop emails, and the user never sees them. Quarantine actions allow the user to evaluate the message in a secured environment (not the user's regular email box) for final verification. In most cases, the system delivers quarantined messages to the user daily in a single email digest for verification.

Adding X-Headers to the delivery of email messages is a good way to flag potential spam or malicious email before sending it to the user. There are two common methods to accomplish this:[34]

- ***Spam X-Header:*** If a message receives a score that prevents the system from definitively classifying it as spam/malicious, the system can tag the message with an X-Header. The system modifies the subject or the top of the body of the message to include a [POSSIBLE SPAM] tag. This advises the user to verify whether a message is legitimate prior to opening it.
- ***External Sender X-Header:*** Another common practice is to add an [EXTERNAL] tag to inbound messages from external senders. The tag can be configured to be highly visible, such as *"WARNING: Stop. Think. Read. This is an external email."* This method is effective at identifying messages that might be spoofed or faked to appear to have come from within your organization. It also informs the email recipient to be cautious when clicking links or opening attachments from these sources. If you leverage DMARC, you might consider exempting the External Sender X-header tag for messages sent on behalf of your organization (e.g., hosted human resources [HR] systems) that pass DMARC authentication. This may help email users understand the trust environment and identify when it is necessary to be extra vigilant. Additionally, you may want to consider exempting messages from other trusted partners to avoid alert fatigue.

Messages can also be marked (or digitally signed) when they originate from approved hosting or cloud-based services with a legitimate need to spoof an internal address. This is common for communications platforms, such as marketing systems, emergency management communications systems, or alert management systems.

33 KC Cross, Denise Vangel, and Meera Krishna, "Use DMARC to Validate Email in Office 365," Microsoft TechNet, (Last modified October 8, 2017), https://technet.microsoft.com/en- us/library/mt734386(v=exchg.150).aspx.

34 KC Cross and Denise Vangel, "Configure Your Spam Filter Policies," Microsoft TechNet, (Last modified December 13, 2017), https://technet.microsoft.com/en- us/library/jj200684(v=exchg.150).aspx.

1.M.B: Multi-Factor Authentication for Email Access

NIST Framework Ref: PR.AC-7

It is common and expected to share sensitive information through email systems. Email is the primary mechanism used by most organizations to communicate electronically. It is also common to access email remotely, as the workforce has become increasingly mobile.

Given the prevalence of credential harvesting attacks, if email systems are available, passwords are the only controls prohibiting malicious users from accessing sensitive information within transmitted emails. This is a critical exposure that increases organizations' susceptibility to phishing attacks.

As discussed in **Cybersecurity Practice #3: Identity and Access Management**, two-factor authentication, or multi-factor authentication (MFA), is the process of verifying a user's identity through more than one credential. The most common method is to leverage a soft token in addition to a password. The soft token is a second credential that can be delivered through a mobile phone or tablet, devices that most people have nearby. For example, the soft token could consist of a text message containing a code, or of an application installed on a smartphone that provides the code and/or asks for independent verification after a successful password entry.

Implementing MFA on the email platform mitigates compromised credential (i.e., user password) risk. With MFA, a hacker requires both the smartphone and the user's password, which significantly reduces the likelihood of a successful attack. MFA has proven to be an effective control to protect an organization's data from unauthorized access.

When implementing MFA, make sure to ensure all protocols used are multifactored. A common method for delivering email to mobile devices is to support Post Office Protocol (POP3) and Internet Message Access Protocol (IMAP) protocols. Unfortunately, these legacy protocols generally do not allow for MFA. As with the email provider, if these protocols are to be used, they must allow them to be accessible by only a single factor, generally the username and password. This back door can allow bad actors to access your email systems that might have MFA protection on the "front door." Be sure to switch over to the usage of modern email authentication, which allows all mobile and desktop clients to leverage MFA and disable these legacy authentication protocols.

1.M.C: Email Encryption

NIST Framework Ref: PR.DS-2

Email is the most common method of communicating content, including sensitive information, among members of an organization. Although email might not be the preferred communication method, one must assume that users will leverage this common and easy-to-use communication channel.

Email encryption is an important security protection. Multiple encryption techniques exist, though the most common use third-party applications to conduct encryption, invoking them by tagging outbound messages in some form. For example, tagging can occur by putting a trigger in the subject line (e.g., *#encrypt*, *#confidential*), or the email client itself can invoke the third-party application. The techniques used depend upon the technology solution deployed. By encrypting the envelope, you can ensure that no matter where the email is forwarded, it will maintain its encrypted status. This level of protection is more robust than implementing only transport layer security (TLS) protection for the message in transit.

When organizations have established partnerships with third-parties, fully encrypted, transparent email delivery can be provisioned between the two entities' email systems. Each system can be configured to require TLS encryption when sending or receiving messages from the other. This ensures that the messages are delivered over the internet in a manner that prevents their interception.

Whichever encryption technique is implemented, an organization's workforce must be trained to use the technique when transmitting sensitive information. This cybersecurity practice can be integrated into the data protection cybersecurity practices discussed in **Cybersecurity Practice #4: Data Protection and Loss Prevention**. Messages that users fail to encrypt can be automatically encrypted or simply blocked.

1.M.D: Workforce Education

NIST Framework Ref: PR.AT-1

While an organization can *reduce* its susceptibility to phishing attacks, it cannot eliminate the risk. Given that phishing is one of the most common methods of attack and initial compromise, a layered defense strategy is important.

Organizations should implement security awareness programs that provide context around email-based attacks. The challenge presented to security departments is how to deliver concise educational and awareness materials for spotting social engineering or phishing attacks when the workforce's knowledge level does not match the hacker's level of sophistication. For example, it is easy to make a phishing email appear to originate from the company itself, incorporating logos, department names, and management names, but it is difficult to train an organization's entire workforce to detect that fake message.

When implementing cybersecurity training programs, consider some of the key techniques outlined in a 2015 HBR article by Keith Ferrazzi:[35]

- ***Ignite each manager's passion to coach their employees:*** Engage and train the management team. Leverage them to communicate security practices and information to staff in all areas of your organization.
- ***Deal with the short shelf life of learning and development needs:*** Security information changes continuously. Implement continuous and ongoing campaigns to maintain awareness of current trends, issues, and events.
- ***Teach employees to own their career development:*** Customize cybersecurity training to the needs of employees in different positions or units in your organization. Develop training techniques and awareness materials that are relevant to the workforce member's role and access.
- ***Provide flexible learning options:*** Provide options, including on-demand and mobile training solutions, that allow the workforce to schedule and complete training independently.
- ***Serve the learning needs of virtual teams:*** Recognize that many workforce members work remotely and virtually. Training solutions should fit within the work environment of virtual employees.
- ***Build trust in organizational leadership:*** Leaders must be open and transparent; to lead by example. Managers must demonstrate to the workforce that they are fully engaged in security strategy and committed to successful execution of security controls and techniques.

35 Keith Ferrazzi, "7 Ways to Improve Employee Development Programs," Harvard Business Review (Last modified July 31, 2015), https://hbr.org/2015/07/7-ways-to-improve-employee-development-programs.

- ***Match different learning options to different learning styles:*** Effective training accommodates the different learning styles and requirements of workforce members who function in diverse work environments within a single organization. Consider multiple options for conducting each training course to maximize training effectiveness and efficiency.

Organizations should implement multi-faceted training campaigns that engage users to catch phishing and other social engineering attempts through multiple channels. Points to include in a successful training campaign include:

- ***Sender verification:*** Users should examine very carefully the sender of the email message. It is common to spoof an organization's name by changing a simple character, for example, "google.c0m" rather than "google.com." Educate users to be on the lookout for emails where your organization's name appears with a separate email domain, such as "!CME.google.com" rather than "acme.com."
- ***Follow the links:*** Every link in an email message is suspect. Organizations should limit the use of links in corporate messages to those that are necessary. Users should hover the cursor over each link to check the corresponding Uniform Resource Locator (URL) and determine whether it is credible. Specifically, mismatched URLs (i.e., those where the name of the link in the email does not match the corresponding URL) are highly suspect. This may not be effective when URLs are rewritten by a security tool to facilitate malicious URL blocking. This process is described in **1.L.A: Advanced and Next-Generation Tooling** under URL click protection via analytics.
- ***Beware of attachments:*** Though it can be difficult to determine whether an attachment is malicious based on the content of an email message, there are often clues. Be wary of messages that require immediate action, for example, "You must read this right away." Be cautious when receiving attachments from senders with whom you do not regularly correspond. It is important to detect malicious attachments, which may contain malware or exploit scripts that permanently compromise your computer. Avoid enabling macros or running executables to view attachment content.
- ***Suspect content:*** In most cases, hackers entice recipients of email to follow a link or open an attachment. They will use messages to play with the natural curiosity and emotions of those receiving the email. These messages vary widely from urgent messages such as, "Your account will be deactivated unless you re-register," to scary messages such as, "The IRS is suing you and you must fill out the attached form." Hackers also prey on hopes and desires. Examples of these messages include, "You have won a $100 Amazon gift card!" and the well-known "Nigerian Prince" messages.
- ***Avoid acting:*** BEC schemes typically encourage the recipient to take an action (e.g., completing a wire transfer). These messages may impersonate a senior executive or key vendor/supplier. In many cases, they may require a quick action to avoid a penalty, lost deal, etc. In all cases, changes to account numbers, wire transfers, requests to send sensitive information (e.g., W2 data) should be confirmed by verifying the sender based on known contact information—not based on the contact details delivered in the malicious email.

As an organization develops its awareness campaigns, keep this simple goal in mind: empower the user community to be "human sensors". Detection of malicious activity and reporting these incidents to the appropriate cybersecurity personnel is crucial. As the saying goes, "If you see something, say something." The earlier cybersecurity personnel become aware of a phishing attack or social engineering campaign, the faster they can execute **Cybersecurity Practice #8: Security Operations Center and Incident Response**.

The following are recommended channels for cybersecurity awareness campaigns:

- ***Email Click Button:*** Add a button to the email client that allows for automated reporting of a suspicious email. This reporting can be configured to go directly to your organization's cybersecurity department and can increase the likelihood your workforce will report suspect messages. The cybersecurity department should maintain a routine procedure for processing any suspicious emails provided to them. For more specifics, review **Cybersecurity Practice #8: Security Operations Center and Incident Response**.
- ***Monthly phishing campaigns:*** The most effective means of training the workforce to detect a phishing attack is to conduct simulated phishing and social engineering campaigns. The authorized cybersecurity personnel or third-party provider crafts and sends phishing emails to users with email accounts. These emails have embedded tracking components (e.g., to track link clicks). Tracking enables your organization to identify employees who detect the email as a phishing attack and those who fail to detect the attack, opening the email or clicking the emailed links. Your organization can then provide the appropriate training and feedback as soon as possible after the event. Simulated phishing attacks provide a cause-and-effect training opportunity and is incredibly effective. Consider conducting phishing simulations on at least a monthly basis for the entire workforce. Develop specialized simulations for higher-risk areas within your organization. These could be based on the department (such as finance and HR) or on data identifying your highest-risk users. Phishing and social engineering campaigns should track (and potentially reward) users that successfully report the test message.
- ***Ongoing and targeted training:*** Organizations should include phishing content in ongoing privacy and security training. Targeted training should be provided to users that experience a high failure rate when presented with a simulated phishing email. Another group that should be provided specific training includes those "high-value assets" of spear phishing targeted attacks such as leadership, management, and other employees with financial responsibilities.
- ***Departmental meetings:*** Hold departmental meetings to disseminate information on cybersecurity events and trends. Brief presentations or informal conversations provide face-to-face context and build relationships between cybersecurity personnel and your organization's workforce. These relationships encourage a continuous dialogue that elevates the visibility of cybersecurity across your organization.
- ***Email campaigns:*** Deliver a pointed email message or alert about specific attacks. Provide Secure Multipurpose Internet Mail Extensions (S/MIME) or other digital certificates as evidence that these messages are authentic. Remember that attackers will attempt to do the same thing!
- ***Newsletters:*** Working independently or with your organization's marketing department, develop and distribute a cybersecurity newsletter. Produce articles that explain how to catch a phishing attack or social engineering campaign. Better yet, provide an example of an actual phishing email, highlighting the warning signs that might have resulted in identifying the message as a fake, thereby preventing the attack.
- ***Change Leader:*** Appoint a change leader to be responsible for internal organizational collaboration. This change leader should look at the internal culture of your organization to determine if employees feel confident on how, when and what to report as early collaboration and coordination can save time and resources.

Sub-Practices for Large Organizations

1.L.A: Advanced and Next-Generation Tooling

NIST Framework Ref: PR.DS-2, DE.CM-5, DE.CM-7

Many sophisticated solutions exist to help combat the phishing and malware incidents. These solutions are called *advanced threat protection services.* They use threat analytics and real-time response capabilities to provide protection against phishing attacks and malware.

The list below describes some of these tools:

- ***URL click protection via analytics:*** In a modern phishing attack, the hacker will create a web page on the internet for harvesting credentials or delivering malware. Next, the hacker will conduct an email campaign, sending emails with a link to a web page that does not have malicious content. Because the linked page is not malicious, traditional spam and AV protections clear the email for delivery to the user. As soon as the emails are delivered, the hacker will change the linked web page to the newly created malicious web page. This allows the hacker to bypass many traditional email protections and leaves your organization to rely on the user's vigilance and awareness.
  Protection technologies that rely on analytics leverage the ability to re-write links embedded in an email message. The rewritten URLs point to secure portals that apply analytics to determine the maliciousness of the request at the time of the click. Therefore, the message is protected no matter where or when the user clicks the link. Such technologies use the cloud and numerous sensors throughout the install base to check linked sites in real time. They can also block discovered malicious sites ahead of time to inoculate your organization.
  It is important to note that, as URL click protection tools will rewrite URLs embedded in emails, it will be difficult for users to "hover" over the URL and determine if it is a legitimate source.
- ***Attachment sandboxing:*** Another common attack technique is to send attachments with embedded malware, malicious scripts, or other local execution capabilities that compromise vulnerabilities on the endpoint where the attachment is launched. These attachments bypass traditional signature-based malware blocking by using multiple obfuscation techniques that alter the attachment's content to provide a different hashing signature.
  Sandboxing technologies open attachments proactively in virtual environments to determine what behaviors occur after the user opens the attachment. The protection system determines whether a file is malicious based on these behaviors, such as system calls, registry entry creation, file downloading, and others.
- ***Automatic response:*** Another useful technique is to implement mechanisms that automatically rescind or remove email messages categorized as malicious after delivery to a user's mailbox.
  After using the analytics approach described earlier in this section to identify malicious emails, cybersecurity response teams remove these messages from the user's mailbox. This manual process requires identifying the characteristics of the malicious email message, searching your organization's email environments, and deleting messages that match the identified characteristics. This time-consuming process is difficult to run in a 24x7x365 operation and can miss malicious emails or remove legitimate ones by mistake.

As an alternative to costly manual removal, automatic response technologies can identify the signature of a delivered email. When advanced threat tools determine that a previously clean message has become malicious, it can automatically delete that email message from all user mailboxes in your organization. This reduces the labor involved compared with the manual processes and provides the automation consistency.

- ***Imposter Protections:*** Another common tactic by bad actors is to create an email that has the same name as a key leader within your organization, doing so within one of the free email systems such as Gmail, Yahoo, Hotmail, and others. The bad actor will then send very targeted messages to specific members inside your organization (usually initially without any malicious attachments or links), with the goal of engaging in a dialogue and establishing some level of trust with the recipient. Once the trust has been established the bad actor will then ask the recipient to take some type of action on their behalf, such as purchasing one-time gift cards, changing bank account numbers, or even providing user credentials. This is a very common tactic with BEC attacks. To protect against these types of attacks, modern email defense tools can flag VIP users, such as the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operations Officer (COO), or even heads of research, and take special precautions against any inbound messages from personal email accounts with these names. This type of system does require some manual tuning and the ability to understand the VIPs legitimate real personal account (to not create false positives). Such a control can effectively mitigate targeted social engineering attacks.

1.L.B: Digital Signatures

NIST Framework Ref: PR.DS-2, PR.DS-6, PR.DS-8

Digital signatures allow a sender to leverage public/public key cryptography to cryptographically sign an email message. This does not encrypt the message itself. Rather, it validates that a received message is from a verified sender and has not changed in transit.

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

Be careful! Many email protection technologies change the content of email messages (e.g., by tagging subject lines, re-writing URLs). Digital signature technology that maintains the integrity of an email will fail when you use these other protection techniques. Currently, there is no method to resolve this problem.

1.L.C: Analytics-Driven Education

NIST Framework Ref: PR.AT-1

Cybersecurity departments use data and analytics from both regular email protection platforms and advanced threat protection systems to identify the most frequently targeted users in an organization. These users might not be the ones you think are highly susceptible, such as the CEO or the finance workforce. With the systems discussed in this section, SOCs can identify targets, implement increased protections (e.g., lower thresholds for spam/malware checking, delayed processing time for attachments), and provide on-the-spot and targeted education. Informing these individuals of their high-risk profile instills a heightened sense of awareness and increased vigilance. Data on the most successful types of phishing messages can help drive greater awareness on the actual threat your organization faces.

Key Mitigated Threats

1. Social engineering
2. Ransomware attacks
3. Insider, accidental or malicious data loss

Suggested Metrics

- ***Number of malicious phishing attacks prevented on a weekly basis, compared to total email volume.*** The goal is to ensure systems are working. Sudden changes in the rate of phishing attacks should trigger operations to checks to ensure that systems are still operating as intended.
- ***Number of malicious URLs and email attachments discovered and prevented on a weekly basis, compared to total email volume.*** The goal is to measure the effectiveness of advanced tools, like click protection or attachment protection.
- ***Number of phishing attacks that bypassed your prevention systems and detected by end users on a weekly basis.*** This measurement will provide a measurement to determine the effectiveness of your preventative controls and identify room for improvement.
- ***Number of accounts compromised through phishing.*** This is based on users who accessed a malicious website. It assumes that a registered click indicates compromised credentials, so be sure to change the credential before further compromise can occur. Implement education to keep this number as low as possible.
- ***Number of malicious websites visited on a weekly basis.*** The goal is to establish a baseline understanding, then strive for improved awareness through education activities that train employees to avoid malicious websites.
- ***Percentage of users in your organization who are susceptible to phishing attacks based on results of internal phishing campaigns.*** This provides a benchmark to measure improvements to the workforce's level of awareness. The goal is to reduce the percentage as much as possible, realizing that it is nearly impossible to stop all users from opening phishing emails. A secondary goal is to correlate the percentage of susceptible users with the number of malicious websites visited or the number of malicious URLs opened.

- ***Percentage of users who report suspected messages received during a phishing campaign.*** The more users that flag suspicious messages, the greater the chance the SOC will be alerted and able to remove messages that evaded technical controls. This is also can be used as a measure of user awareness.
- ***List of the top 10 targeted users each week, with corresponding activity.*** For example, how many phishing emails do the top three users receive compared with the rest of the workforce? What positions do these users hold in your organization? Are there correlations among the user, the user's position, and the number of phishing emails received? What inferences and conclusions are possible? The goal is to conduct targeted awareness training to these individuals, advising them that they are targets more often than other users, and increasing their vigilance as well as their ability to detect and report phishing attacks.
- ***Average time to detect (mean time to detect) and average time to respond (mean time to respond) statistics for phishing attacks on a weekly basis.*** Time to detect measures how long the phishing attack was in progress before the cybersecurity department was aware of it. Response times measure of how quickly the cybersecurity department neutralized the messages to end the attacks. Ideally, both metrics should be as low as possible. Establish a baseline to understand the current state and set goals to improve performance.
- ***Number of users sent internal campaign, percentage that never opened it, percentage that reported it, and percentage that clicked.*** Of the number that clicked, what is the percentage that attempted to provide credentials or download and run an executable file?

Cybersecurity Practice #2: Endpoint Protection Systems

Endpoints are the assets the workforce uses to interface with an organization's digital ecosystem. Endpoints include desktops, laptops, workstations, and mobile devices. Current cyber-attacks target endpoints as frequently as networks. Implementing baseline security measures on these assets provides a critical layer of threat management. As the modern workforce becomes increasingly mobile, it is essential for these assets to interface and function securely.

Endpoints are not static on a healthcare organization's network. Organizations commonly leverage virtual teams, mobility, and other remote access methods. In some cases, endpoints rarely make it to the corporate network. It is important to build cybersecurity hygiene practices with these characteristics in mind.[36]

Areas of Impact
Passwords, PHI

Medium Sub-Practices
- **2.M.A** Basic Endpoint Controls
- **2.M.B** Mobile Device Management

Large Sub-Practices
- **2.L.A** Automate the Provisioning of Endpoints
- **2.L.B** Host Based Intrusion Detection/Prevention Systems
- **2.L.C** Endpoint Detention Response
- **2.L.D** Application Allowlisting
- **2.L.E** Micro-Segmentation/ Virtualization Strategies

Key Threats Addressed
- Ransomware attacks
- Loss or theft of equipment or data

405(d) Resources
- Prescription Poster: Endpoint Protection Systems

Sub-Practices for Medium-Sized Organizations

2.M.A: Basic Endpoint Protection Controls

NIST Framework Ref: PR.IP-1, PR.IP-12, PR.AC-4, PR.DS-1, DE.CM-4

Table 3 describes basic endpoint controls with practices to implement and maintain them.

Table 3. Basic Endpoint Controls to Mitigate Endpoint Risk

Control	Description	Implementation Specification
Antivirus (AV)	Technology capable of detecting known malicious malware using signatures, heuristics, and other techniques.	• Push out AV packages using endpoint management systems that interface with Windows and Apple operating systems. • Develop metrics to monitor the status of AV engines, signature updates, and health. • Dispatch field services/desktop support for malware that is detected but not automatically mitigated. • Leverage network access control (NAC) to conduct a validation check, prior to enabling network access.

36 "CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers," Center for Information Security Controls (Accessed September 24, 2018). https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/.

Control	Description	Implementation Specification
Full disk encryption	Technology capable of encrypting an entire disk to make it unreadable for unauthorized individuals.	• Ensure encryption is enabled on new endpoints acquired by your organization. • Connect encryption management to endpoint management systems that interface with mobile and traditional operating systems. • Develop metrics to monitor the status of encryption. • Dispatch field services/desktop support teams to resolve encryption errors. • Use anti-theft cable locks to lock down any device that cannot support encryption. • Leverage NAC to conduct a validation check prior to enabling network access. • Maintain audit trails of this encryption in case a device is ever lost or stolen.
Hardened baseline images	Configure the endpoint operating system in the most secure manner possible.	• Enable local firewalls and limit inbound access to the endpoint to only required ports. • Disable weak authentication hashes (e.g., LANMAN, NTML Version 1.0). • Prevent software from auto-running/starting, especially when using any directly connected USB device (e.g., a thumb drive). • Disable unnecessary services and programs. • Permit usage only of known hardware encrypted any directly connected USB device (e.g., a thumb drive) for writing data. • Review and consider the implementation of Security Technical Implementation Guides.[37]
Local administrative rights	The provisioning of privileged access to users for installing or updating application and OS software.	• Limit local administrative rights deployed to endpoints. Use endpoint management systems to install new programs and patch systems. • 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. Doing so increases vulnerability to malware and client-side attacks.

37 "Security Technical Implementation Guides (STIGs)," Information Assurance Support Environment (IASE) (Accessed September 24, 2018), https://public.cyber.mil/stigs/.

Control	Description	Implementation Specification
Patching	A process ensuring regular patching of endpoint OS and third-party applications.	• Establish an endpoint management system which covers mobile and traditional network, desktop and server devices and distribute OS patches during regular maintenance times. • Automatically update and distribute patches to third- party applications that are known to be vulnerable, such as internet browsers (e.g., Adobe Flash, Acrobat Reader, Java). • Develop metrics to monitor patch status. Review on a weekly basis. • Dispatch field services/desktop support for endpoints that fail to patch. • Systems often need to be rebooted before patching takes effect. • Organizations should reference Cybersecurity Practice #9: Network Connected Medical Devices for additional considerations for patching medical device firmware.
End-of-Life (EOL) Management	Operating systems, software and applications no longer supported by the vendor/provider and do not receive product updates and security patches. Use of these products represents a significant risk to your data, information systems, and overall mission. Operating systems, software and applications that are no longer supported by the vendor/ provider should be removed from the environment.	When an operating system, software or application is determined to have reached EOL or will reach EOL within the upcoming year based on vendor notifications and other listings/sources, the risk must be mitigated in one of the following ways: 1. Upgrade, retire or stop the use of an unsupported operating system, software or application immediately by the date specified in the extended support agreement or the announcement by the vendor/provider. 2. When the removal or retirement of an unsupported operating system, software or application is not operationally feasible, the System Owner should attempt to acquire additional support from the vendor. When not feasible, your organization should follow their risk acceptance/policy exception process to document reasonable and appropriate mitigating controls and a timeline for resolving the risk.

Control	Description	Implementation Specification
Tap-n-Go Authentication	Multi-factor, or secondary factor, authentication systems that allow users to log in to their workstations by "tapping" their badge.	Requires the installation of a Tap-n-Go compatible system. Consider the following: 1. Establish institutional Identities, as defined within Cybersecurity Practice #3: Identity and Access Management. 2. Tie an individual's identity to the Tap-n-Go system. 3. Establish a reasonable timeout period (usually less than 15-30 minutes) so the session can be 'locked' after inactivity. 4. Enable session persistence in the Tap-n-Go system, so that when a user taps into a separate endpoint, the session can migrate over in its current state.

Organizations should reference Cybersecurity Practice #5: IT Asset Management to determine whether their endpoints meet IT asset management (ITAM) requirements. Examples include maintaining a proper inventory of endpoints, reimaging endpoints as they are redeployed, and securely removing endpoints from circulation when decommissioned.

When employees leverage personally owned devices (i.e., BYOD) that are not managed by your organization, care should be taken to determine how these practices should be applied. If minimum standards can't be enforced by NAC (or similar mechanisms), a separate segmented network should be provided for personal devices used to access your organization's systems and applications.

Ensure workforce members are trained on the need to report any lost or stolen endpoints to your organization's cybersecurity department.. Reporting should occur promptly so the cybersecurity department can execute the proper incident response (IR) procedures, outlined in Cybersecurity Practice #8: Security Operations Center and Incident Response.

2.M.B: Mobile Device and Mobile Application Management

NIST Framework Ref: PR.AC-3

Mobile devices, such as smartphones and tablets, present their own management challenges. Multiple security configuration options exist for these devices, and organizations should configure the devices consistently to comply with organizational security policies.[38]

Mobile device management (MDM) technologies manage the configuration of devices connected to the MDM system. In addition to configuration management, they may offer application management and containerization. Mobile application management (MAM) solutions are a type of containerization where your organization can control where the application is installed, how it is configured, and aspects of the device's security (e.g., data encryption, biometric authentication). All three elements are important to consider, especially for organizations that allow the use of personal devices in business operations.

38 "CIS Benchmarks," Center for Information Security (Accessed September 24, 2018), https://www.cisecurity.org/cis-benchmarks/.

MAM works best where people may only need access to specific applications and offer flexibility when employees leverage their own devices in a BYOD environment.

Because most mobile devices travel on and off your organization's network, it is important to consider cloud-based MDM systems to enable consistent check-in. If cloud-based systems are not available, then the onsite MDM systems must be accessible over the internet through virtual private network (VPN) connectivity or in your organization's demilitarized zone (DMZ). The list below further outlines the capabilities of MDM systems.

- ***Configuration management:*** At minimum, ensure that passcodes are in place and encryption is enabled. Be sure each device locks automatically after a predefined duration (i.e., one minute). Implement device wipe functions after a series of unsuccessful logins (i.e., 10 unsuccessful logins). Limit the amount of time that an email can reside on the mobile device (i.e., 30 days maximum). Consider leveraging an "Always on VPN" to protect the corporate device when users connect to unsecured wireless networks. Also, consider prohibiting the installation of unsigned applications.
- ***Application management:*** Malicious applications reside in app stores and may appear to be legitimate (e.g., PDF readers, Netflix apps), when they really contain malicious code that provides access to data elsewhere on the mobile device. MDM solutions use allowlisting or denylisting techniques to limit the installation of these malicious applications. Consider both, especially for devices that run on the Android platform (an open platform that accepts a wide range of applications).
- ***Containerization:*** Organizations with BYOD policies should consider containerization technologies, such as MAM. These technologies segment and process business data on a mobile device separately from personal data. Containerized business applications exist only in a hardened container on the mobile device. Examples of such business applications include email, calendaring, and data repositories. Containerization allows your organization to wipe the container and clear business data from the device when the workforce member leaves or changes position in your organization. It also limits the risk that personally downloaded malicious applications will access business data.

Sub-Practices for Large Organizations

2.L.A: Automate the Provisioning of Endpoints

NIST Framework Ref: PR.DS-5

It is challenging to manage thousands of endpoints consistently, especially when endpoint provisioning processes are manually executed. Most organizations do not have the necessary resources to run such an operation.

Value-added resellers (VARs) that sell endpoints through supply chains can preconfigure endpoints before delivering them to an enterprise. To implement preconfiguring, your organization must build a "gold image," with a series of checklists and configuration procedures, and provide it to the VAR. This approach helps to ensure a consistent and resilient deployment of endpoints. The image must be updated periodically so new computers are deployed with the latest patches, agents, and other configurations. There should also be a process for updating systems already deployed so they remain aligned with current standards.

In some cases, vendors provide the ability for an organization to provision devices centrally. For example, Apple provides this service for its devices through its Device Enrollment Program (DEP). The DEP enables an organization to simplify enrollment and endpoint security management. Your organization enters the serial number or order number of the new device in the DEP, initiating a series of device configuration tasks that are specific to your organization's requirements. Further information is available in Apple's DEP Guide.[39]

2.L.B: Host-Based Intrusion Detection and Prevention Systems

NIST Framework Ref: PR.DS-5

Host-based intrusion detection systems (HIDS) and Host-based intrusion prevention systems (HIPS) use a protection method like network-based intrusion detection and prevention systems. These technologies should be deployed on endpoints to detect patterns of attacks launched. Attacks can originate at the endpoint's network, or through client-side attacks that occur when using email or browsing the web.

HIDS and HIPS technologies are usually deployed and managed through central endpoint management systems used to manage endpoint software and patching. Configure them to auto-update against their command servers. The command servers should be configured to regularly download fresh signatures of attack indicators.

2.L.C: Endpoint Detection and Response

NIST Framework Ref: PR.DS-5, RS.AN-1

Endpoint detection and response (EDR) technologies (also known as Advanced Threat Protection or ATP) helps bridge the gap between execution and processing that occurs in an organization's fleet of endpoints. These agent-based technologies utilize the continuous monitoring features provided by anti-virus vendors and augment the data with analytical analysis and rules-based automated response. These new features provide real-time response and mitigation for suspicious running processes, network connections, file actions, and other irregular activities. Most of the major anti-virus vendors have updated their offerings to include these added EDR analytical features and are highly recommended to enable within an organization. Key features include:

- Analysis of newly installed processes and services.
- If malware is installed in your organization's environment, cybersecurity professionals can "reach in and remove" the malware from thousands of devices using a single action.
- Providing cybersecurity departments with forensic and analysis capabilities to search for suspicious activities and supplement IR processes.

To ensure EDR implementation and use success, the following best practices/guidelines have been gathered.

39 "DEP Guide," Apple (Last modified October 2015), https://www.apple.com/business/site/docs/DEP_Guide.pdf.

Have a Plan

Review your current anti-virus solution to understand their EDR capabilities and what is needed to enable the new features. If your current solution does not provide these new capabilities, carefully evaluate which solution best meets your needs and organization. Consider the time for installation and support, whether to use an in-house or managed EDR, how to best prevent threats to your organization, and finally how to respond to threats. Primary components of a successful EDR implementation plan should include:

- ***Endpoint agent deployment:*** Endpoint agents conduct the real-time monitoring and data collection. The data collection should include start/stop of processes, network connections, and data collection. To minimize performance and the number of endpoint agents, it is highly recommended that these features are enabled through your current anti-virus solution. The deployment of these agents should be enforced for all endpoint assets during the build process.
- ***Automated response:*** Using pre-configured rules, EDR can respond to the threats and anomalous behaviors real-time. The automated response can provide the opportunity to alert a SOC, disconnect a user, or quarantine/delete a suspicious file. Initially, the plan should enable the EDR solution to be entered into a 'log-only' or 'notify' configuration. As the product is deployed and gains data on endpoints, the appropriate blocking and real-time automated response rules should be implemented.
- ***Forensic investigation and real-time analysis using analytics:*** Real-time analysis utilizes normal patterns to create a security baseline. Once the baseline has been created, security events can be generated for anomalous patterns as they occur outside the baseline. Forensic investigation tools provide an analyst the capability to research past incidents and activity on the endpoint. Existing IR playbooks should be updated to include these new forensic investigation capabilities. In addition to IR playbooks, the forensic investigation capabilities should be implemented into daily hunting exercise and threat intelligence reviews of indicators of compromise (IOCs).

Train and Educate

As EDR is deployed to endpoints, an appropriate training and education plan should be created for the various roles that may be impacted. A specific training plan should be created for:

- ***Cybersecurity incident responders and hunters:*** EDR provides a vast knowledge of information related to cybersecurity incidents. Develop a training plan for cybersecurity analysts to use the new features to extend investigation to the endpoints. Training should also include IR steps and processes. An understanding of the MITRE ATT&CK® framework will help the analyst to understand the various attack methods and capabilities.[40]
- ***Service or help desk analysts:*** As the agent is deployed to the various endpoints, the device may experience some negative impact to applications or endpoint performance. Service or help desk analysts need to be aware the type of calls that may come into the service desk and the steps to remediate these problems. Additionally, if the endpoint user is notified of a security event, the service desk employee needs to be aware to quickly escalate the call to the appropriate IR team.
- ***Client field services team:*** Endpoint IT support techs need to be aware of the new technologies and how to support reported endpoint errors. They should also be aware of the various IR touchpoints and escalation steps.

40 MITRE ATT&CK® (Accessed May 26, 2022), https://attack.mitre.org/.

Assess All Permissions and Access Codes

Social engineering is still one of the most dangerous threats to enterprise security today. It is important to implement appropriate segregation of duties and rights to maintain the installation and removal of the EDR agent. Configure a password or PIN that must be entered to remove or disable the EDR software. This removal password should not be shared or provided to the endpoint user. This also minimizes the risk to malicious software that will first try to disable the software before infection.

Monitor 24/7

Be sure to integrate the events from the EDR into your security incident and event management (SIEM) and security operation center. Remember to constantly collect and analyze the security data you need. Remember that EDR stands for endpoint detection and response. It involves detecting and responding to threats, which means it must be both *proactive* and *reactive*. Proactive EDR is focused on finding and preventing attacks before they happen. Alternatively, if an attacker *does* get into your network, it's time for reactive EDR.

Use EDR as a Complement

Using EDR as a complement to other security applications strengthens the overall protection of your organization to an attack. Numerous network security services and vendors exist today. EDR security is a tool to enhance your enterprise's defenses, but it's not the only thing you need. Make sure you have a full lineup of network security features, including AV, firewalls, patch management, and others.

2.L.D: Application Allowlisting

NIST Framework Ref: ID.AM-2, PR.DS-6

Application allowlisting technologies permit only applications that are known and authorized to run, rather than identifying applications that not permitted to run. These technologies assume it is impossible to identify and denylist (or block) every malicious application, so all applications are blocked except those that are allowlisted. In concept, this is application-level zero trust.

Application allowlisting can be based on a variety of application file and folder attributes, including the following:

- ***File path:*** This is the most general attribute to permit all applications contained within a particular path (directory/folder). Used by itself, this is a very weak attribute, because it allows any malicious files placed within the directory to be executed. However, this attribute becomes stronger if the path is protected by strict access controls that only allow authorized administrators to add or modify files. Paths can be beneficial by not requiring each file within the path to be listed separately, which reduces the need to update the allowlist for every new application and patch.
- ***Filename:*** The name of an application file is too general to be used on its own. If a file were to become infected or be replaced, its name would be unchanged so the file would still be executed under the allowlist. Also, an attacker could simply place a malicious file onto a host and use the same name as a common benign file. Because of these weaknesses, this attribute should not be used on its own; rather, it should be paired with other attributes. For example, it would be stronger to combine path and filename attributes with strict access controls or to combine a filename attribute with a digital signature attribute (described below).

- ***File size:*** This is typically only used in combination with other attributes, such as filename. Monitoring the file size assumes that a malicious version of an application would have a different file size than the original; however, attackers can craft malicious files to have the same length as their benign counterparts. Other attributes, such as digital signature and cryptographic hash, provide substantially better unique identification of files than file size does, and should be used instead of file size whenever feasible.
- ***Digital signature or publisher:*** Publishers are digitally signing their application files more frequently than ever. A digital signature provides a reliable, unique value for an application file that is verified by the recipient to ensure that the file is legitimate and has not been altered. Unfortunately, many application files are not yet signed by their publishers, so using only publisher-provided digital signatures as attributes is generally not feasible. Some application allowlists can be based on verifying the publisher's identity instead of verifying individual digital signatures. This assumes that all applications from trusted publishers can themselves be trusted. This assumption may be faulty if the software vendor has multiple applications, and your organization wants to restrict which of those applications can be executed. Also, relying on the publisher's verified identity might only allow older software versions with known vulnerabilities to be executed. However, the benefit of basing an allowlist on publisher identities is that the allowlist only needs updates when there is a new publisher (i.e., software vendor) or when a publisher updates its signature key.
- ***Cryptographic hash:*** A cryptographic hash provides a reliable, unique value for an application file, so long as the cryptography being used is strong and the hash is already known to be associated with a good file. Cryptographic hashes are accurate no matter where the file is placed, what it is named, or how it is signed. However, a cryptographic hash is not helpful when a file is updated, such as when an application is patched; the patched version will have a different hash. In these cases, the patch should be identified as legitimate through its digital signature first; then, its cryptographic hash should be added to the allowlist. It is important to note that if the allowlist is not continuously updated with new hashes for new and updated applications, there is a significant risk of software not functioning correctly. Further, if the allowlist is not continuously updated to remove existing hashes for older software versions with known vulnerabilities, there is a significant risk of vulnerable software being allowed to run.

Choosing attributes is largely a matter of achieving the right balance of security, maintainability, and usability. Simpler attributes such as file path, filename, and file size should not be used by themselves unless there are strict access controls in place to tightly restrict file activity. Even then, there are often significant benefits to pairing them with other attributes. A combination of digital signature/publisher and cryptographic hash techniques generally provides the most accurate and comprehensive application allowlisting capability, but usability and maintainability requirements can put significant burdens on your organization.

Application allowlisting is most often associated with monitoring executables. However, most application allowlisting technologies can also monitor at least a few other types of application-related files, such as libraries, scripts, macros, browser plug-ins (or add-ons or extensions), configuration files, and application-related registry entries (on Windows hosts)."[41]

41 Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, *NIST Special Publication 800-167: Guide to Application Whitelisting*, National Institutes of Science and Technology (NIST) (October 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

Initial implementation of application allowlisting may have major impacts to organizations as they try to identify the multitude of executables used for approved applications. A clear plan should be created to minimize operational impact. The plan should include:

- ***Audit mode:*** When deploying a solution, first implement the software in audit mode. This will provide a log of executables outside of the current approved list. Review the list to determine if any executable should be added to the approved list.
- ***Enforcement mode:*** Once the solution has run for an appropriate time and the audit list has been reviewed, update the solution to run in enforcement mode. This will begin to block the non-approved executables from running.
- ***Support and tuning:*** After the solution has been implemented in enforcement mode, new applications will be purchased and existing applications will be upgraded. Support and tuning needs to be integrated into the application management lifecycle. Implement a plan to review new requests; ensure this includes a process to review urgent requests, minimizing operational impact.

Organizations should maintain a current inventory of all software on endpoints to facilitate complete and consistent maintenance and patching to protect against client-side attacks.[42]

When examining solutions, organizations should consider choosing machine-level (PC/servers) or network-level application allowlisting, or both. Configuration of application allowlisting is complex and outside of the scope of this document. This activity should be done in conjunction with reviewing administrative rights to endpoints.

2.L.E: Micro-Segmentation/Virtualization Strategies

NIST Framework Ref: PR.AC-5

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

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

Key Mitigated Threats

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

42 "CIS Control 2: Inventory of Authorized and Unauthorized Software," Center for Internet Security Controls (Accessed September 24, 2018), https://www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-software/.

Suggested Metrics

- ***Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly.*** The first goal is to achieve a high percentage of encryption, over 99 percent. Achieving 100 percent encryption is nearly impossible because process defects always exist. Additionally, the percentage of endpoints encrypted will vary as you discover new assets, which is why it should be measured at least weekly.
- ***Percentage of endpoints that meet all patch requirements, measured monthly.*** The first goal is to achieve a high percentage of success. Secondary goals are to ensure that there are practices to patch endpoints for third-party and OS-level application vulnerabilities, and to be able to determine the effectiveness of those patches. Without this metric, there might not be checks and balances in place to ensure satisfactory compliance with expectations. Rather than use the software distribution technology for measurement, a secondary solution like a vulnerability scanner could be leveraged to measure patch effectiveness.
- ***Percentage of endpoints with active threats, measured weekly.*** The goal is to ensure that practices are in place to respond to AV alerts that are not automatically quarantined or protected. Such alerts indicate that there could be active malicious action on an endpoint. An endpoint with an active threat should be reimaged using genersal IT practices and managed using a ticketing system if forensics/ additional diligence is not required.
- ***Percentage of endpoints that run non-hardened images, measured monthly.*** The goal is to check assets for compliance with the full set of IT management practices, identifying assets that do not comply. To do this, place a key or token on the asset indicating that it is managed through a corporate image. Separate practices are necessary for assets that are not managed this way to ensure that they are properly hardened and patched.
- ***Number active endpoints with EOL issues or reaching EOL within the next 12 months.*** The goal is to bring visibility to any ongoing or upcoming EOL concerns to assist in timely responses and resolutions. To accomplish this, the asset management process is used to flag assets running EOL software and use automated scans periodically to identify new or existing EOL. Separate practices are necessary for assets that are not managed this way to ensure that they are properly decommissioned.
- ***Percentage of local user accounts with administrative access, measured weekly.*** The goal is to keep this number as low as possible, granting exceptions only to local user accounts that require such access.

Cybersecurity Practice #3: Identity and Access Management

Areas of Impact
Passwords

Medium Sub-Practices
3.M.A Identity
3.M.B Provisioning, Transfers, and Deprovisioning Procedures
3.M.C Authentication
3.M.D Multi-Factor Authentication for Remote Access

Large Sub-Practices
3.L.A Federated Identity Management
3.L.B Authorization
3.L.C Access Governance
3.L.D Single Sign-On

Key Threats Addressed
- Ransomware attacks
- Insider, accidental or malicious data loss
- Loss or theft of equipment or data

405(d) Resources
- Prescription Poster: Identity and Access Management

Identity and access management (IAM) is a program that encompasses the processes, people, technologies, and practices relating to granting, revoking, and managing user access. Given the complexities associated with healthcare environments, IAM models are critical for limiting the security vulnerabilities that can expose organizations. A common phrase used to describe these programs is "enabling the right individuals to access the right resources at the right time."

Most access authentication methods rely on usernames and passwords, a model proven to be weak by the success of phishing and hacking attacks. Establishing IAM controls requires a distinct and dedicated program to accommodate its high level of complexity and numerous points of integration. You can find a toolkit for establishing an IAM program on the EDUCAUSE website.[43]

This section will focus on the critical elements of an IAM program required to manage threats relevant to the HPH sector.

Sub-Practices for Medium-Sized Organizations

3.M.A: Identity

NIST Framework Ref: PR.AC-1

As defined in NIST Special Publication 800-63-3, "Digital identity is the unique representation of a subject engaged in an online transaction."[44] A common principle to follow is "one person, one identity, multiple contexts." In healthcare, a person can have the context of a patient, payor, or even employee of the health system. For clinical staff, one person can have one identity, but that person's ability to practice specialties will depend on context. This includes the country, practice area, or hospitals where the person has a business or employee relationship.

Within the United States, each worker is provided with a unique SSN. Similarly, a person who joins an organization should be given a unique identifier. That unique identifier should not be used as a secret authenticator, the way a person's SSN is often used. The unique identifier is not the authenticator.

43 Erik Decker, et al., "Toolkit for Developing and Identity and Access Management (IAM) Program," EDUCAUSE (May 7, 2013), https://library.educause.edu/resources/2013/5/toolkit-for-developing-an-identity-and-access-management-iam-program.

44 Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *NIST Special Publication 800-63: Digital Identity Guidelines*, NIST (June 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.

Establish each person's identity through onboarding systems of record. The most common of these systems is the ERP or HR system. When onboarding new employees in your organization, HR business processes identify and establish the new employee in your organization. Onboarding involves many processes, such as background checks, employment verification, and payroll preparation. They provide solid identity proofing used to verify the employee's identity in the future. They trigger the generation of the employee's new digital identity. These identity-proofing practices respond to the need to understand a person's relationship and context within your organization. Therefore, it is imperative that IAM programs and functions align with HR practices and business processes. Identities maintain a series of attributes that describe the common user elements. The series of attributes comes from the system of record, whether that is an HR, contingent workforce, medical staffing office, or other system in your organization's ecosystem. Examples of common elements include a person's name, location, telephone number, email address, job title/job code, and specialization/practice data.

The system of record transmits attributes to the IAM system, enriching the identity data and facilitating the flow of information to systems for login, access management, and other cybersecurity- and business-related functions. In addition to common descriptive attributes, there may be other system-defined attributes (e.g., roles or affiliations used to describe populations of individuals: clinician, staff, staff nurse, visitor, student). Organizations can leverage both types of attributes for future authorization components. For example, you can use attributes to authorize eligibility for various systems (using a technique called attribute-based access control [ABAC]).

Users defined under proper identity management processes will include more than your employees. These processes should account for volunteers, locums, contractors, students, visiting scholars, visiting nurses, physician groups staff, billing vendors, visiting residents, organ procurement organizations, special statuses (such as emeritus professors), and third-party vendors that require access to provide services to your organization. Each identity type must have an approved channel to serve as the system of record, where the identity proofing activities will occur. Care should be taken to manage non-employees throughout their lifecycle since changes to their role and departure may not be as obvious as it is for employees. Additionally, since a person can be an employee and non-employee (e.g., nursing technician, nursing student, and volunteer) it is important to have the right contexts assigned to the individual based on their roles. Ultimately, there should be an employed sponsor accountable for all non-employee accounts.

This identity information can be stored in a single repository, enabling its consumption for other purposes. IAM systems, in principle, are an aggregate of system of record data. IAM systems should be a system of last resort when none exists (e.g., contingent workforce if HR/business does not have a solution). At a minimum, follow these basic principles:

- ***Enumerate all authorized sources of identity.*** These sources are often referred to as the systems of record. Examples include HR systems, vendor management systems, contingent workforce systems, medical staffing offices or practice offices, and student information systems. Ensure that all users receive a unique identity and identifier. Smaller organizations without multiple constituents may consider using the employee ID number from the system of record. Larger organizations with many constituents should establish a unique identifier for each user and reconcile. *Do not use SSNs as unique identifiers.* An individual with multiple contexts should have one user record with one unique identifier that ties to all contexts.

- ***Maintain the integrity and uniqueness of digital identities.*** Never reuse identities for different people. People come and go throughout the life of an organization. Maintain their records perpetually.
- ***Proper identity management enables the automation of functions such as system access and authentication.*** Enumerate and establish attributes, which are critical to provide context to the identity and required for access and authentication controls. For complex and large organizations, this is an important principle to ensure the consistent application of attributes. For example, it enables automated authentication and authorization through automated provisioning and deprovisioning.
- ***Store identity information in a database or directory capable of registering identity information and associated attributes.*** Such databases aggregate systems of record data. Consider specialized tools for organizations with multiple constituent types.
- ***Use a single namespace to establish user accounts.*** Tie these user accounts back to the identity so that you can always trace individuals to their digital identities.

3.M.B: Provisioning, Transfers and Deprovisioning Procedures

NIST Framework Ref: PR.AC-4

After you establish digital identities and user accounts, you must provision users with access to information systems prior to using them. It is important to ensure that provisioning processes follow organizational policies and principles, especially in the healthcare environment.

The HIPAA Privacy Rule's minimum necessary standard requires organizations to implement procedures that limit uses, disclosures, or requests of PHI to the minimum amount of data required to accomplish the intended purpose. This same principle applies to reducing the attack surface of potentially compromised user accounts. By limiting access, you can limit the scope of a ransomware outbreak or data attack.

Follow these principles for provisioning:

- ***Identify common systems that users need to access, and the least level of access required for each of those systems.*** These common systems are referred to as birthright entitlements.
- ***Define birthright entitlements in organizational policies, procedures, or standards.*** Documentation should exist that describes the access rights that all users receive.
- ***Establish procedures and workflows that ensure consistent provisioning of birthright entitlements.*** Consider employing specialized tools to automate this process for accuracy and reliability. Do not automate bad or unknown workflows.
- ***Establish procedures and workflows that enable provisioning of required access in addition to birthright entitlements, such as access to auxiliary or ancillary systems.*** Pay special attention to cloud-based systems. Consider leveraging federated access management tools that automatically provision access in the cloud.
- ***Consider a two-part process that allows users to request access but requires a second individual to approve the request prior to granting access.*** A common approach is to designate an employee's supervisor as the approving party. A secondary approval may be required for access to these sensitive systems. The secondary approval can come from the executive owner of the data, or their delegate.

Leverage IT ticketing systems by building the provisioning workflow into the ticketing system. This establishes consistency in the approval processes, automates the requesting and granting of approval, and documents the granting of access. It is important to ensure access provisioning processes are auditable.

It is just as important to deprovision access in a timely manner as it is to enable the access when the users request it. Unfortunately, unless deprovisioning processes are automated, it is likely that disabling access might be missed, especially inside of a larger organization. As much as possible, it is recommended to tie your key applications into a standard Single Sign-On platform, then deprovision access in an automated manner once the termination request is conducted. This ensures that when the termination is processed by HR, the user access will be promptly terminated. Follow these principles for deprovisioning:

- ***Establish procedures to terminate access to user accounts.*** Execute these procedures promptly at the time of termination. Consider leveraging tools that automate this process after receiving notification of termination from the system of record. The system of record is usually the HR system, although other systems may trigger access termination.
- ***Ensure that your termination process, whether manual or automated, includes session termination steps to prevent active sessions from remaining active.*** An example of this would be an email login on a mobile phone remaining active after the employee leaves your organization.
- ***Establish an "urgent termination" process outside of the normal termination procedures.*** Use urgent termination in cases of sensitive termination, such as an involuntary termination.
- ***Ensure that termination procedures include both critical business systems and ancillary or auxiliary systems.*** Pay special attention to cloud-based systems that are accessible outside of your organization's standard network. These assets will remain accessible to the user if the deprovisioning process is not completed, or if the system is not connected to an organization's single sign-on system. Consider using federated access management tools to deprovision access to cloud-based systems automatically.
- ***Build automatic timeouts for nonuse in critical systems.*** These timeouts can catch edge cases where deprovisioning procedures are not executed, ultimately reducing the exposure to unauthorized access.

Removal of access should occur when users terminate their relationships with your organization and when users transfer to new functions in your organization. For example, if a patient care services (PCS) manager transfers to the nursing department, access granted when the user was a PCS manager should be removed prior to granting access required by the user as a nurse. This helps to prevent users from accumulating unnecessary access rights.

3.M.C: Authentication

NIST Framework Ref: PR.AC-7

User accounts must engage in authentication to properly assert the user's identity in the digital ecosystem. The most common and, unfortunately, weakest method for authentication relies on password credentials. Nevertheless, password-based authentication systems will continue to exist for the foreseeable future, and organizations should develop solid password authentication practices. Examples of such practices are:

- ***Centralized authentication:*** Use central authentication systems, such as Lightweight Directory Access Protocol directories or Active Directory, to the greatest extent possible. Tying authentication mechanisms back to these central systems enables enterprise management of credentials. You can manage the access rights of your user base from a single location. This is incredibly important when access needs to be deprovisioned in a timely and automated manner.
  Passwords are the most common credential used to authenticate users. The strength and management of passwords are paramount. Strong passwords combat brute force or password guessing attacks. Assuming you can limit the exposure to brute force and guessing attacks, NIST recommends the following techniques as part of NIST Special Publication 800-63:[45]
  - Limit the rate at which authentication attempts can occur. Spacing out each password attempt by a second or two severely limits the ability of automated systems to brute force the password.
  - Ensure the use of cryptographically strong hashing and salting for password storage.
  - Use passphrases in place of passwords. Require a minimum of eight characters and permit up to 64 characters, as well all printable ASCII characters and spaces.
  - Implement dictionary-based password checking and compromised password denylists. Prohibit users from establishing risky passwords, such as those used in previous breaches, repetitive or sequential characters, or context-specific words (such as a name of a service, username, or derivatives thereof).
- ***Privileged account management:*** Centralized authentication should be used for both general user access and privileged administrative accounts. Additionally, you should separate privileged administrative accounts from general user accounts. For example, provision an IT administrator at least two accounts: an account for use completing day-to-day activities and a separate administrative account with access only to systems required by the IT administration function. This second step is critical; the use of privileged accounts during normal day-to-day business may expose these accounts to malware attacks, giving an attacker elevated access to your organization's environment. Limit this exposure as much as possible. Consider the following controls for managing your privileged accounts:
  - Ensure that the passwords set for service accounts are large and complex (at least 32 characters, preferably 64).
  - Rotate these passwords on a frequency you define and require that the passwords are changed if ever compromised.
  - Escrow privileged systems credentials, making them unique for each system or device.
  - Link privileged access to problem, change, or service tickets in your organization's ticketing system.
- ***Require the use of a jump server when elevating privileges.*** Ensure full recording and auditing of the jump server.
- ***Require brokered access to a privileged account.*** This should register which user is using the privileged account and record all actions taken.
- ***Require MFA for all privileged accounts used interactively.*** Strong consideration should be made for the use of hardware tokens, such as a Yubikey, when using MFA for privileged accounts.

45 Paul A. Grassi et al., *NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST (June 2017), https://pages.nist.gov/800-63-3/sp800-63b.html.

- ***Conduct regular reviews of privileged access.***
- ***Limit actions that privileged accounts can take by using access control lists.*** Check for the use of sensitive commands and alert the IT or Cybersecurity departments if there is misuse.
- ***For further details on how to securely configure privileged access, consider the following resources:***
  - For Windows, see Microsoft's article "Implementing Least-Privilege Administrative Models."[46]
  - For Linux, see Redhat's article "Controlling Root Access."[47]
- ***Local application authentication:*** There may be cases where applications do not support a centralized authentication model. Although there are increasingly fewer onsite systems that cannot bind to centralized authentication systems, these systems are still prevalent in the healthcare environment. As organizations migrate applications to the cloud, it is easy to accidentally instantiate a cloud-based service that lacks robust authentication and focuses on local user accounts.
  Whenever you use systems with local authentication, you must maintain solid access control procedures to manage user accounts. This requires designating a responsible IT owner who will manage and regularly review these accounts. Failure to do this allows users access to systems for longer than necessary and is especially risky when an employee leaves your organization and continues to have access to these systems. Consider implementing these extra controls:
  - Designate an IT owner for each legacy/cloud-based system.
  - Establish a distribution list in your organization which includes your IT owners as members. Submit terminations out to these IT owners as they occur.
  - Ensure that IT owners comply with standard operating procedures for the onboarding, review and, most importantly, termination of users.
  - Regularly audit compliance with these manual processes. Ensure compliance with regular account review and termination procedures.
  - Monitor authentication attempts: Monitor both regular and privileged user accounts for security and compliance purposes. Details are discussed further in **Cybersecurity Practice #8: Security Operations Center and Incident Response**.

It is recommended to align authentication practices against NIST's 800-63 Special Publication Series (SP 800-63). Specifically, within SP 800-63-B, three levels of authenticator assurances have been established.[48] These levels can be applied based upon the sensitivity of the systems being accessed. The higher the level of authentication assurance, the more sophisticated a bad actor will need to be to bypass or circumvent these processes.

The 800-63B standard defines very specific authentication requirements. Below is a summary of these for reference purposes. Detailed requirements should be referenced directly from NIST rather than this publication.

46 Bill Mathers et al., "Implementing Least-Privilege Administrative Models," Microsoft Windows IT Pro Center (Last modified May 31, 2017), https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

47 "Controlling Root Access," Redhat Customer Portal (Accessed September 24, 2018), https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-controlling_root_access.

48 Paul A. Grassi et al., *NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

Authenticator Assurance Level (AAL1): Single factor authentication

1. ***Types of authenticators:*** Username/Password, one-time password (OTP)
2. ***Reauthentication:*** Once every 30 days, regardless of user activity
3. ***Identity Proofing:*** Meets low-impact systems defined in SP 800-53.

Authenticator Assurance Level 2 (AAL2): High confidence of authentication requiring two different authentication factors (multi-factor).

1. ***Types of authenticators:*** MFA (OTP, cryptographic), Username/Password + Single-Factor (OTP, Cryptographic): If deployed via mobile phone the unlocking of a phone is NOT considered an authentication factor.
2. ***Reauthentication:*** Once every 12 hours during extended sessions, once every 30 minutes for inactivity. Can prompt user to cause activity prior to timeout.
3. ***Identity Proofing:*** Meets moderate-impact systems defined in SP 800-53.

Authenticator Assurance Level 3 (AAL3): Very high confidence of authentication through hardware-based and cryptographic protocols.

1. ***Types of authenticators:*** Single-Factor Crypto HW + Username/Password, MFA OTP + Single-Factor Crypto HW/SW, Single-Factor HW + MFA SW, Single-Factor HW + Single-Factor SW + Username/Password.
2. ***Reauthentication:*** Once every 12 hours during extended sessions, once every 15 minutes for inactivity. Can prompt user to cause activity prior to timeout.
3. ***Identity Proofing:*** Meets high-impact systems defined in SP 800-53.

3.M.D: Multifactor Authentication

NIST Framework Ref: PR.AC-3, PR.AC-7

MFA systems require the use of several authentication methods to verify a user's identity. According to the common description, MFA systems use at least two of the following: something you know, something you have, and something you are. Users must correctly address at least two of these three categories before the system will verify their identities and allow access.

The most common MFA techniques use smartphone applications and deliver either push notifications to the phone or provide a one-time-code from the application that can be entered into the system being authenticated to. Other examples include printing out one-time-codes ahead of time, use of hardware tokens, or delivering one-time-codes through SMS messages. Another example is using biometrics as a MFA technique. In all cases, the second factor is delivered to the user out-of-band from the authentication technique. For example, most banks have MFA capabilities, which require the customer to enter a password (something you know) followed by a verification code that is texted to the customer's smart phone (something you have).

MFA should be implemented on remote-access technologies to limit the value of password credentials that could be compromised through phishing or malware attacks. MFA is an incredibly impactful method for limiting an attacker's ability to compromise your organization's environment. Consider implementing MFA on the following types of technologies:

- ***VPNs:*** These allow remote network access to your environment. VPNs should be configured to limit user access based on role-based access control (RBAC) or ABAC rules and to enable MFA.
- ***Virtual desktop environments:*** These are environments where virtual terminal sessions can be exposed to remote access, allowing your employees to work remotely. Although highly useful for workforce flexibility, virtual desktop environments systems can be compromised easily if they lack MFA authentication.
- ***Email access:*** If your organization permits email access, MFA should be enabled to limit the risk of compromised credential access in the email system. It is common for healthcare environments to store PHI with these systems, and this exposure could result in a breach of sensitive information, especially if MFA is not used. Take special precautions on the use of legacy email protocols, such as IMAP and POP3, as these are not always compatible with MFA. For more details see **Cybersecurity Practice #1: Email Protection Systems**.

One must also consider MFA techniques for hosted, or cloud-based systems. Internet accessible applications (cloud or hosted on-premise) that allow access to sensitive information (e.g., payroll, electronic medical records) should leverage MFA for authentication. To help organizations adopt MFA to cloud based systems, tie MFA technologies into your single sign-on (SSO) platform. This way, any time you deploy a new SSO implementation, you automatically get MFA added to it at no extra charge.

Sub-Practices for Large Organizations

3.L.A: Federated Identity Management

NIST Framework Ref: PR.AC-6

Federated identity management enables identity information to be shared between organizations in a trusted manner. This allows identities from home institutions (e.g., individual clinics) to be used across a greater ecosystem (e.g., the entire health network). In healthcare organizations, it is common for providers, payors, and other affiliates to work together in an integrated manner. In large complex environments, multiple organizations operate jointly, with different HR practices inside each organization.

Rather than creating identities in each organization of a joint operation, federated identity management tools and processes allow the identity assertions of the home institutions to be used throughout the federation.

Consider the following example: a clinician is part of a practice group that is credentialed within a regional hospital. From the hospital's perspective, this clinician is not an employee but must be credentialed with access to the electronic medical record (EMR). From the practice group's perspective, this clinician has been onboarded through standard HR background checks and processes. If the practice group and the hospital were operating within a federation, the clinician's "home" identity could be established from the practice group and asserted to the hospital as part of the clearance processes. If the clinician's relationship with the practice group were to change, this identity information would be revoked within the hospital based upon assertions from the federation. These processes would be completely automated.

The same model can be leveraged when working with third-party vendors that provide workforce support or staff-augmentation capabilities. In this case, the third-party is the "home institution" that requires

access to resources in your organization. To monitor the activities of each of those workforce members would involve a highly complicated and largely manual process unlikely to be effective. A federation can solve this problem.

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

3.L.B: Authorization

NIST Framework Ref: PR.AC-6, PR.AC-4

After authentication has occurred, the mechanism to obtain specific access to an information resource, such as an application system, is referred to as authorization. Authorization processes check the level of access that has been granted to a user credential and ensures that the credential can access only preauthorized areas. Consider the analogy of traveling at the airport. When you pass through the security lines, your identity is authenticated using your ID card or passport, and you are then authorized to access the terminals based on a ticket for a flight. You are not permitted to access any other flight than the one authorized on your ticket.

Access authorization controls support the HIPAA Privacy Rule's minimum necessary standard to limit the use, disclosure or request of PHI to the least amount of data to accomplish the intended purpose. In addition to HIPAA compliance, minimum necessary is a leading practice to limit malicious use of credentials. In most cases, when hackers break into systems, they are trying to access the "keys to the kingdom" or privileged access credentials that permit access to the most sensitive resources. **Do not risk unauthorized access by granting more access than necessary to your users.**

Consider adding the following controls to limit authorization to only those components required by the user:

- ***Role-based access control (RBAC):*** Conduct a high-level role-mining exercise to map out the role types that exist within your organization and the access they require. For example, identify access requirements for clinicians, support staff, unit secretaries, switchboard operators, case managers, and others. For example, the clinician may need access to the medical record (though not necessarily the entire medical record), whereas the support staff may not need access at all. By defining the unique requirements for these two roles, you have begun to differentiate access models. It can be difficult to provision granular authorization models based on users' roles. In healthcare, two individuals might have the same job title and role, yet completely different tasks within your organization. Relying solely on a person's role to grant access could thus limit the ability for users to fulfill other authorized responsibilities.
- ***Attribute-based access control (ABAC):*** Attribute-based authentication models consider the attributes associated with a user's identity, the attributes of the information system being accessed, and the context associated with the access request. In this model, a user may, for example, be granted an attribute that enables the user to access a specialized function within an information system, but only during business hours or only while onsite. When the user requests access, ABAC systems check the actual context against the access requirements to determine whether access should be granted.[49]

49 "Attribute Based Access Control," NIST Computer Security Resource Center (Last updated February 13, 2013), https://csrc.nist.gov/Projects/Attribute-Based-Access-Control.

This highly effective model limits access based on user-specific rules established in the ABAC systems that define access parameters. As an example, a request is made to grant all nurses with access to all patients on a specific floor in a specific hospital to support flexible care requirements. You might be concerned that this access is excessive because a nurse might not be part of a care team for a particular patient. To reduce the risk to data, you can leverage ABAC, limiting access to times when the nurse is physically present at a specific hospital and ensuring that access is granted only after the nurse has been authenticated using both a password and MFA. The ABAC access credentials cannot be used to grant remote access to the same patients or to grant access anywhere else within the healthcare system. In this model, even a hacker with access to the password and the MFA answer would be unable to access patients using those credentials.

3.L.C: Access Governance

NIST Framework Ref: PR.AC-4

When a user joins your organization, the onboarding processes generate a lot of access request activities. Once access is established for a user, it can be a challenge to determine, at a given future time, whether that access continues to be required. Consider an employee who has worked for your organization for many years, serving in multiple capacities, and has been placed on special projects across your organization. Over time, this employee might accumulate more access than was ever intended.

Conducting a manual review of each employee's access to each of an organization's critical application systems would be nearly impossible. Fortunately, specialized tools are available that enable an organization's leadership to review system access in an automated, self-service capacity. These tools are generally referred to as access governance tools. Below are the relevant components:

- ***Tooling:*** Specialized tools bind to identity management systems and connect to critical business systems to understand the access in place for all users in these systems. These tools require the ability to connect with and parse through specific aspects of the applications in question, such as EMR systems, revenue cycle systems, imaging systems, lab systems, and more.
- ***Segregation of duties:*** Within access governance tools, specialized rules can be defined based on roles or user attributes. For example, a financial system must define roles so that a clinician does not have access to revenue cycle management functions. No employee should be capable of access with both roles. Otherwise, a fraudulent purchase order could be generated, and the invoice paid by the same person, resulting in a fraud loss to your organization. Understanding the characteristics and requirements of these critical roles enables you to create automated alerts that control user access. In addition to the standard segregation of duties checks, some specialized tools compare access profiles of certain users in a role to identify outliers. For example, these tools can assess the usual pattern of access granted to nurses across multiple systems. This pattern can then be set as a baseline of access, and the tool can compare each user against that baseline. If a specific nurse is determined to have excessive access, the user can be reviewed for appropriate adjustments.
- ***Access review:*** Through workflows established with these advanced tools, supervisors within your organization can review the access that their employees currently have in critical environments. This can be done on a regular schedule established by policy. In the case where an employee has retained access that is no longer necessary, the manager can use self-service portals to identify these access violations and flag them for removal. In automated systems, once a manager flags an access for

removal, it be configured to be automatically stripped.
At the end of an access review, the manager can certify that the review is accurate. This documentation is useful for audit practices and to demonstrate effective reviews.

3.L.D: Single Sign-On (SSO)

NIST Framework Ref: PR.AC-7

Federated Single Sign-On (SSO) is an effective method to authenticate users against centralized credential repositories. SSO techniques abstract authentication principles away from the general Microsoft- or Linux-based methods into a generalized standard that can be implemented across platforms. SSO involves securely conducting a general authentication process and passing additional identity attribute information to the specific authorization processes in the resources being accessed. It also has the benefit of requiring only one login while an active SSO session is enabled, eliminating annoying password prompts.

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

A healthcare specific SSO model leverages a second authentication factor at clinical workstations for easy access within a healthcare provider space. These systems can be configured to require a user to authenticate once per day or per shift at a clinical workstation, after accessing the larger clinical setting, using a password and key card/access badge. Subsequent authentications are conducted by tapping the key card to provide secure, easy access to the clinical workstations. These systems provide MFA within the clinical environment while easing the password authentication processes.

Key Mitigated Threats

1. Ransomware attacks
2. Insider, accidental or malicious data loss
3. Attacks against network connected medical devices that can affect patient safety

Suggested Metrics

- ***Number of alerts generated for excessive access to common systems, measured weekly.*** For example, "allow any" permissions to core applications, SharePoint, file systems, etc.
- ***Number of users with privileged access, measured monthly.*** The primary goal is to establish a baseline of the normal number of privileged accounts and monitor variances from the sbaseline.
- ***Number of automated terminations, measured weekly.*** The goal is to establish a baseline for normal terminations and monitor variances from that baseline. A decrease in the number of terminations can indicate that the automated systems are not terminating access properly.
- ***Number of elevated privileged access requests, measured weekly.*** The goal is to establish a baseline to determine how much privileged access is granted over a one-week period and monitor variances from that baseline.

Cybersecurity Practice #4: Data Protection and Loss Prevention

Areas of Impact
Passwords, PHI

Medium Sub-Practices
4.M.A Classification of Data
4.M.B Data Use Procedures
4.M.C Data Security
4.M.D Backup Strategies
4.M.E Data Loss Prevention

Large Sub-Practices
4.L.A Advanced Data Loss Prevention
4.L.B Mapping of Data Flows

Key Threats Addressed
- Ransomware attacks
- Insider, accidental or malicious data loss
- Loss or theft of equipment or data

405(d) Resources
- Prescription Poster: Data Protection and Loss Prevention

All organizations within the HPH sector access, process, and transmit sensitive information, including PHI or other personally identifiable information (PII). The data used in operations are highly sensitive, representing a unique challenge to the HPH sector. It is common for the healthcare workforce to leverage this type of data to carry out their respective missions.

In that context, healthcare faces a growing challenge of understanding where data assets exist, how they are used, and how the data that is processed is transmitted. PII is exchanged, processed, and transmitted between information systems daily. Protecting this data requires robust policies, processes, and technologies.[51]

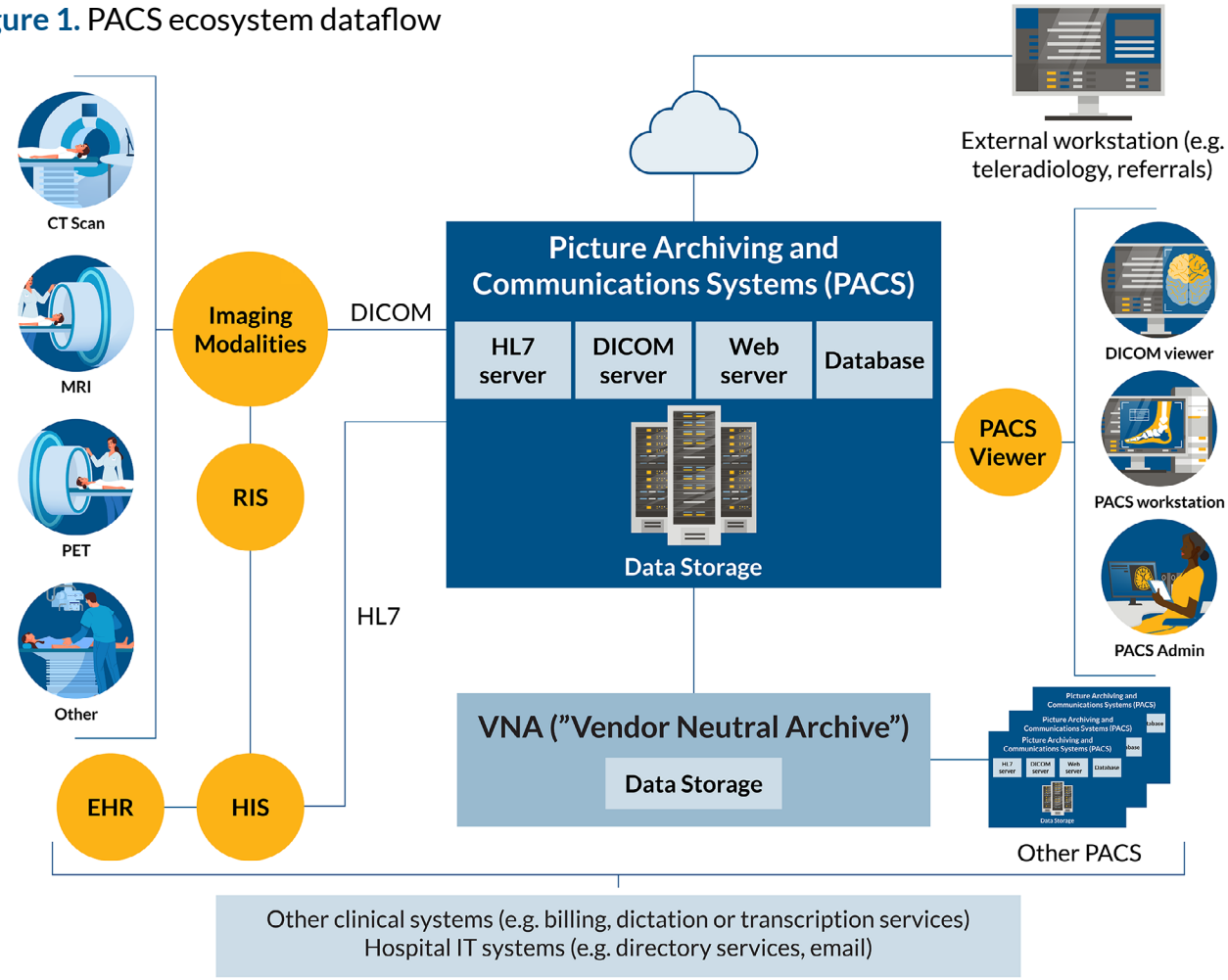
As your organization substantiates its data protection and prevention controls, it is best to begin by understanding the types of data that exist in your organization, setting a classification schema for these data, and then determining how the data are processed. Establish a set of policies and procedures for normal data use and then build in "guardrail" systems to guide your user base toward these business processes.

Information can leak outside your network if you are not aware of your network design, Healthcare Delivery Organizations (HDOs) networks consist of dozens of traditional IT protocols (Server Message Block [SMB], Remote Authentication Dial-In User Service [RADIUS], Universal Plug and Play [UPnP], Secure Shell [SSH], Remote Desktop Protocol [RDP], etc.) and unique medical protocols (standard protocol such as Digital Imaging and Communications in Medicine [DICOM], Health Level Seven [HL7], American Society for Testing and Materials [ASTM], Laboratory Information Systems [LIS], Management Information Base [MIB] and several vendor proprietary protocols). Organizations should monitor unencrypted traffic. With such a large and diverse network to secure, aim for 360° top-down visibility to intelligently define trust relationships between device families, restrict lateral (in-group) communications, logically impose segmentation regimens outlined with **Cybersecurity Practice #6: Network Management**, and easily maintain network architecture per best practices. Traffic monitoring is needed to determine which devices are generating different type of traffic and to establish a baseline for anomaly detection. For a visualization of this, see the **PACS ecosystem dataflow** visualization example.

Further details can be found in **Cybersecurity Practice #5: IT Asset Management**.

51 Erika McCallister, Tim Grance, and Karen Scarfone, *NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, (April 2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

Figure 1. PACS ecosystem dataflow



Sub-Practices for Medium-Sized Organizations

4.M.A: Classification of Data

NIST Framework Ref: (ID.AM-5)

There is a vast proliferation of data in healthcare environments. Data can range from PII (i.e., treatment information, SSNs, insurance numbers, billing information) to research information. Data in healthcare environments can also include business sensitive information such as strategies and development plans, financial data, HR information, and corporate board materials.

When determining data classifications, consider not only confidentiality but data integrity and availability as well. For example, what if you can no longer trust the data is accurate because it has been damaged? What if you can never have access to that data again because you can never retrieve or restore it?

Before establishing policies on how various data types should be used and disclosed, it is best to classify them into high-level categories. This provides a consistent framework when developing policies and procedures. Table 4 outlines a sample classification schema, with examples of the types of documents the classification comprises.

Table 4. Example of a Data Classification Schema

Classification	Description	Examples
Highly Sensitive Data	Data that could easily be used for financial fraud or could cause significant reputational damage.	SSN, credit card number, mental health information, substance abuse information, infectious disease treatment, employment/professional details, or other demographic information.
Sensitive Data	Regulated data, or data that could cause embarrassment to patients or organizations.	Health information, clinical research data, insurance information, human/employee data, and board materials.
Internal Data	Data that are not considered sensitive but should not be exposed publicly.	Policies and procedures, contracts, business plans, corporate strategy and business development plans, and internal business communications.
Public Data	All data that have been sanitized and approved for distribution to the public with no restrictions on use.	Materials published on websites, presentations, and research publications.

4.M.B: Data Use Procedures

NIST Framework Ref: ID.GV-1

After data have been classified, procedures should be written on how to use these data based on classification. These procedures describe the processes of setting usage expectations and of labeling the information properly. These two functions are described further in the following paragraphs.

- ***Usage and disclosure:*** Based on the classification type, data use should be limited appropriately and disclosed using specific methods. Consider the procedures in Table 4.
  Be careful when sending information through email. Ensure that sending PHI via email is consistent with the standards of the HIPAA Security Rule.[52] Do not send unencrypted PHI through regular email or text message. Patients can request and receive access to their PHI via unencrypted electronic communications following a brief warning that unencrypted communications could be accessed by a third-party in transit. After reading this disclaimer, the patient must confirm that they still want to receive the unencrypted communication.
- ***Labeling:*** It is important to label information properly to facilitate restriction implementation related to its usage and disclosure. Labeling helps keep data secure in two ways. First, users will understand how to handle information that is properly labeled. Second, specialized security tools, such as data loss prevention (DLP) systems, can be configured to discover and control properly labeled information.

52 "Does the Security Rule allow for sending electronic PHI (e-PHI) in an email over the Interent? If so, what protections must be applied?," HHS OCR (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html.

At a minimum, the labeling process should ensure that labels are readily apparent when users view information. Use techniques like placing the classification in the footer of the document. Collaborate with your marketing and communication departments to create document templates based on data classification levels. Organization-wide document templates allow specialized tokens or signatures to be embedded in the documents and tracked by DLP systems.

Table 5. Suggested Procedures for Data Disclosure

Classification	Use	Disclosure
Highly Sensitive	1. Must be restricted to the minimum necessary for individual job function. 2. Must use extreme caution when handling data.	Only share information internally and only when expressly permitted and when directed by the data owner.
Sensitive	3. Must be restricted to the minimum necessary for individual job function.	Only share information internally and only when expressly permitted.
Internal Use	4. Can be generally used, but care should be considered in its consumption.	Only share information internally within your organization.
Public	5. No restrictions.	Share freely with no restrictions.

4.M.C: Data Security

NIST Framework Ref: PR.DS, PR.DS-1, PR.DS-2, PR.IP-6, PR.DS-5

After policies and procedures have been defined, you can establish additional data security methods. Consider the security methods described below in Table 6.

Table 6. Security Methods to Protect Data

Security Method	Description	Considerations
Enable encryption	Encrypt data in rest and in transit	• When using the cloud-based services, enable native encryption capabilities to prevent exposures if the cloud provider is hacked. • Ensure that full disk encryption is enabled on all workstations and laptops. • Encrypt highly sensitive data stored in filesystem or within applications.

Security Method	Description	Considerations
Encrypt data in transit	Data retention and destruction	• Ensure that websites containing sensitive data use encrypted transport methods, such as Hypertext Transfer Protocol Secure (HTTPS). • Enable internal encryption methods when moving data in your organization. • Never send unencrypted sensitive data outside your organization.
Data retention and destruction	Contractually bind third-parties to destroy data when terminating contracts.	• Use standard destruction forms and require vendors to attest that data have been destroyed pursuant to those forms. • Set retention policies and quotas on email systems to reduce the amount of data that can be exposed. Ensure that legal retention requirements are met. • Establish a purge strategy that includes secure deletion mechanisms.
Protect production data	Scrub production data from test and development environments	• Leverage specialized tools to deidentify data elements within large systems (such as EMRs). • Regularly audit data elements within test and production environments to ensure that they are clean.
Protect sensitive data	Mask sensitive data within applications	• Permit SSN access only to members who require it (e.g., registration desks, admitting desks, payor processing).

4.M.D: Backup Strategies

NIST Framework Ref: PR.IP-4

A robust backup strategy for enterprise assets is critical to daily IT operations. It is equally important to have 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, routine backups can be the only way to ensure proper execution of the recovery phase of your IR process. Fully decommissioning affected assets and restoring them to a time before the compromise occurred is the best method to neutralize the compromise.

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

No matter what backup strategy you choose, it is very important to make sure these backup locations are not accessible from the general network or from general user populations. Backups may be the last line of defense against a ransomware attack, so access to them should be severely limited.

This includes access from the servers and systems themselves that are being backed up. Consider only allowing systems to write new data rather than overwrite existing data. This can thwart the attempts of encryption attacks against backup files.

Several commonly used backup strategies are listed below.

- ***Disk-to-tape:*** This method makes backups by accessing designated systems and files and writing all content to a tape drive, or a tape library. Specialized software, hardware, and inventory controls are required. To conduct backups efficiently, you will need tape robots and a tape library appropriate to the number and size of systems being backed up. These backups can be very large. Configure the tapes to use a "write once and read many" option. It is of utmost importance that encryption is enabled in writing to these tapes. If a tape is lost or stolen, unencrypted data could be breached. There are great advantages to maintaining offline backups. You can rely on these copies to be available when you need them, and tape backups prevent attacks against the backup medium itself, because they are offline.
- ***Disk-to-disk:*** This method involves taking backup copies from a disk and replicating them to a separate disk, or storage array dedicated to maintaining backup copies. This option generally costs less than disk-to-tape strategies, and disk-to-disk backups usually execute more quickly than disk-to-tape. It is important to use encryption on backup files in the event the files are copied outside of your organization.
  It is important to consider controlling access to the disk storage system as part of a disk-to-disk approach. With cyber-attacks like ransomware, attackers intend to disrupt both production and backup files. Attackers that launch ransomware attacks are aware that an organization's first response will be to contain the ransomware and then restore the uncorrupted files from a backup source. If they can compromise the backup and production files, it is more likely your organization will pay a ransom to get its files back. Access control mechanisms should prevent the system being backed up from accessing the disk array, except via required access channels. Do not permit other access to the array from other accounts, including administrative accounts. Remember, everyone is a potential target of a ransomware attack, especially administrators.
  New "backup vaulting" tools can manage these access permissions and make it near impossible for automated ransomware attacks to compromise the disk storage arrays. The use of these tools tends to be expensive, so it is recommended to start with your mission critical applications and data first, as part of your Business Impact Analysis (BIA) processes.
- ***Disk-to-cloud:*** This method is very similar to disk-to-disk backup. Cloud backup offers multiple added values, however. With a disk-to-cloud backup, you get the resiliency and flexibility of the cloud environment, as well as the benefits from investments made by the cloud providers, to maintain 100 percent data availability. Rather than a single-point-of-failure model, as seen in disk-to-disk and disk-to-tape backups, cloud providers replicate data backups, leveraging cloud infrastructure with multi-fault–tolerant capabilities.
  As with the disk-to-disk model, it is important to limit access to cloud-based backup storage to only the systems and disks that are backed up and the data repository. Never implement a drive that maps to the backup repository. That mapped drive could be the vehicle that delivers the ransomware encryption. Always encrypt backup files to protect your organization if the cloud provider is breached.

- ***Disk-to-disk-to-cloud:*** This method combines the speed and local accessibility achieved with disk-to-disk with the redundancy and off-site capabilities of the cloud. Information is backed up locally to devices that meet the disk-to-disk requirements mentioned above. Those local devices then backup to a cloud copy with archives.
  When using cloud solutions, it is important to understand what your restore options are with any selected solution. Ideally, if you must restore from the cloud copy of your data you want the backup provider to ship you a disk with that data on it. Restores directly from the cloud can take an exorbitant amount of time.

Two values every backup plan must include are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Your organization may have an affordable backup solution that you believe meets your needs until you need to recover or restore data from the backup. One of the most crucial elements of a backup plan is the plan's restore capabilities, that is, to know how long it will take to do a complete restore of the data and know what point in time your data will be at when the restore completes. A backup plan alone is ineffective without the ability to restore the data.

Testing the restore is essential, as it determines if the backup contains the required information can be restored at the point in time and within the timeframe you need. Without the objectives set (and a test to prove the plan works) it is only a backup plan, not a restore plan.

Lastly, whatever method of backup is used, it is important to test the restoration of these backups on a periodic basis to ensure data availability. Remember, your backup process is the last line of defense and must be trustworthy in a time of need. Another consideration for selecting a backup method is the amount of time it takes to restore data. Assessment of available methods should include disaster recovery timing objectives.

4.M.E: Data Loss Prevention (DLP)

NIST Framework Ref: PR.DS-5

Once standard data policies and procedures are established and the workforce is trained to use them, DLP systems should be implemented to ensure that sensitive data are used in compliance with these policies.

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

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

- ***Identify sensitive data based on dictionary words that may trigger the inclusion of sensitive data.*** These dictionaries include robust language repositories that identify health information. The challenge with this technique is terminology. Medical terms are often used in the regular course of business, outside the context of sensitive information. This can lead to a high rate of false positives, forcing the workforce to apply prevention practices that are not necessary.
- ***Identify sensitive data based on identifiers that are known to be sensitive, a process known as matching.*** There are two popular methods of matching: (a) leveraging tokens embedded in documents classified as sensitive (document matching) and (b) leveraging actual patient identifiers from your EMR (exact

data matching). Document matching dramatically reduces the number of false positives. However, the workforce must be trained on proper data classification. With exact data matching, the false positive rate will be lower than with the dictionary approach since it involves positive confirmation. Exact data matching requires regularly extracting information from the EMR to load these identifiers into the system. Extra precautions must be taken so that the resulting large datasets are not exposed.

Once your identification methodology is established, DLP systems can be configured to monitor data access channels of interest and make policy decisions based on the data types and the access channels.

It is best to provide direct feedback to users when the data policy has been violated, to avoid recurrent violations. Real-time feedback helps users adjust their data usage behaviors effectively. Data channels are presented in Table 7 for your consideration.

Keep in mind DLP technology does not have perfect visibility and matching. If data is encrypted, DLP may not have visibility to the contents. In addition, DLP may not have visibility to all communication channels (e.g., SFTP, SCP). For a determined insider, DLP may not prevent theft of data captured through cameras, copy/paste, printing, etc.

Table 7. Data Channels for Enforcing Data Policies

Data Channel	Implementation Specification	Considerations
Email	Implement inline through Simple Mail Transfer Protocol (SMTP) routing for email messages delivered outside your organization.	• Define thresholds of risky behavior. Implement a DLP block for these thresholds (e.g., > 100 records of PHI in the email). • Define thresholds of risky behavior. Implement a DLP encrypt action for these thresholds, forcing the message to be encrypted before delivered.
Endpoint	Install DLP agents on managed endpoints that can apply data policies.	• Standardize and deploy encrypted thumb drives to users who require mobile storage options. • Prevent the copying of data to unencrypted thumb drives, or force encryption when copying data. • Control the use of noncontrolled peripherals and/or storage devices (e.g., backups of iPhones on devices). Permit only when specifically authorized. • Conduct data discovery scans of data residing on endpoints, exposing data on the endpoint so the user can make data destruction decisions.
Network	Implement through Switched Port Analyzer (SPAN) ports from egress network points or through internet Security Content Application Protocol (SCAP) on web proxies.	• If online, prevent the leakage of unencrypted sensitive data based upon predefined thresholds (e.g., files that contain > 100 records of PHI). • If out of band, activate IR procedures to contain data leakages that occur through the network.

Sub-Practices for Large Organizations

4.L.A: Advanced Data Loss Prevention

NIST Framework Ref: PR.DS-5

After implementing basic DLP controls, consider expanding your DLP capabilities to monitor other common data access channels. Table 8 below includes recommended methods for this.

Table 8. Expanding DLP to Other Data Channels

Data Channel	Implementation Specification	Considerations
Cloud storage	Use cloud access security broker (CASB) systems to monitor data flows into cloud systems.	• Label data identified as sensitive. Implement digital rights and encryption to limit access to sensitive data. • Ensure that cloud-based file storage and sharing systems 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). • Establish technical cloud-based security policies matching your organizational security policies.
Onsite file storage	Point discovery scanning systems at known file servers or other large data repositories.	• Conduct regular DLP scans against the file systems to scan and identify sensitive data. • Query security access permissions for each file containing sensitive data. Define thresholds for excessive access and set alerts if these are crossed. Forward alerts to the SOC for response, as described in Cybersecurity Practice #8: Security Operations Center and Incident Response. • Determine relevance and age of records with sensitive data. Consider executing data destruction practices for records that have not been opened or viewed for an extended duration. • Determine data ownership of sensitive files identified in file storage systems, leveraging automated tools. Establish workflow options allowing data owners to provide input into access permission reviews of their sensitive files.
Web-based scanning	Configure DLP systems to crawl known public websites for sensitive information.	• Conduct a "spearing" exercise, which is like methods deployed by search engines. Compare files and results posted on websites against DLP matching policies and respond quickly to any sensitive data that are exposed. • 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).

4.L.B: Mapping Data Flows

NIST Framework Ref: ID.AM-3, DE.AE-1

The process of mapping data flow requires evaluating each application used and the information that flows throughout your organization. This process is broader than IT, so all data stakeholders must be engaged. The data mapping process should include both vended as well as internally developed applications. For internally developed applications, you may be able to partner with stakeholders in your organization's software development lifecycle process. For vended applications, you may be able to partner with stakeholders in your organization's supply chain process.

In 2019 the Healthcare and Public Health Sector Coordinating Council (HSCC) released a new publication, the Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM).[53] This publication describes processes and techniques for managing all third-party risk. It also includes sample questionnaires for vendors to complete, which can be used to gather information for mapping data flows. These same questions can be asked of internal development teams.

The process also requires an understanding of all the applications used, as well as the information they contain and exchange with other applications. Data mapping documentation should be reviewed periodically to reflect changes in your organization's data needs. Leverage contract initiation or renewal events as ideal times to review non- or pre-existing data mapping documentation.

By following this process and maintaining an accurate mapping of data flow, an organization can quickly adapt to application system changes, such as upgrades, patches, integrations, and migrations. The mapping process also ensures protection of data integrity through the understanding of "what data lives where."

After data business practices are defined, it is advisable to outline these processes in a data map. Data maps should include the following components:

- Applications that house sensitive data
- Standard direction movement of data
- Users of applications and data
- Methods used to store and transmit data

Data mapping documentation does not need to be visually formatted, although data flow diagrams can be very useful. The data mapping documentation should provide enough information to answer some basic questions about the data itself:

- Where does the data come from?
- Who can access the data and how do they do it?
- How are users authenticated?
- Once authenticated, what data can users access?
- Where is the data stored?
- What can users do with the data?
- Where is the data retained, and for how long?

53 *Health Industry Cybersecurity Supply Chain Risk Management Guide v2.0*, Healthcare and Public Health Sector Coordinating Council (HSCC) (September 2020), https://healthsectorcouncil.org/hic-scrim-v2/.

Conducting this type of mapping, and potentially adding it to a larger enterprise architecture reference, enables an organization to identify data protection and monitoring requirements. Data mapping often results in more concrete information about the data managed by the enterprise, due to the ability to track attributes such as:

- Data ownership (business and technical owners)
- Data classification (public, private/internal, sensitive/regulated, etc.)
- Data type (PHI, PII, PCI, etc.)
- Data elements (patient name, MRN, DOB, etc.)
- Data location (data center, cloud, mobile device, etc.)
- Number of records stored
- Number of records processed, annually
- Number of users

Data mapping exercises can be a daunting task. It is important to understand that this may take time and effort to fully implement. It is recommended that a data mapping plan be created to ensure success. The plan should include:

- ***Start with one set of data at a time.*** Focus on one set of data at a time. For example, start with PCI information and then move to PHI, etc.
- ***Inventory of location.*** Once you understand the category of data, create an inventory of where the data is located. This can be done through surveys or interviews of application and database owners.
- ***Source categories and data collection.*** Once you know the location, develop categories of where the data comes from and how the data is collected.
- ***Access rights.*** Once you know the location and the data collection source, understand how access is granted to the data. This should include an understanding of the various business roles with access to the data.
- ***Data flow.*** Once the location is understood and the source of the data, appropriate data flow diagrams can be created to understand the data in transit (as it is forwarded in and outside your organization).

If your organization is new to the process of mapping data flows, various tools and examples can be found online.

Finally, note that not all data managed or owned by your organization will be contained or used in applications. In addition to internally developed and vended applications, consider data exchanges/interfaces (SFTP, HL7, FHIR, etc.), research projects, cloud APIs, medical devices, networking devices, mobile devices, etc. as potential data mapping subjects.

Key Mitigated Threats

1. Ransomware attacks
2. Insider, accidental or malicious data loss
3. Loss or theft of equipment or data

Suggested Metrics

- ***Number of encrypted email messages, measured weekly.*** The goal is to establish a baseline of encrypted messages sent. Be on the lookout for spikes of encryption (which could indicate data exfiltration) and no encryption (which could indicate that encryption is not working properly).
- ***Number of blocked unencrypted email messages with sensitive data, measured weekly.*** The goal is to detect large numbers of blocked messages, which could indicate potential malicious data exfiltration or user training.
- ***Number of files with excessive access on the file systems, measured weekly.*** The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets, and deliver to access management.
- ***Number of unencrypted removable devices with access attempts, measured weekly.*** The goal is to use this information to educate the workforce on the risks of removable media.
- ***Number or names of applications in high-risk categories.*** The goal is to identify and prioritize applications to protect. Applications that manage many sensitive, regulated, or protected data records with many users may be candidates for higher levels of protection than applications that manage fewer records, don't manage sensitive, regulated, or protected data, and have few users.
- ***Percentage of applications with complete data mapping documentation.*** The goal is to measure how much of your organization's data is documented and ultimately, appropriately protected.
- ***Number or percentage of applications with refreshed data maps that comply with the refresh policy.*** The goal is to ensure that data mapping documentation does not become stale and is refreshed at appropriate timeframes.

Cybersecurity Practice #5: IT Asset Management

Areas of Impact
PHI

Medium Sub-Practices
5.M.A Inventory of Endpoints and Servers
5.M.B Procurement
5.M.C Secure Storage for Inactive Devices
5.M.D Decommissioning Assets

Large Sub-Practices
5.L.A Automated Discovery and Maintenance
5.L.B Integration with Network Access Control

Key Threats Addressed
- Ransomware attacks
- Insider, accidental or malicious data loss
- Loss or theft of equipment or data
- Attacks against network connected medical devices that may affect patient safety

405(d) Resources
- Prescription Poster: IT Asset Management

The process by which organizations manage IT assets is generally referred to as IT asset management (ITAM). ITAM is critical to ensuring proper cyber hygiene controls are in place across all assets in your organization. ITAM increases the visibility of cybersecurity professionals in your organization and the use of discovery tools reduces unknowns.

ITAM processes should be implemented for endpoints, servers, application, and networking equipment. The cybersecurity practices in this section assist and support every other cybersecurity practice identified in this publication. ITAM cybersecurity practices can be difficult to implement and sustain, but they should be incorporated into every lifecycle stage of IT operations to maintain data accuracy and integrity. For each asset, the lifecycle includes procurement, deployment, maintenance, and decommissioning. Though each type of asset is used differently during its lifecycle, the lifecycle itself is consistent. As part of its public–private partnership with the NIST National Cybersecurity Center of Excellence (NCCOE), the financial sector has written a detailed ITAM practice guide: IT Asset Management.[54] Though written for a financial-sector audience, the methods discussed in the guide are easily applied to the HPH sector.

Sub-Practices for Medium-Sized Organizations

5.M.A: Inventory of Endpoints and Servers

NIST Framework Ref: ID.AM-1

The first ITAM component that should be implemented is an inventory archive buildout. This critical technology component provides a normalized, consistent approach for organizations to store inventory data.

Important data elements and attributes should be captured for each asset in the ITAM. It is recommended to evaluate following granular device attributes for inclusion in your ITAM:

- AssetID (primary key)
- Hostname
- Operating System—Type, version, patch level, hostname

54 Michael Stone et al., *NIST Special Publication 1800-5b: IT Asset Management*, NIST(October 2015), https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5b-draft.pdf.

- Media Access Control (MAC) Address
- Internet Protocol (IP) Address
- Deployed to (User)—Users associated with current of past login or sessions
- Last Logged on User
- Purchase Date
- Device Category
- Manufacturer and model
- Firmware—Type and version
- Software Profile—Installed applications version, open ports
- External components—DOK, Portable Hark Disk, etc.
- Network Context—MAC, IP, VLAN, Connection Type, Access Point/Switch, SSID, managed/unmanaged device, open ports, inbound/outbound traffic
- Organizational Context—Location, site, organizational unit
- Unique Tags—Serial number, Recall needed, MDS2, Lost, New, Device ownership (company managed device, employee's personal device, vendor's device etc.)
- Data Type—PHI (storing/transmitting), PCI

A robust ITAM repository becomes your single source of truth for all IT assets in your organization. This repository will be maintained and trusted to be highly accurate and actionable.

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

IT service management tools (e.g., ticketing systems) can be integrated with IT general controls to ensure accurate and precise asset management through standard performance management activities.[55]

55 "CIS Control 1: Inventory and Control of Hardware Assets," Center for Information Security Controls (Accessed September 24, 2018), https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/.

5.M.B: Procurement

NIST Framework Ref: ID.AM

A critical milestone for success is to incorporate the ITAM processes into the supply chain program. The goal is to have supply chain activity from across your organization proactively entered in the ITAM system. The result will be that each technology asset, endpoint, server, or networking equipment is registered in the ITAM system as it is acquired.

An example of integration of the ITAM process into your organization's existing supply chain scheme is to introduce a process. This process should include the following steps:

- ***Step 1:*** Identify each department that can procure or acquire technology.
- ***Step 2:*** Work with the supply chain departments and establish a centralized workflow (such as a ticketing system) for the ordering of technology. This could be considered the first step in the asset's lifecycle tracking.
- ***Step 3:*** As part of the workflow, inform the IT department of the new technology being ordered. This can be accomplished through a ticket that assigns a specific task to the IT department for setting up the asset.
- ***Step 4:*** Receive the asset from the supplier. As part of the receiving of the asset, update the workflow (or ticket) and collect the asset information previously referenced in section **5.M.A: Inventory of Endpoints and Servers**. Data about the new asset can be captured physically, at a shipping dock, or virtually for virtual technology purchases.
  Some organizations may choose to adopt an advanced approach where the procurement process may be automated to capture characteristics or attributes details of new assets. Automation of the process reduces the manual labor required and the exposure to human error in collecting the data.
- ***Step 5:*** As an asset is acquired, it must be tagged it with an asset tag. These tags can be physical or logical. The tagging process ensures that the asset has a unique ID that can be used to identify it in the ITAM system. Assigning a unique ID that uses existing attributes of the technology (e.g., hostname, IP address, MAC address) is not recommended. These fields aligned with these attributes may change, potentially creating duplicate records.

5.M.C: Secure Storage for Inactive Devices

NIST Framework Ref: PR.AC-2

Assets that are not in circulation should be returned to the appropriate IT department for secure storage. Storage areas (e.g., lockers, cages, rooms) should be secured with physical access controls. Access should be limited to those who require it. As assets are being stored they should either be securely wiped or full-disk encryption should be verified. In both cases, it is important to have these records in place in the event the device is misappropriated, and a forensic analysis of data exposure is necessary. Physical access controls may include badge readers, video camera surveillance, and door alarms.

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

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

5.M.D: Decommissioning Assets

NIST Framework Ref: PR.IP-6, PR.DS-3

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

- ***Central collection:*** IT assets should be collected and stored in centralized, physically locked areas prior to decommissioning. Your workforce must be trained to turn in any asset that they no longer use.
- ***Central destruction/wipe:*** Assets that are collected for decommissioning must undergo a secure process to destroy or electronically wipe the storage media. This ensures devices are properly sanitized before leaving your organization's possession for destruction. Permanent removal of storage media may be completed by your IT organization or an external service provider. It is a good practice to obtain and archive a certificate of destruction for audit purposes.
- ***Record keeping:*** Once the IT asset has been cleared for removal from your organization, the asset ITAM record should be registered for destruction or decommissioning. Certificates of destruction can be stored in the ITAM record for easy access. It is highly advisable to not delete the asset record. Instead, update the asset's status in the ITAM system to reflect it has been decommissioned and is no longer owned by your organization. You may need to refer to the asset record in the future.

Sub-Practices for Large Organizations

5.L.A: Automated Discovery and Maintenance

NIST Framework Ref: PR.MA-1, PR.MA-2, PR.DS-3

Once your ITAM system is in place and your procurement processes are registered, the challenge is maintaining the records. Large organizations can have tens of thousands of endpoints and thousands of servers. As attributes must be kept for each asset, it can mean hundreds of thousands to millions of unique data elements require management across the entire ITAM system.

It is very difficult to manually maintain hundreds of thousands of data elements. After an asset is acquired, without the exercise of proper asset management controls, it could be deployed sometime in its lifecycle in unforeseen ways. For example, a new laptop may be issued to a user. That user may leave your organization, turning in the laptop to a supervisor. The supervisor may assign the laptop to the new employee who fills the open position. Unless IT is informed and the ITAM is updated, the asset record for the laptop (now assigned to a different user) will be wrong.

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

Automated discovery systems can maintain these records and account for both scenarios described above. In the case where an asset changes hands to a new user, discovery tools can register login occurrences for the "assigned user" and for the "actual logged in user." If a threshold is triggered (indicating that the assigned user no longer logs in and a different user continually logs in), a change-in-ownership process can be triggered. This process may be automated, requiring no intervention, or manually completed by generating a ticket to validate the change of ownership. In the case of operating systems patching levels, automated discovery systems can provide snapshot views of current patching levels for assets. When these snapshots are compared by cybersecurity vulnerability management systems, vulnerabilities due to obsolete software versions will be identified across the fleet.

5.L.B: Integration with Network Access Control

NIST Framework Ref: PR.AC-4, PR.AC-5, PR.AC-6

The practices outlined so far assume normal acquisitions processes. However, there are times when IT assets are integrated in your organization by means other than standard supply chain channels. Examples include personal devices (i.e., BYOD) and assets that are donated or provided free-of-charge as part of a third-party contract.

Without oversight, it is difficult to detect and track these assets. Outliers can be controlled by integrating your NAC and ITAM systems. Further details can be found in Cybersecurity Practice #6: Network Management. It is also difficult, and time consuming to track and protect the flow of data through these assets. Further details can be found in Cybersecurity Practice #4: Data Protection and Loss Prevention.

Key Mitigated Threats

- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that may affect patient safety

Suggested Metrics

- ***Percentage of devices added to ITAM system through procurement channels, measured monthly.*** The goal is to establish a baseline and achieve a higher percentage over time.
- ***Number of devices added to the ITAM from NAC systems, measured weekly.*** The goal is to analyze spikes after initial deployment, which may indicate a problem capturing or maintaining asset records.
- ***Number of devices properly removed from asset management system using proper decommissioning channels, measured weekly.*** The goal is to ensure devices are properly decommissioned. Lack of execution of these processes over a period may indicate a compliance issue.

Cybersecurity Practice #6: Network Management

Organizations leverage IT networks as a core infrastructure to conduct business operations. Without networks, there would be no interoperability. Networks must be deployed securely to limit exposure to the potential impacts of cyber-attacks. Network design will have a direct impact on how well you can thwart some of the more nefarious cyber-attacks, such as ransomware attacks. Network diagrams are crucial to network management. They can:

- Provide visibility to current network segmentation, including analysis of each device type (medical and non-medical devices) in each segment, connectivity between VLANs, and breakdown of devices by type and vendor.
- Be designed to associate a risk level for each segment/VLAN.
- Demonstrate highly granular visibility to achieve more precise baselining and greater context awareness.
- Allow for more accurate device classifications, delivering greater functionality and safe use insights (with which to define trust relationships).
- Represent a real-time viewpoint into inter-device traffic flows to inform attack detection and access policies.

Areas of Impact
PHI

Medium Sub-Practices
6.M.A Network Profiles and Firewalls
6.M.B Network Segmentation
6.M.C Intrusion Prevention Systems
6.M.D Web Proxy Protection
6.M.E Physical Security of Network Devices

Large Sub-Practices
6.L.A Additional Network Segmentation
6.L.B Network Analytics and Blocking
6.L.C Network Access Control

Key Threats Addressed
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against medical devices that can affect patient safety

405(d) Resources
- Prescription Poster: Network Management

Sub-Practices for Medium-Sized Organizations

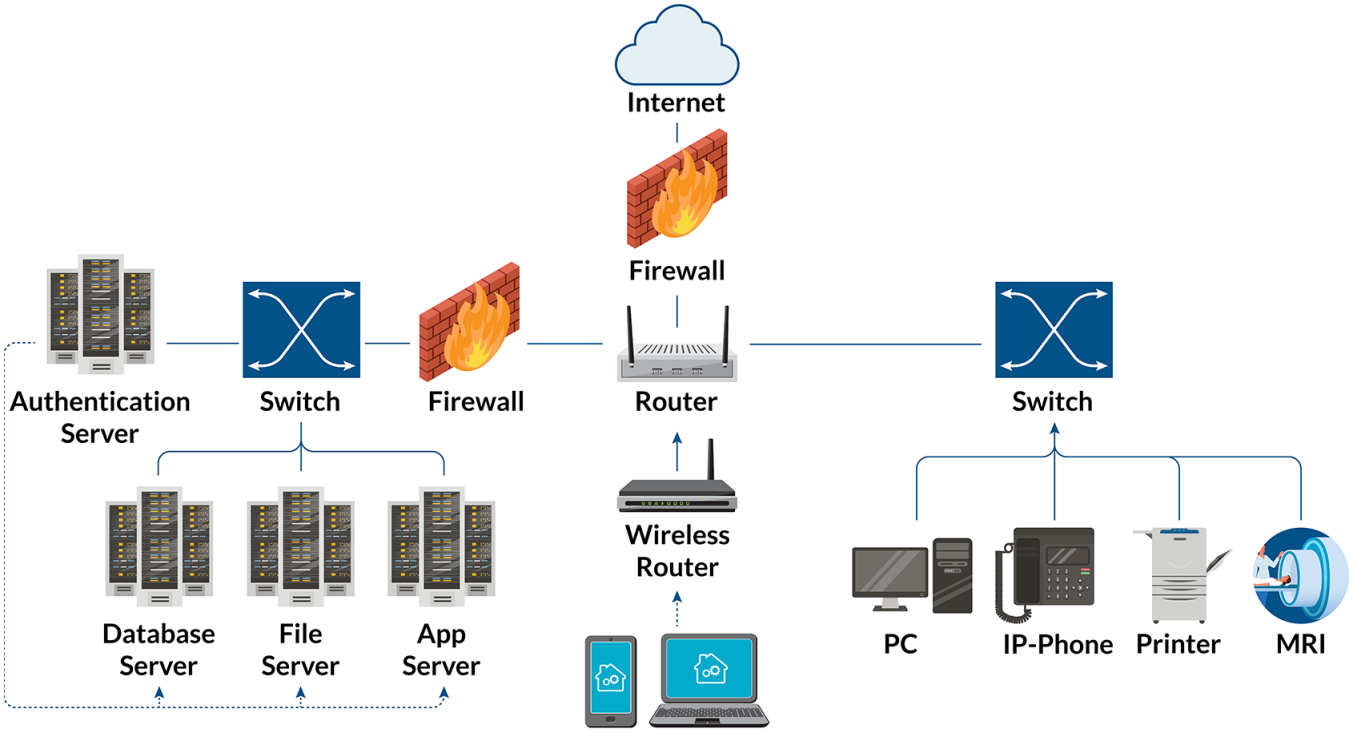
6.M.A: Network Profiles and Firewalls

NIST Framework Ref: PR.AC-5, PR.AC-6

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

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

Figure 2. Firewall Segmentation



Consider limiting the outbound connections permitted by assets in your organization. This can be a challenge to implement organization-wide. However, for zones of high sensitivity, egress limiting can prevent malicious callbacks or data exfiltration. The SOC should monitor egress logs, as outlined within Cybersecurity Practice #8: Security Operations Center and Incident Response.

Firewall rules may change when technology is added or removed. A robust change management process should include reviewing every firewall to identify necessary changes. These change requests should comply with standard IT operations change management processes and be approved by cybersecurity departments before any firewall is modified. Refer to sub-practice 7.M.E: Change Management for more details on change management.

As part of standard rule management for firewalls, it is important to periodically review firewalls to ensure they are properly structured as required by cybersecurity teams. Consider implementing a monthly or quarterly review of the highest-risk rulesets.

6.M.B: Network Segmentation

NIST Framework Ref: PR.AC-5

Partitioning networks into security zones is a fundamental method of limiting cyber-attacks. These zones can be based on sensitivity of assets within the network (e.g., clinical workstations, general user access, guest networks, medical device networks, building management systems, IoT networks) or standard perimeter segmentations (e.g., DMZ, middleware, application servers, database servers, vendor systems). Examples of standard network zones are as follows:

- ***Perimeter defenses:*** Most organizations host services that are accessed through the internet. A robust defense strategy should be deployed to monitor these "front doors."[56]
  Best practices for perimeter defenses include the following:
  - Implement highly restrictive rules on inbound and outbound ports and protocols. Use default-deny rules in firewalls and enable access only when clearly understood.
  - Restrict DMZ from middleware, application, and database servers. DMZ controls are critical, as these servers are exposed to the internet and, therefore, have a large threat footprint.
  - Restrict the ability for DMZ servers to log directly into inside network servers, specifically using remote desktop protocol, server message block, SSH, or other remote access ports (tcp/3389, tcp/445, tcp/139, tcp/22).
  - Ensure local administrator passwords are unique to each DMZ server and do not use these passwords for any other server in your organization.
  - Ensure DMZ servers cannot connect directly to the internet. Instead, these servers should access the internet through outbound proxy services. Outbound proxy rules should limit the sites, URLs, IPs, and ports that a DMZ server can access to only allowlisted sites required for updates or application functionality. Be cautious of allowlisting hosting organizations like Amazon Web Services, as malicious actors may use them to download malware to a compromised server.
  - Do not provide access to the internal network directly via protocols like telnet, SSH, or RDP. Instead, leverage a VPN with MFA for accessing internal network resources.
  - Consider this type of restriction configuration for partner WAN links or site-to-site VPN connections. Do not permit access to systems/applications that are not required by the user.
- ***Data center networks:*** Servers in the data center should be segmented into appropriate zones. Several different layers of segmentation may occur within data center networks, including
  - database servers;
  - application servers; and,
  - middleware.
- ***Critical IoT assets:*** It is important to restrict access to assets that have a potentially high impact on the business or patients if compromised. Management and patching of security vulnerabilities in IoT devices is often limited. Examples include medical devices, security cameras, badge readers, temperature sensors, and building management systems. These assets generally exist outside of the data centers. Without proper segmentation, they may infiltrate general access networks. To achieve segmentation in physical buildings, leverage multiprotocol label switching to build out virtual networks. Place these network access restrictions behind core firewalls.
- ***Vendor access:*** Vendor access should be limited based on need. It should be temporary, and only access to required information should be granted. Some assets are managed exclusively or accessed by third-party vendors. These vendors may need continual access to your organization's network. It is important to segment this vendor access from other networks and limit the vendor's ability to access other parts of your corporate network. Whether these networks exist inside or outside of the data center, the principles are the same. In 2015, the retailer Target was the victim of a cyber-attack

56 "CIS Critical Security Control 12: Network Infrastructure Management," Center for Information Security Controls (Accessed June 2, 2022), https://www.cisecurity.org/controls/boundary-defense/.

leveraging these channels.[57] Common examples include building management systems, security systems, physical access controls, and persistent tunnels required to enable cloud functionality.

- ***General access networks:*** Most of your workforce will operate on general access networks. These are "edge" networks that provide connectivity back to the services offered in data centers, the internet, or other assets. General access networks require a sense of openness when communicating with services that are hosted by your organization. However, restrictions should be implemented that prohibit the assets in one general access network from communicating with the assets in another general access network. This critical control that can help stop the outbreak and spread of malware and ransomware attacks.
- ***Payment Card Processing networks:*** Establishing a dedicated zone specifically for systems processing credit card data will limit the scope of PCI compliance obligations and minimize cardholder data exposure.
- ***Guest networks:*** It is common for organizations to provide guest access to the internet, especially in provider organizations visited by patients and their friends and families. However, it must be restricted and controlled appropriately. These restrictions should exist on wireless networks (where it is most common), as well as wired networks often located in public spaces or conference rooms. Explicitly prohibit access to the internal network from networks. Guest users requiring access to internal resources should leverage a publicly available website or VPN. To the extent possible, limit the ability of your workforce to access guest networks. Guest networks may not have the same controls as your internal network.

6.M.C: Intrusion Prevention Systems

NIST Framework Ref: DE.CM-1

An intrusion prevention system (IPS) is important for your network perimeter, data center, and partner connections. An IPS is capable of reading network traffic to detect and potentially prevent known attacks. IPS will typically leverage deep packet inspection to look at the context of protocols.

Increasingly, IPS is integrated with next generation firewalls and are not often found as a standalone device. When deploying IPS systems for the first time, it is recommended to enable them into a 'monitor only' mode so they system can be properly tuned without causing disruptions. When the tuning is complete, you can then enable them in "prevention mode" or "quarantine mode" to proactively stop malicious attacks.

Savvy attackers will take steps to obfuscate or mask malicious traffic to avoid detection. To stay up to date, IPS should leverage a Structure Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) feed to obtain IOC from an Information Sharing and Analysis Center (ISAC) or similar source. While an IPS may not identify every single attack, it can be useful for baselining your network activity (as covered in **Cybersecurity Practice #8: Security Operations Center and Incident Response**). An IPS may also provide information enabling your IR team to conduct forensic activities.

57 Michael Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet (February 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

6.M.D: Web Proxy Protection

NIST Framework Ref: PR.AC-3, PR.AC-5

Web proxy systems provide important protections against phishing and malware attacks. These systems are implemented at the perimeter of the network or in the cloud to provide protections for your mobile workforce. Because most phishing and malware attacks are web-based, web proxy systems provide user friendly error pages explaining that they have been restricted from accessing a known malicious website. Such pages also provide informative feedback for users. When configured properly, web proxy systems leverage the following methods to limit client-side attacks:

- ***Reputation blocking:*** Many blackhole lists are available publicly or through Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs); proxies can use these lists to prevent users from accessing malicious websites. The lists are usually integrated into proxy systems through automated feeds.
- ***Organizational block lists:*** As part of an organization's IR, malicious websites and other sites can be identified based on actual attacks against your organization. Web proxy systems are critical shut-off points to limit access to websites quickly.
- ***Category blocking:*** Most modern, commercial web proxy technologies will pre-categorize websites on behalf of your organization. Considering the millions of websites that exist, this is a highly useful service. Consider blocking categories that contain malicious, suspicious, or illegal websites.

In addition to blocking traffic to specific sites, web proxies can inspect TLS traffic. This is important since over half of all malicious traffic is sent encrypted. Unencrypting HTTPS traffic allows:

- the data to be checked for malicious content;
- downloads to be sandboxed prior to delivery; and
- other functions to occur that reduce the likelihood of web-based attacks and compromise.

Sandboxing is one function of a web proxy. Through monitoring common protocols that allow downloading of binaries and files, organizations can check a download prior to permitting it to run on your organization's devices. Downloaded binaries, executables, or even data files (e.g., docx, xlsx) run in a virtual environment that looks for malicious activities when the file executes. Tools that facilitate automated sandboxing look for suspicious outputs or actions, rather than attempting to base actions on a particular signature of a specific configuration.

Web proxies and similar infrastructure can inspect files, and other content, passively or actively. Passive systems monitor network traffic at the stream level, not residing in line with the communication flows. Active systems insert themselves into the communication flows and conduct checks automatically, denying access to downloaded files until they are cleared.

6.M.E: Physical Security of Network Devices

NIST Framework Ref: PR.AC-2

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

- ***Data and network closets should always be locked.*** Consider the installation of badge readers instead of traditional key locks to monitor access.
- ***Disable network ports not in use.*** Ensure procedures are in place to maintain ports in shutdown mode (until an activation request is submitted and approved).
- ***Establish guest networks in conference rooms configured to access specific networks that do not have access to individually identifiable information or other sensitive data.***

Sub-Practices for Large Organizations

This section includes methods to detect and potentially prevent cyber-attacks against an organization's network. These methods should be engineered into network management practices. Once network-level detection and prevention methods are established, cybersecurity departments can follow Cybersecurity Practice #8: Security Operations Center and Incident Response to monitor and respond to attacks on the network.

6.L.A: Additional Network Segmentation

NIST Framework Ref: PR.AC-5, PR.AC-6, PR.PT-4

Further limiting access to sensitive resources can lessen the potential impact of a security incident. Consider the following additional segmentation approaches:

- ***Required VPN access for data center:*** Consider implementing a VPN, or bastion hosts, that must be enabled before access is granted to privileged servers in the data center. The VPN/bastion hosts should be equipped with MFA. Only authorized IT administrators should be granted access. Logs should be routed to the SOC for monitoring.
- ***Zero Trust:*** One emerging framework for organizational cybersecurity is "zero trust." This framework has a basic design principle of "never trust, always verify." In practice, this means a more active role is taken in managing and granting access to network resources—continually verifying identities, devices, and services. In contrast to the traditional perimeter security mindset, this framework is designed to address the more fragmented nature of network use emerging in the past few years (as due to home and mobile workers, network connected medical devices, employee-introduced mobile devices, and network use by contractors and vendors). Zero trust is a framework used to deliver a more granular segmentation of users, assets, and resources on your network. For example, in a zero trust environment, a user affiliated with HR would not be able to make a network connection to a radiology system. This can help reduce the spread of malicious software like ransomware on a network.

6.L.B: Network Analytics and Blocking

NIST Framework Ref: DE.CM-1, DE.CM-7

Advanced persistent threats (APT), botnets, backdoors, and other technically sophisticated attacks may leverage concealed or camouflaged network traffic to bypass typical network protections. This includes command and control (C2) traffic to maintain access to compromised computers. C2 traffic consists of beacons, typically outbound from the computer, that check back into a central server. Identifying such traffic can help detect where an attacker has maintained persistence. Signs of C2 traffic include:

- ***Direct to compromised server via Internet Protocol (IP) or Internet Control Message Protocol (ICMP):*** Traffic runs over the network using outbound ports or protocols that are generally open (e.g., HTTP, HTTPS, or ICMP protocols).
- ***DNS queries:*** The attacker establishes control using a DNS query embedded in malware that is downloaded to a computer. If the DNS record is maintained, the servers that maintain C2 communications can switch out and flex as they are discovered.
- ***Fast flux DNS queries:*** The hacker leverages DNS to maintain persistence, knowing that the DNS registrations will likely be taken down at some point. When this occurs, malware downloaded to the local client and C2 services runs an algorithm that checks the first several bytes of well-known sites (e.g., cnn.com, nbc.com) to create and register fake DNS names on your organization's DNS resolvers. To effectively address C2 traffic and other potential malicious activity, the best approach is to analyze network traffic rather than focus on a particular vector or attack style. Network tools may support "deep inspection," which allows the full contents of a packet to be analyzed, categorized, and built into massive databases of network-based metadata. Since traffic may not be easily detected, multiple different methods may be used together including:
- ***Intrusion Prevention System:*** As noted in cybersecurity practice 6.M.C: Intrusion Prevention Systems, an IPS combined with IOC can identify traffic to known command and control servers as well as common methods highlighted above.
- ***Netflow:*** Solutions exist that can leverage netflow data (e.g., source, destination, protocol) can perform analytics to look for anomalous activity (e.g., infusion pump communicating over DNS to an internet server).
- ***Next generation firewall:*** These devices can profile traffic and help monitor and block persistence mechanisms.

After metadata on the network traffic profile is gathered, analytics can be conducted to look for outliers, anomalous traffic, and other highly sophisticated methods of discovery. Network monitoring tools are not preventative in nature. Rather, they are intended to widely increase the SOC's visibility, facilitating detection, confirmation, or validation of suspicious actions. These tools are especially useful in replaying events that occurred as part of an attack to support network forensic activities. To block C2 traffic and other malicious network activity, consider using:

- ***DNS filtering:*** DNS providers will automatically block connections to known command and control servers (as well as DNS based persistence mechanisms), instead of allowing computers to leverage any authoritative DNS source.
- ***Egress filtering:*** Allowing the minimum necessary outbound protocols to restrict the ability of C2 traffic to blend into background.

6.L.C: Network Access Control (NAC)

NIST Framework Ref: PR.AC-5, PR.AC-6, PR.AC-4

NAC systems are engineered to automatically profile new IT assets that connect to network resources. Examples include wireless networks, wired networks, or VPN. NAC systems execute these controls in real time when the asset connects to the network. Common NAC use cases include:

- ***Discovering personal devices (i.e., BYOD) leveraged on the network.*** They can be configured to permit authorized BYOD devices to access the network or prohibit them entirely.
- ***Authenticating users associated with devices to confirm no authorized access of the network.***
- ***Quarantining connected devices that do not meet your organization's minimum standards.*** For example, they help ensure that the controls discussed in Cybersecurity Practice #2: Endpoint Protection Systems are in place on each asset.
- ***Implementing granular network segmentation.*** As devices are connected to the network, they can be automatically added to the correct VLAN to limit communication.
- ***Isolating affected devices from the rest of the network.*** This can take place during an incident (e.g., ransomware).
- ***Integrating with other systems (e.g., firewall, ITAM repository, SIEM).*** This provides greater visibility of connected devices.

As discussed in Cybersecurity Practice #5: IT Asset Management, ITAM repositories should be populated using your organization's standard procurement processes. That said, not all processes run perfectly. There are other ways that assets are integrated into an organization's environment, often due to human error or sidebar procurement channels that are not leveraged consistently.

Configuring your NAC solution to check against your ITAM enables assets to be profiled spontaneously, providing self-directed work streams to users. Use the following steps to achieve this type of configuration:

- Set up application programming interfaces between the NAC solution and the ITAM solution that enable read and write options.
- Query the ITAM database when an asset connects to the network. If the asset does not exist, present the user with a splash page.
- Determine whether the asset is owned by your organization or a personally owned device.
- Register the selection, conduct the NAC security scan, and publish the results in the ITAM.
- Execute IT general controls that reconcile assets that are out of compliance with standard asset management procedures. Such controls can include:
  - ensure that appropriate monitoring controls are in place;
  - register the asset with the right identifiers (asset IDs); and
  - update asset ownership based on actual human interaction.

These mechanisms are effective at providing visibility to the devices being used on the network, increasing the ITAM system's accuracy and consistency.

Key Mitigated Threats

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

Suggested Metrics

- ***The amount of time since last review of firewall and network segmentation configurations, reviewed on a weeky basis.*** The goal is to have a regular process to review and validate existing firewall and network settings, but also search for any undocumented firewalls or network segments.
- ***Number of assets on the network that have not been categorized, measured weekly.*** The goal is to establish a process to register and understand all assets on the network. After the baseline is complete, minimize the number of uncategorized assets.
- ***Number of organizationally owned assets discovered using NAC that were not previously categorized through asset management procedures, measured monthly.*** The goal is to monitor this lagging metric that measures effectiveness of the supply chain and IT operations processes. Increases in the number of organizationally owned assets not previously categorized indicates that standard processes are not being executed properly. Implement continuous improvement processes for IT operations.
- ***Percentage of assets that comply with security policies, measured weekly.*** The goal is to establish a baseline, then set stepwise goals to improve compliance over time. Ultimately, compliance percentage should range from 95 to 99 percent.
- ***Number of malicious files captured and secured with advanced networking tools (sandboxing), measured weekly.*** The goal is to capture all malicious files. An extended trend of no detected malicious files may indicate that sandboxing solutions are not working.
- ***Number of malicious C2 connections discovered and removed, measured weekly.*** The goal is a weekly report showing that all detected C2 connections are mitigated successfully.
- ***Number of approved servers/hosts in the DMZ compared to hosts in the DMZ, measured weekly.*** The goal is zero servers/hosts in the DMZ that are not understood. IT operations practices should be reviewed if servers are added that were not previously authorized.

Cybersecurity Practice #7: Vulnerability Management

Areas of Impact
PHI

Medium Sub-Practices
- **7.M.A** Host/Server Based Scanning
- **7.M.B** Web Application Scanning
- **7.M.C** System Placement and Data Classification
- **7.M.D** Patch Management, Configuration Management
- **7.M.E** Change Management

Large Sub-Practices
- **7.L.A** Penetration Testing
- **7.L.B** Vulnerability Remediation Planning
- **7.L.C** Attack Simulation

Key Threats Addressed
- Ransomware attacks
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that may affect patient safety

405(d) Resources
- Prescription Poster: Vulnerability Management

Organizations use vulnerability management for the proactive discovery of vulnerabilities. These processes enable your organization to classify, evaluate, prioritize, remediate, and mitigate the technical vulnerability footprint from the perspective of an attacker. The ability to mitigate vulnerabilities before a hacker discovers them gives your organization an operational advantage by providing time to address these vulnerabilities in a prioritized fashion.[58]

There are multiple types of vulnerability scanning. The most well-known methods are scans against servers (or hosts) and against web applications. These two scan types focus on different considerations.

Sub-Practices for Medium-Sized Organizations

7.M.A: Host/Server-Based Scanning

NIST Framework Ref: DE.CM-8

Vulnerability scanners are leveraged to identify weaknesses in operating systems or third-party applications that reside on a server. There are two scan options: unauthenticated and authenticated.

When performing unauthenticated scans, the scanner software does not have server privileges. The scan is performed through queries of the server based on ports that are active and present for network connectivity. Depending on the level of sophistication of the software scanner, each server is queried and checked for vulnerabilities. Scan results provide the perspective of an attacker who lacks server access. Vulnerabilities that rate high in this space should be mitigated first, as they are the most likely points at which a hacker could enter the server.

Authenticated scans are conducted by letting the vulnerability scanner log in to the server and query all active software with all running versions. The resulting vulnerability lists are usually compared against a database maintained by the scanner's vendor. Vulnerabilities are enumerated based on the known software version's disclosed issues.

Authenticated scanning provides a much higher degree of accuracy in enumerating vulnerabilities. It does not necessarily provide context that describes how the vulnerabilities might be exploited. Another

58 "Common Vulnerability Scoring System version 3.1: Specification Document," FIRST (Accessed June 2, 2022), https://www.first.org/cvss/specification-document.

advantage of the authenticated scan is that it will identify client-side vulnerabilities that exist on the server that may otherwise be difficult to discover (e.g., vulnerable versions of Java).

Most scanning systems can categorize vulnerabilities against the MITRE Common Vulnerability Scoring System (CVSS). The CVSS system helps organizations prioritize identified vulnerabilities, which enables development of a prioritized response. Version 3 of the CVSS system considers three factors: base score, temporal score, and environmental score. These factors, along with their sub-factors, are used to calculate vulnerabilities on a low-to-high scale range from 1 to 10. For more information, refer to the CVSS Specification Document.[59]

7.M.B: Web Application Scanning

NIST Framework Ref: DE.CM-8

Specialized vulnerability scanners interrogate a running web application to check for vulnerabilities in the application design. Most web applications run dynamic code, run atop a web server, interact with middleware, and connect to databases. If the web application is not coded securely, this architecture may enable unanticipated access to data or systems.

Common web application attack types include Structured Query Language (SQL) injection, cross-site scripting, and security misconfigurations. In these cases, attackers can:

- bypass web application security controls and pull data directly from the database
- steal an already authenticated cookie on a vulnerable website to get access
- exploit misconfigurations that can permit properly formatted commands or scripts to execute privileged content on the webserver itself

More information can be found on the Open Web Application Security Project's (OWASP) Top 10 website.[60]

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

7.M.C: System Placement and Data Classification

NIST Framework Ref: ID.RA-5

Organizations should apply **Cybersecurity Practice #4: Data Protection and Loss Prevention** and **Cybersecurity Practice #5: IT Asset Management** to understand IT assets and asset classifications. These cybersecurity practices answer the question, "How bad would it be if this asset were breached?" It is important to understand the exposure of each system in your environment. Organizations should apply **Cybersecurity Practice #6: Network Management** to determine the likelihood that a system can be compromised.

59 "Common Vulnerability Scoring System version 3.1: Specification Document," FIRST (Accessed June 2, 2022), https://www.first.org/cvss/specification-document.

60 "OWASP Top 10 - 2017: Ten Most Critical Web Application Security Risks," OWASP (2017), https://raw.githubusercontent.com/OWASP/Top10/master/2017/OWASP%20Top%2010-2017%20(en).pdf.

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

When establishing your vulnerability management program, consider the above practices for the identification of risks and their impacts. The following scenarios are cases where risks should be ranked higher, and remediation should be prioritized for vulnerabilities discovered:

- Internet-exposed, highly sensitive systems
- Systems necessary for life safety and patient safety
- Internet-exposed systems used for remote access
- Vendor-managed systems used for remote access

7.M.D: Patch Management, Configuration Management

NIST Framework Ref: PR.IP-1, PR.IP-3, PR.IP-12

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

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

Not all vulnerabilities are created equal. Some are easier to exploit than others. The National Vulnerability Database (NVD) has produced the CVSS, a standard measurement across all industries that normalizes and ranks the severity of a vulnerability.[61]

The more a vulnerability is exposed, the higher priority an organization will generally assign to mitigate it. Exposure may be a more critical variable than the potential impact to an asset, considering that hackers attempt to gain a foothold on organizational assets before conducting additional internal attacks. Another factor to consider is the level of active exploitability. A less-critical vulnerability may have an active threat against it. In such a case, an organization might want to consider proactively executing IR processes, organizing the response team, and quickly patching systems. The WannaCry exploit of 2017 is a classic example of an organization identifying an active threat and quickly implementing previously neglected patches.[62]

If your information systems are running end-of-life operating systems or software, associated vulnerabilities should be identified, and steps taken to bring these systems back to a supported state. This may include decommissioning systems that run on unsupported operating systems, which may require additional investments. Once systems are unsupported, it is usually impossible to apply security patches, potentially increasing your organization's risk.

Table 9 below provides general guidelines for planning remediation efforts based on criticalities.

61 "National Vulnerability Database: CVSS," NIST (Accessed September 24, 2018), https://nvd.nist.gov/vuln-metrics/cvss.
62 Brandon Vigliarolo, "Report: The IT Response to WannaCry," TechRepublic (July 25, 2017), https://www.techrepublic.com/article/report-the-it-response-to-wannacry/.

Table 9. Recommended Timeframes for Mitigating IT Vulnerabilities

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

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

In addition to conducting routine patch management activities, organizations should ensure that proper security configuration management activities are in place. Common vulnerabilities can be introduced in systems with insecure configurations. Examples of insecure configurations include permitting a file transfer protocol (FTP) server to allow anonymous login, making that login credential accessible to the internet, or failing to change default account passwords on applications. According to the 2020 Verizon Data Breach Report, in 2020, more than 40% of breaches analyzed were due to configuration errors. This failure has been trending upwards since 2015, where just less than 10% of breaches were due to configuration errors.[63] Organizations that follow **Cybersecurity Practice #2: Endpoint Protection Systems** (and expand these practices to their servers) will be positioned to minimize these issues.

7.M.E: Change Management

NIST Framework Ref: PR.IP-1, PR.IP-3, PR.IP-12

When changes are made to information systems, they should be conducted in a controlled manner to minimize disruption and outages made by human error. This process also allows for changes to be reviewed by a Change Advisory Board (CAB) to ensure the change would unwittingly expose the information system to an unacceptable vulnerability.

There are multiple types of changes that could occur in an organization. If following standard Information Technology Infrastructure Library (ITIL) practices, you could break these changes into **normal changes, standard changes** and **emergency changes.**

- ***Normal system change:*** This type of change is what most people think of when they go through the change process. This is a change that is made to an information system to enhance a feature, maintain the system, or otherwise update its services or configurations. These types of changes are planned out and prioritized.
- ***Standard system change:*** A subset of normal changes, standard changes are those that are recurring, routine and very specific. These changes have a standard operating procedure and have been conducted on a regular cadence, proven to cause minimal to no disruption as risks are known upfront. Standard changes offer flexibility to an organization once they have demonstrated to be stable. They can be pre-determined on a schedule, approved ahead of time by CAB so they do not need an approval every time, and otherwise permit standard flexibility.

63 2020 Data Breach Investigations Report (DBIR), Verizon (2020), https://www.verizon.com/business/resources/reports/dbir/2020/.

- ***Emergency system change:*** Emergency changes are changes that must happen immediately due to the unavailability of an information system or service, or perhaps due to an imminent outage. These types of changes need to occur immediately and without the standard approval process, but still must be controlled carefully. Emergency changes should be few and far between, measured, and require an after-action review for each emergency change that occurred.

All changes, regardless of their type, should be reviewed by a CAB. In some cases (i.e., standard changes), the CAB can approve the change to reoccur on a set schedule after it has been determined to be a stable and repeatable process. Other changes, such as emergency changes, might not go to the CAB prior to implementation, but must be discussed after the change has been made.

A CAB should have representation across your IT division. It is not just the responsibility of the person implementing the change to review it. Each department within your IT division should weigh in and review the impact of the change to ensure the stability of the digital environment. Cybersecurity teams should provide specialized insight to the change and make sure it will not introduce a vulnerability that is unacceptable to your organization.

A change ticket should capture, at a minimum, the following fields:

- ***Implementation Plan:*** The change must describe, with sufficient level of detail, the steps that will be taken to implement the change requested. The detail must be robust enough to allow for members of the CAB to make an informed decision. Consider placing a vulnerability scan as part of your testing plan to ensure no new vulnerabilities were introduced. These vulnerability scans should be done within the test environment and made prior to the change being implemented into production.
- ***Testing Plan:*** The change must incorporate a plan on how to test that the change was successful. Every change should have a test plan to validate its effectiveness.
- ***Back-out Plan:*** Not all changes are successful, so you must plan for how you will reverse the change and bring the information system back up to its current state. No change should take place without an approved and tested Back-out Plan.
- ***Communication Plan:*** Changes should include the mechanisms by which you will communicate how the change was completed, new features being released, and new adjustments that are necessary by your organization to adjust to the change that was introduced.

Sub-Practices for Large Organizations

7.L.A: Penetration Testing

NIST Framework Ref: ID.RA-1, PR.IP-12, DE.CM-8, RS.AN-5

Penetration testing is an important tool that layers additional protections when added to vulnerability scanning. Penetration testing is sometimes called “red-teaming”. The goal is to actively exploit your own environment before malicious actors do.

Penetration tests involve more than simply conducting vulnerability scans and attempting to exploit the findings. A proper penetration test should mimic the same attack methodologies that are deployed by the adversaries. CIS Control #18 tells us penetration testing involves mimicking the actions of computer

attackers to identify vulnerabilities in a target organization and exploiting them to determine what kind of access an attacker can gain. Penetration tests typically provide a deeper analysis of security flaws than a vulnerability assessment.[64]

Penetration tests should blend client-based, internet-based, web application–based, and wireless-based attacks. When selecting a testing method, consider the types of attacks that might occur most frequently against your organization. With these scenarios, you can test the resiliency of your cybersecurity program.

Penetration tests can be run internally by qualified individuals, or they can be run by external partners. No matter who will conduct the test, proper authority to perform the test must be documented. This must clearly define the scope of the assets that may be tested, the methods that may be deployed, and the timing for conducting the tests. Assets and methods not permitted should be clearly articulated. This documentation is especially important if internal staff will conduct the test, and documentation may be necessary to comply with legal and HR obligations.

Multiple variations of penetration tests that can be conducted. Review each of the factors in **Table 10** below and select what works best for your organization.

Table 10. Factors for Consideration in Penetration Test Planning

Factor	Options	Description
Type	1. ***White box:*** Tester is permitted to know all aspects of the target 2. ***Grey box:*** Tester is permitted to know some aspects of the target 3. ***Black box:*** Tester is not permitted to know any details of the target	Depending on the type of test you want to conduct, it might be useful for the tester to know some details of the target or organization. Such knowledge might reduce the effort of common reconnaissance activities, such as finding phishing target email addresses or discovering all vulnerabilities on externally facing servers.
Resources	1. ***External expert:*** A subject matter expert (SME) who specializes in the specific methodologies you wish to deploy 2. ***Internal expert:*** A SME on an internal team who has context to the environment	Both types of resource can be useful. The benefit of using internal staff is that they understand the technical nuances of your environment. In some cases, targeted tests requiring specialized skillsets might be desired. External experts are useful in these cases, or when internal resources are committed to other activities.

64 "CIS Critical Security Control 18: Penetration Testing," Center for Internet Security (Accessed September 24, 2018), https://www.cisecurity.org/controls/penetration-testing.

Factor	Options	Description
Methods	1. ***Social engineering:*** Attacks geared towards "tricking the human" 2. ***Web application:*** Attacks centered on attacking web application infrastructure 3. ***Host based:*** Attacks focused on attacking host infrastructure, inclusive of servers, or endpoints 4. ***Client based:*** Attacks centered on attacking the client, such as laptops or desktops (usually bypassing perimeter protections) 5. ***Network based:*** Attacks against the network infrastructure itself, such as physical connections or wireless attacks 6. ***Privileged escalation:*** Once a foothold has been made, conducting secondary attacks to further escalate privileges for more lateral movement	Many methods exist; those listed here are the most common. These methods can be combined, based on the type of attack you are looking to carry out. For example, if you want to see whether it is possible for an external attacker to gain access to your EMR, you might use social engineering, client-based, and privileged- escalation attacks. The goal of each of these attacks is to discover a user with sensitive EMR access, compromise the user's credentials, and get remote access to the environment to be able to log in to the EMR with those credentials.
Targets	1. ***Data:*** Discover and exfiltrate sensitive data to test data security controls 2. ***IT assets:*** Compromise IT assets, such as servers or endpoints, to test system security controls 3. ***People:*** Compromise individuals to test educational controls 4. ***Medical technologies:*** Determine how vulnerable your organization is to attacks against medical devices. For additional clarity on actions to be taken when vulnerabilities are identified in medical devices, please refer to Cybersecurity Practice #9: Network Connected Medical Devices 5. ***Infrastructure:*** Determine how vulnerable your organization is to digital extortion attacks, such as ransomware outbreaks	Each test conducted should have different targets and goals in mind. In some cases, you might want to test how susceptible your user population is to phishing attacks; in that case you will set "People" as the target. In other cases, you might want to understand how vulnerable your organization is to a ransomware attacks; in that case, you might select "IT Assets" and "Infrastructure" as your targets

7.L.B: Vulnerability Remediation Planning

NIST Framework Ref: PR.IP-12

It is important to classify and prioritize vulnerabilities that remain after completion of standard patch management practices. Typically, these remaining vulnerabilities are issues that cannot be mitigated

with a patch. They may require system configuration changes, code updates, or perhaps even a full-blown version upgrade. The process of resolving these vulnerabilities tends to be more time-consuming and complex.

Like risk management activities, remediation efforts should be prioritized to resolve identified vulnerabilities. The most common practice is to first patch identified vulnerabilities and then rescan the system to validate that those vulnerabilities are closed. Most vulnerability scanning systems can track the opening, closure, and reopening of vulnerabilities over time. It is highly encouraged to track these metrics.

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

- ***Plan owner:*** The single individual accountable for ensuring that the vulnerabilities are addressed. It is important to assign remediation plans to a single owner, otherwise they are likely to stall due to lack of leadership.
- ***Plan:*** A full description of the remediation plan to be completed. The remediation plan owner and the cybersecurity office should develop this plan. Once the plan is approved, execution tasks can be started.
- ***Stakeholders:*** The individuals responsible for completing tasks in the remediation plan or organizing others who will complete tasks. Stakeholders may include those who need to be informed of remediation activities and others who complete the work.
- ***Dates:*** Major milestone dates and remediation plan due dates must be captured on the remediation plan. The remediation plan owner must commit to these dates.
- ***Status:*** Periodically, the plan should be updated to remain current. Updating generally occurs between once per week and once per month. The remediation plan owner may be accountable for providing status updates.

After a remediation plan is completed, your organization's cybersecurity office should implement a monitoring process. This monitoring process may include all remediation plans in progress and current activities. The security office may provide support to activities that are behind schedule. Consider implementing a monitoring process once per week to maintain momentum.

7.L.C: Attack Simulation

NIST Framework Ref: DE.DP

The last time you want to find out about a vulnerability is during a cyber-attack. Attack simulations, also known as threat emulation exercises, can help you expose your known and unknown vulnerabilities and stress-tests your organization's cybersecurity. The purpose of a threat emulation exercise is to closely mimic the tactics, techniques, and procedures (TTPs) of real-world adversaries and determine how they might be leveraged against your organization. There are a few important considerations that organizations should consider when building a threat emulation exercise.

First and foremost, an organization needs to understand their own threat profile. Each organization has a unique threat profile that is comprised of their internal mix of people, and processes, technologies. This task requires an organization to develop a comprehensive understanding of their systems, applications, networks, online presence, workforce, and the threat actors that focus on their industry. There are open-sourced resources available to assist organizations in collecting this information. This task can be aligned

to the reconnaissance and Open-Source Intelligence (OSINT) activities that normally happen as part of a red team or penetration engagement.

Second, an organization will need to determine which framework and methodology to be used to conduct the exercise. This will be the basis for how the specific parameters of the exercise will be carried out. Additionally, the metrics of the exercise should also be based on the framework and methodology.

Lastly, an organization needs to determine the goals of the exercise. Once the goals are set your organization can begin to build a threat profile. This includes identifying the specific TTPs of the "attacker", identify targets, develop real world scenarios, and determine the "attack" infrastructure needed to achieve the goals they set for the threat emulation exercise.

When it comes to building a threat emulation exercise there are three phases that all the activities fall under: **Get in, Stay in** and **Act.** The goals of these phases include activities such as:

- Acquiring elevated access to a domain controller or other critical servers.
- Accessing a client data repository, intellectual property, and/or application data.
- Creating a new cloud instance in the client's on-premises or cloud infrastructure.
- Gaining access to and leaving a physical note in a datacenter or other restricted area.
- Posting a comment into production source code.
- Obtaining physical access to data or devices and accessing the ability to remove the data/device.
- Keeping a low profile (i.e., not generating alerts that will raise suspicions or having the attack infrastructure get burned).

For additional guidance, there are several resources that offer options around attack simulation training.

The **Identify, Mitigate, and Recover (IMR)** incident response curriculum, developed by the Cybersecurity and Infrastructure Security Agency (CISA), provides a range of training offerings for beginner, intermediate, and advanced cyber professionals. It encompasses basic cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time IR scenarios, and hands-on cyber range training courses for IR practitioners. Course types include awareness webinars, Cyber Range Training, Cyber Range Challenges, and Observe the Attack.[65]

- **Cyber Range Training** courses are hands-on labs designed to teach the basics of network investigation and defense. They are accessible to new cybersecurity workers who may lack hands-on skill practice, but some theoretical understanding of cybersecurity and IR enhances the value of the instruction.
- **Cyber Range Challenges** are hands-on IR scenarios designed for experienced practitioners. Students are asked to complete class profiles to summarize their skill and experience, and teams are balanced so that newer incident responders can learn from and work with more experienced professionals. These are critical thinking and problem-solving challenges as much as they are a test of investigation and network defense skills.
- The **Observe the Attack** series red/blue team demonstration events are ideal for those who supervise, manage, support, or facilitate incident or crisis response.

The Department of Homeland Security (DHS), the Department of Health and Human Services (HHS), and the National Health Information Sharing and Analysis Center (NH-ISAC) developed a Cyber Tabletop

65 "Incident Response Training," CISA (Accessed May 26, 2022), https://www.cisa.gov/incident-response-training#.

Exercise for the Healthcare Industry intended to assist healthcare industry organizations in planning and organizing a cyber tabletop exercise.[66]

CyberStorm, CISA's biennial exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. The exercise series brings together the public and private sectors to simulate discovery of and response to a significant cyber incident impacting the Nation's critical infrastructure. CyberStorm exercises are part of CISA's ongoing efforts to assess and strengthen cyber preparedness and examine incident response processes.[67]

An additional resource is the MITRE ATT&CK® framework. This is an open and publicly available resource for understanding, planning, and designing attack simulations throughout the attack lifecycle. Per their website: "MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."[68]

Key Mitigated Threats

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

Suggested Metrics

- ***Stacked aggregate of vulnerabilities in DMZ measured by month, with vulnerabilities categorized using CVSS categories (Critical, High, Medium, Low, None) and plotted as a simple stacked bar.*** The goal is to mitigate the most severe vulnerabilities first, through patching and configuration management. Of the remaining vulnerabilities, the most critical should be mitigated within 30 days. The total number of vulnerabilities should be reduced over time.
- ***Stacked aggregate of vulnerabilities in data center measured by month, with vulnerabilities categorized using CVSS scores and plotted as a simple stacked bar.*** The goal is to mitigate the most severe vulnerabilities first, through patching and configuration management. The total number of vulnerabilities should be reduced over time.
- ***Number of unmitigated new vulnerabilities introduced into the environment, measured on a weekly basis.*** The goal is to keep the number of new vulnerabilities as low as possible, defined by your organization's level of risk tolerance.

66 "DHS Cyber Tabletop Exercise (TTX) for the Healthcare Industry [Exercise Materials]," Homeland Security Digital Library (2013), https://www.hsdl.org/?abstract&did=789781.
67 "Cyber Storm: Securing Cyber Space," CISA (Accessed May 26, 2022), https://www.cisa.gov/cyber-storm-securing-cyber-space.
68 MITRE ATT&CK® (Accessed May 26, 2022), https://attack.mitre.org/.

Cybersecurity Practice #8: Security Operations Center and Incident Response

Areas of Impact
PHI

Medium Sub-Practices
8.M.A Security Operations Center
8.M.B Incident Response
8.M.C Information Sharing and ISACs/ISAOs

Large Sub-Practices
8.L.A Advanced Security Operations Center
8.L.B Advanced Information Sharing
8.L.C Incident Response Orchestration
8.L.D Baseline Network Traffic
8.L.E User Behavior Analytics
8.L.F Deception Technologies

Key Threats Addressed
- Social engineering
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that can affect patient safety

405(d) Resources
- Prescription Poster: 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, implementing the cybersecurity 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.

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

Maintaining detection and response capabilities requires establishing an IR program and an SOC to manage the IR, along with security engineering that enhances an organization's ability to detect and respond to cyber-attacks.

Sub-Practices for Medium-Sized Organizations

8.M.A: Security Operations Center (SOC)

NIST Framework Ref: RS.RP

A SOC is an organizational structure that leverages cybersecurity frameworks, people, tools, and processes to provide dedicated cybersecurity operations. SOCs are the areas within an organization that dedicate 100 percent of their time to cybersecurity prevention, detection, or response capabilities, providing the execution arm of cybersecurity IR. A SOC is generally segmented into three main functions, depending on your organization's level of maturity. These functions are as follows:

- ***Operations:*** The process of managing and maintaining the cybersecurity tools within the SOC. This is sometimes referred to as 'keeping the lights on'. 'Keeping the lights on' generally means monitoring critical cybersecurity systems to ensure that they operate at agreed-upon performance levels.
- ***Threat intelligence:*** A specific function that focuses entirely on how to discover cybersecurity threats that may be relevant to your organization, along with the means and methods these threats may use to infiltrate your organization. This function focuses on the threat actors themselves, the tools they leverage, and the digital signatures they leave in the process of conducting their activities. Upon establishing these digital footprints, sometimes called IOCs, engineering teams can integrate IOC patterns into cybersecurity systems. IR plays can be set to execute when the IOCs are activated.
- ***Incident response:*** The process of conducting a structured and consistent response to any IR plays that have been created. The goal of this function is to:
  - validate an IR process that has been triggered;
  - contain any successful cybersecurity attacks to your organization;
  - eliminate the threat from the environment;
  - recover systems or data that might have been affected by the attack; and
  - ensure that any attack vectors that were exploited are well understood and fed back to the security engineering teams for future prevention or enhanced detection capabilities, further minimizing the impacts of those vectors.

Supporting the SOC is the cybersecurity engineering function. This team builds new cybersecurity capabilities into the existing toolsets in an environment. Examples include building new alerts within a SIEM system, establishing new log sources for log management systems, establishing new analytics patterns for detection, or simply implementing new cybersecurity systems to add capabilities into the environment. Additionally, the cybersecurity engineering team may take the lessons learned from the SOC to improve your organization's preventative and detective controls.

It is critical to create a continuous feedback loop between your SOC and cybersecurity engineering teams, so your organization continues to learn and grow based on the actual success of threats and threat actors.

As SOCs are developed, a core concept is to ensure that IR teams and handlers apply consistent methods to execute response practices. SOCs and IR teams should establish playbooks, also known as runbooks, that describe existing detection mechanisms and the procedures to be followed if the mechanisms are triggered. For each detection, the triggered process may be referred to as a play, like plays that football teams maintain in their playbooks.

Examples of plays that might be found in an IR playbook are provided below in **Table 11**. The table provides high-level play details, including what the play 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 required. Information on how to configure this information can be found in multiple publications.[69]

69 David Swift, *Successful SIEM and Log Management Strategies for Audit and Compliance*, The SANS Institute (November 9, 2010), https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log- management-strategies-audit-compliance-33528.

Table 11. Example Incident Response Plays for IR Playbooks

Play Category	Play	Description	Source Data
Reconnaissance	Vulnerability scanning sweep of DMZ.	Large numbers of vulnerabilities are scanned across the DMZ spectrum. Could involve scanning a single server over multiple ports or scanning multiple servers on a single port.	• Server list in DMZ • Intrusion detection system (IDS) or intrusion prevention system (IPS) logs configured to detect vulnerability scanning • Firewall logs • Netflow data
Reconnaissance	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 (e.g., IOC).	• IOC list from threat-sharing sources (e.g., ISACs) • IDS/IPS logs • Firewall logs • Netflow data
Reconnaissance	Successful access from known malicious IPs.	Successful authentications from known malicious IP addresses. Authentications through standard remote access channels (e.g., VPNs, virtual terminals, jump boxes, or other mechanisms).	• Authentication logs • Firewall logs • IOC list from threat-sharing sources (e.g., ISACs)
Reconnaissance	Internal attacks from third-party VPNs.	Detection of attacks coming through partnering third-party VPN connections (e.g., organizations that provide building automation).	• Firewall logs (from segmented networks) • IDS/IPS logs • Authentication log • EDR logs
Exploitation	Phishing attacks successfully delivered to users.	Detection of phishing attacks by IT systems, or users reporting phishing attacks. Contain the issue by blocking URLs provided, proactively resetting passwords for users that clicked, and conducting AV scans against endpoints where malicious attachments were opened.	• Email protection systems • Firewall logs • Web proxy logs • Endpoint AV management logs • EDR logs

Play Category	Play	Description	Source Data
Exploitation	Successful ransomware attack	Detection of ransomware attacks that occur inside your organization. These may be small outbreaks or larger issues. Consider: • Setting up detection alerts for indicators of known ransomware (AV, threat feeds, etc.) • Setting up detection alerts for symptoms of ransomware attacks (such as large IOPs on file systems, encryption of large amounts of files, user experience issues) • Determining severity; lower severity issues can be dealt with operationally; high severity issues should instantiate the Cybersecurity Incident Response Team (CIRT) • Containing and responding accordingly • Recovering through backups (do not simply clean a system with an AV scanner, but rather rebuild and reimage)	• File system logs • Endpoint AV management logs • Firewall logs • Web proxy logs • Threat feeds • Email security logs • EDR logs
Persistence	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.	• Logs from local servers • EDR logs
Persistence	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.	• Critical server lists • Known process baselines • Logs from server task or scheduled job management • URL filtering logs by server • EDR logs

Play Category	Play	Description	Source Data
Privilege Escalation	Privileged account brute force success	Large number of invalid login attempts followed by a successful login to a known privileged account.	• Privileged account list • Authentication logs (e.g., active directory, servers)
Privilege Escalation	Default account password guessing	Large number of invalid login attempts followed by a successful login to a known default user account.	• Default account list • Authentication logs (e.g., active directory, servers)
Privilege Escalation	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.	• Service account list • Authentication logs (active directory, servers) • EDR logs
Data Exfiltration	Data transfer	Detection of data transfers occurring outside of your organization from servers that normally do not conduct such activities. Must normalize/baseline server network behavior and detect anomalous activities off baseline.	• Netflow data, or firewall traffic profile data • List of permitted remote storage sites (e.g., box)
Data Exfiltration	Lost/stolen device	User reports that a device was lost or stolen from their possession. Conduct standard actions to immediately reduce the impact, including, at minimum: • Issuing a device wipe and remote lock • Checking for last encryption status in control systems • Executing CIRT if device is unencrypted	• Users • Mobile device management systems • Endpoint configuration systems

In each of the cases outlined in Table 11, 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, rule matching, and analytics capabilities to specific events in the logs to call out potential incidents of interest. These specialized systems are referred to as SIEM systems.

Besides cybersecurity specific responses, consideration should be given to potential incidents that have a physical component as well. For example, ransomware could impact the controller for a prescription drug dispenser, digital lock, etc. In these cases, IR needs to consider how critical functions will need to be maintained and restored while the investigation and containment activities are being performed.

8.M.B: Incident Response

NIST Framework Ref: PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC

A basic and important function of a cybersecurity organization is the IR process. The IR process provides your organization with standardized procedures to respond to cyber-attacks. The attack may be as simple as an attempted phishing attack against users, or a highly sophisticated extortion attack that shuts down digital operations. In both cases, from minimal to significant impact, the organized manner of an IR is critical to managing these threats.

Large-Scale Response

In parallel with establishing a response process inside of a SOC, it's also advisable to create a large-scale cybersecurity incident response plan in coordination with your emergency management and business continuity teams. This large-scale response is designed to allow for the continuity of operations of the business during a cyber-attack. Other useful tools in response planning includes leveraging the ONC's SAFER guides, and specifically their downtime procedures recommendations.[70] Another useful tool is CISA's Table-Top Exercise (TTX) scenarios, which are helpful when exercising and testing your large-scale plans.[71]

This section does not outline all the elements of covering a large-scale response, but rather takes elements from NIST's Computer Security Incident Handling Guide and outlines some key roles and responsibilities that can be tied into an organization's larger Incident Command System.[72]

In addition to these roles and responsibilities, it is advisable for organizations to have established disaster recovery plans (DRPs) as well as downtime procedures, in the event of a large-scale disruption. Generally, a structured IR process contains the following segments:

- ***Preparation:*** Before you respond to a cybersecurity incident, it is important to have policies, processes, and procedures in place, including the following components:
- ***IR policy:*** A policy that defines the categorization and severity of incidents, the stakeholders involved in IR, the roles and responsibilities of each person, the entry criteria when a security incident occurs, and the person who oversees IR plays. The stakeholders that may play a role in IR could range from the standard blocking and tackling personnel in IT operations to non-IT related professionals in such diverse areas like privacy, legal, marketing, and public affairs for high-impact incidents. A template IR policy is provided in Appendix G, Resources and Templates.
- ***Cybersecurity incident response team (CIRT):*** A pre-formed and "on the ready" group that knows how to navigate issues when critical- or high-severity security incidents arise. This team develops and manages your organization's response. CIRTs are formed in the HPH sector when potential data breaches occur, and your organization must manage the potential breach. It is important to identify the incident commander, the most senior official who will oversee managing cybersecurity incidents. The incident commander is usually the Chief Information Security Officer (CISO) or equivalent. Note

70 "SAFER Guide: Contingency Planning," ONC HealthIT (July 2016), https://www.healthit.gov/sites/default/files/safer/guides/safer_contingency_planning.pdf.

71 "CISA Tabletop Exercises Packages," CISA (Accessed May 31, 2022), https://www.cisa.gov/cisa-tabletop-exercises-packages.

72 Paul Cichonski et al., *NIST Special Publication 800-61r2: Computer Security Incident Handling Guide*, NIST (August 2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

that the incident commander should not dive into the technical weeds of the incident, rather keep the various teams organized and focus on their objectives. Table 12 below describes the teams that may be involved in resolving a critical security incident and potential breach.

Table 12. Roles and Responsibilities for an Organizational CIRT

Role	Responsibilities
Incident Commander	Individual who will oversee the cybersecurity incident and interact with other stakeholders in the table.
Executive/Senior Leadership	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 lifecycle of a significant cybersecurity incident.
Cybersecurity Teams	Teams comprised of cybersecurity experts who understand attacks, vulnerabilities, and the methods by which threat vectors are exploited. They provide technical knowledge and detail to technical teams and execute procedures in the playbook.
Technical Teams	Teams comprising SMEs for the technologies that have been compromised and who 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.
Legal Teams	Teams comprised of attorneys in your general counsel (internal or external) that help manage the incident under privilege as well as consult on regulatory expectations.
Emergency Management	With the potential for cybersecurity incidents to have an operational and patient safety impact, clinical emergency management function should be connected to the CIRT. In some organizations the CIRT may take direction from emergency management, in others it may be reversed. This relationship should be determined prior to an incident.
Public Affairs/ Marketing and Communications	Individuals who manage external and internal communications to deliver a consistent voice and message in the event of a high-visibility cybersecurity incident. This team is crucial in managing the reputation of your organization.
Privacy and Compliance Team	Teams responsible for understanding the full extent of a cybersecurity incident that involves PHI/PII. This includes conducting a breach assessment for compliance with federal/state reporting and notification requirements.
Other external teams	Supporting an incident may require specialized forensics teams, law enforcement, representatives from CISA or HC3, and other teams to support the investigation and remediation of the incident. Consider proactive notification to both CISA and the H-ISAC as part of your IR playbook. Both notification channels can provide defensive measures to other HPH organizations based on the context of your security incident. Sharing of IOCs to either CISA or H-ISAC is protected under the Cybersecurity Act of 2015. Regulators are not permitted to use any shared information as part of their enforcement actions.

Security Operations Center Response

The response inside of a SOC is more focused and technical in its nature. The goal of the SOC is to identify any bad actors that have compromised your organization's environment and evict them before wide-spread damage can occur. Typical procedures and processes to consider for the establishment and running of your SOC are as follows:

- ***Playbook/Runbook:*** As mentioned previously, this is a document that contains standard operating procedures to respond to different types of cyber-attacks. 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 attack types is a distinct play in an organization's cybersecurity playbook. For each play, it is 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 attack has its own unique characteristics and nuances, your procedures should follow the steps provided in your playbook for that type of attack. For your reference, a template playbook is provided in Appendix G, Resources and Templates. Cybersecurity incidents may have a broader organizational impact. Playbooks should tie to organization-wide emergency management plans (e.g., downtime procedures). It is important to understand the potential ramification of a cybersecurity incident (e.g., ransomware) may have on clinical technology and have alignment between the responses. Care should also be taken to ensure paper documentation (e.g., playbook, phone lists, prescription pads, paper charts) are up to date and available if a cyber incident has rendered those systems unavailable.
- ***Tools and technologies:*** After you establish your policies, CIRTS, and playbook, the next level of improvement is to configure your tools and technologies to streamline the execution of your plays. Streamlining connects your IR processes to your security engineering processes to create a continual feedback loop, which is essential to becoming a resilient organization.

A typical SOC response includes five key processes:

- ***Identification:*** The first response to any cyber-attack is to understand the scope and extent of the attack. The identification phase of an attack response involves 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 that targets a small user set and 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.
  The identification exercise in a phishing process may be as simple as:
  - Receiving notification from your user base or through your own detection systems of a phishing attack or campaign.
  - Profiling and understanding the extent and scope of the phishing attack. Determining its level of sophistication and intent.
  - Conducting a basic investigation to determine whether links were clicked, or malware was delivered.

Once a potential attack is identified, organizations should connect with their cyber liability insurance carrier (as required by their policy of insurance). The insurance policy will specify the timeliness and procedures for notification to qualify as a covered claim. Many insurance carriers designate panels of service providers that provide services covered under the policy. It is important to use these panel of forensic firms, legal counsel, or breach notification services to receive the benefits under the insurance policy. Ideally, organizations should identify and establish a relationship with their preferred vendor from the insurers list of panel providers prior to needing the services.

- ***Containment:*** After the extent and scope of the attack is understood, the next step is to contain the attack before it penetrates further into your organization. This phase is critical and must not be overlooked; less mature organizations may start fixing the vulnerability that was exploited before they stop the attack. Your playbook should include containment procedures for each play. In some cases, containment may require shutting down information systems to prevent them from being compromised if they are vulnerable to the attack.
  A containment exercise for a phishing attack may be as simple as the following:
  - Shunning/preventing any remote access C2 traffic that might be established as part of the attack.
  - Changing credentials proactively for users who clicked to open a credential-theft phishing campaign.
- ***Eradication:*** This phase of your response focuses your IR effort on eliminating all traces of the attack, including the attack foothold. This step includes:
  - Identification of all emails that were delivered to your user base
  - Removal of these emails from mailboxes of the same user base
  - Reimaging of endpoints where malicious binaries or malware were downloaded to ensure no foothold exists
- ***Recovery:*** After the threat is neutralized and all malicious activity is removed from your organization's systems, you must determine whether to reactivate the compromised technology. In most cases, the answer to this question will be "of course," as these technologies fulfill a larger purpose in your organization. In cases where legacy technologies were compromised, however, it might not be worth the effort and investment to bring them back online.
  In either case, the process to restore technical capability in your organization is as important as the process to remove the threats and malicious activities in your systems. As you restore functionality, shut down the vectors that made the attack successful. This may be done by patching an exploited vulnerability or rebuilding an entire system to leverage hardening processes such as those identified in **Cybersecurity Practice #2: Endpoint Protection Systems**.
- ***Lessons Learned/After-Action Report:*** Arguably, the most important stage of your IR process is a full debrief with your IR teams after the attack is mitigated and systems are returned to full functionality. This debrief should profile the successful attack vectors and identify short-term adjustments to introduce enhanced prevention, detection, or response capabilities, as well as long-term strategic elements that require more detailed planning.
  For example, if your organization falls prey to a sophisticated phishing attack that results in the theft of multiple credentials, followed by the installation of remote-access tools, a multifaceted set of mechanisms may be considered for short-term and long-term improvement.

Examples may include the following:

- Refining a play within the playbook that did not execute as efficiently as possible. Timeliness is one of the most critical aspects of any response; taking too long to ramp up your IR playbook increases your exposure to a successful attack.
- Refining and expanding logging capabilities to detect threats more quickly. Implementing these capabilities into your SIEMs. Delve into the specific patterns of the attack as much as possible for lessons learned.
- Sharing attack details and information with participating ISACs and ISAOs. This helps other organizations to prevent validated and vetted threats. It provides greater credence to the intelligence and increases resiliency of the sector.
- Leveraging advanced analytics-based phishing protection tools such as "click protection" or "attachment sandboxing." These usually require investment and budget allocation by your organization.
- Refocusing and prioritizing resources to build out greater capabilities to identify and respond to phishing attacks. From a strategic perspective, it is important to refocus your resources in response to a threat that is ramping up against your organization.

A feedback loop from your IR processes back into engineering and operations is a key to becoming a resilient organization. This type of feedback loop enhances an organization's cybersecurity capabilities over time and organically, while increasing flexibility and agility in IR response processes.

To read an example case of a mock attack, consider the SANS whitepaper "A Practical Example of Incident Response to a Network Based Attack."[73] Further details associated with IR playbooks can be found in the SANS whitepaper, "Incident Handler's Handbook."[74]

Ransomware-Specific Response

For those specifically concerned about ransomware prevention and response, another useful reference is CISA's Stop Ransomware website.[75] This site outlines several resources, alerts, and methods for interfacing with the federal government in event you become a victim to this type of attack. A few resources to consider on this site include:

- The MS-ISAC Joint Ransomware Guide, which outlines preventative and responsive techniques for combating ransomware[76]
- The CISA Bad Practices, a list of known practices that are considered risky and highly leveraged by bad actors[77]
- A series of training materials for training technical and non-technical users
- A series of freely available services provided by CISA to protect critical infrastructure, such as phishing simulations, vulnerability assessments, and penetration assessments

73 Gordon Fraser, "A Practical Example of Incident Response to a Network Based Attack," The SANS Institute (August 16, 2017), https://www.sans.org/white-papers/37920/.
74 Patrick Kral, "The Incident Handlers Handbook," The SANS Institute. February 21, 2012 https://www.sans.org/white-papers/33901/.
75 StopRansomware.gov, CISA (Accessed May 31, 2022), https://www.cisa.gov/stopransomware.
76 "Ransomware Guide," MS-ISAC and CISA (September 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.
77 "Bad Practices," CISA (Accessed June 2, 2022), https://www.cisa.gov/BadPractices.

It is highly recommended to contact the FBI or CISA if you have been a victim of a ransomware attack. The FBI and CISA both recommend strongly against paying any ransoms, as ransom payments continue to fund the bad actors and criminal enterprises. If your organization decides to pay the ransom, although extremely discouraged, it is highly advisable to do so under the guidance of CISA, the FBI, and/or legal counsel. As this is an ever-evolving situation, you will want to ensure you have the proper legal authorizations in place if a payment is deemed necessary.

Contact the local FBI office closest to you.[78]

Contact CISA directly at: report@cisa.gov or (888) 282-0870.

8.M.C: Information Sharing and ISACs/ISAOs

NIST Framework Ref: ID.RA-2

Security engineering and operations activities tend to focus on preventing cyber-attacks and building out systems that enable streamlined execution of IR functions. However, not all attacks are equal. Some are perpetrated by "script kiddies," relatively unskilled individuals who use crude scripts and programs to attempt to exploit whatever organization they can. Some threat actors are highly competent hackers backed by substantial resources and a strong desire to gain entry to your specific organization. Differentiating these types of attacks falls under the discipline of threat intelligence.

By banding together with peer organizations, ISACs and ISAOs establish and maintain channels for sharing cyber intelligence. The means to share this intelligence vary in sophistication; most mature ISACs leverage common standards and formats, such as STIX and TAXII, as well as flash reports that profile current attacks. ISAC or ISAO participation offers substantial value to an organization. It connects your cybersecurity professionals with the greater cybersecurity community.

As with all disciplines, there are multiple levels of maturity within the threat intelligence discipline. The most basic sharing of threat intelligence involves consuming lists of "vetted bad IP addresses" or "feeds" from commodity sources. These sources have been well curated to identify where the loudest and most obvious attack space resides. Organizations can use multiple means to consume these feeds, but the most usual process is to subscribe to a daily download of IOCs.

Health-ISAC (H-ISAC)

The largest ISAC for the Health and Public Health Industry is H-ISAC. H-ISAC is a member driven organization that offers an array of cyber threat intelligence and hygiene services.[79] Members share threat intelligence, IOCs and TTPs in both an automated and manual method. Your organization also produces advisories for the whole HPH sector, regardless of membership, as well as more specialized analysis provided to members. H-ISAC is connected to other sectors' ISACs as well as maintains information sharing protocols with the federal government.

78 "Field Offices," FBI (Accessed May 31, 2022), https://www.fbi.gov/contact-us/field-offices.
79 Health-ISAC (H-ISAC), https://h-isac.org/.

Other ISAOs and ISACs

Members of the HPH Sector can join other ISACs or get involved in smaller ISAOs. The Population Health ISAC (PH-ISAC) is a member driven organization and focuses on community health centers, behavior health, rural and community hospitals and provides proactive services for these systems.[80] The IT-ISAC focuses on all IT cross sector. Other organizations can create their own ISAOs, the terms of which are dictated under the ISAO Standard Organization.[81]

CISA Cyber Hygiene Services

CISA also provides a wide variety of free services to Critical Infrastructure, referred to as "CyHy."[82] The services available are as follows:

- ***Vulnerability Scanning:*** Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- ***Web Application Scanning:*** Evaluates known and discovered publicly accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- ***Phishing Campaign Assessment:*** Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
- ***Remote Penetration Test:*** Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open-source information.

To request any of these services, send an email to vulnerability_info@cisa.dhs.gov with the subject line of "Requesting Cyber Hygiene Services."

Sub-Practices for Large Organizations

8.L.A: Advanced Security Operations Center

NIST Framework Ref: N/A

In addition to the basic SOC practices already discussed, an organization's move to more advanced security management should include expanding its SOC to be staffed and monitored 24 hours per day, 7 days per week, 365 days per year (24x7x365). This is strongly recommended for medium and large organizations, given that cybersecurity incidents may happen any time of day. Delays between the initial incident and response may result in a worse outcome.

The models described below can account be used in whole or part, based on the types of technologies and processes running within your SOC. For example, some organizations might elect to outsource Tier 1 playbook monitoring of their SIEM and EDR tools but keep Tier 2 escalations in-house. Other

80 "CommHIT Information Sharing & Analysis Centers (ISACs)," CommunityHealth IT (Accessed May 31, 2022), https://www.communityhealthit.org/isacs/.
81 ISAO Standards Organization, https://www.isao.org/.
82 "Cyber Hygiene Services," CISA (Accessed June 2, 2022), https://www.cisa.gov/cyber-hygiene-services.

organizations might elect to keep all SIEM management in-house but elect to use EDR monitoring in an outsourced manner. The models selected should be based on the best risk management and financial model for your organization. There are multiple methods to achieve this model, all of which have benefits and constraints. Some of these methods are described below:

- ***Fully outsourced:*** All SOC and threat actions are outsourced to a third-party provider who has the required infrastructure, staff, and capabilities. Such providers normally install sensors on your networks and use them to collect necessary log information that enriches detection and response activities. SOC analysts actively look for threats and provide your internal IR personnel with specific actions to take when threats are identified.
  This model has the advantage of scale and capability. It is difficult to hire and retain qualified security analysts to provide this dedicated function. Additionally, organizations benefit from the shared intelligence discovered by the service provider's other clients. The main disadvantage from the use of analysts supplied through third-party vendors is that they often do not fully complete response actions. Your internal teams must be available to provide follow-up engagement. Furthermore, cybersecurity tool investments made by your organization might not be fully leveraged, as third-party service providers are likely to use their own tools.
- ***Fully insourced:*** All SOC and threat actions are handled with internal staff and infrastructure. This model requires the buildout of a dedicated physical space with the IT infrastructure and tools necessary to support your IR personnel. It requires a combination of skills from security engineers, incident handlers, and threat hunters.
  This model has the advantage of situational awareness and an in-depth understanding of your organization's business requirements and nuances. Internal staff are accustomed to the specific needs of your organization. Additionally, internal staff understand the context of an organization's various systems in far more depth than an outside service provider could. The main disadvantages of this model relate to cost, workforce retention, and threat intelligence. Building out an internal SOC can be costly if your organization lacks existing facilities to support it. Moving to a 24x7x365 operation requires hiring new employees and supervisors to ensure effective management and coverage during holidays and time off. With this model, your organization does not necessarily get current information about threat actions occurring in other organizations. Consider leveraging student workers/internships to staff a fully insourced SOC. This model has been outlined within HSCC's Health Industry Cybersecurity Workforce Guide.[83]
- ***Hybrid:*** The SOC and incident handling functionalities attempt to take advantage of the strengths of the outsourced and the insourced models while minimizing the disadvantages of each. In the hybrid model, organizations contract with a service provider who provides 24x7x365 monitoring and response by remotely accessing your organization's existing security technologies (e.g., SIEMs, IPS, firewalls). The service provider provides facilities and staff for monitoring and response actions, and your organization provides the tools and escalation processes.
  The hybrid model tends to offer flexibility and scaling of existing investments made in cybersecurity technologies, processes, and people. However, it requires specific and scripted procedure playbooks (developed by your organization) to be effective. It is up to the contracting organization to ensure that their service provider has implemented and is performing to the specifications set by the

83 *Healthcare Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent*, Healthcare & Public Health Sector Coordinating Council (HSCC) (June 2019), https://healthsectorcouncil.org/workforce-guide/.

established procedures. Lastly, in this model, organizations lose some of the situational awareness normally provided by internal handlers. Precise roles and responsibilities must be established to achieve the desired outcome.

8.L.B: Advanced Information Sharing

NIST Framework Ref: ID.RA-2

Leveraging threat intelligence can be challenging. Your organization must establish a threat model, ingest data according to the model, and automate data collection and response. This requires dedicated human and technology resources to be successful.

MITRE has developed a model to manage threats. "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)" is a curated knowledge base and model for cyber adversary behavior. It addresses the phases of an adversary's lifecycle and the platforms that are targeted. ATT&CK is useful for understanding security risks from known adversary behavior, planning security improvements, and verifying that defenses work as expected.[84] It is recommended that organizations consider using this model in addition to STIX and TAXII automation methods to build out a robust threat intelligence program.

Intelligence gathering organizations or departments within organizations, including some ISACs/ISAOs, have a vested interest in getting "deep intelligence" directly from the attacker community. This capability requires substantial investment and specialized talent (e.g., intelligence officers), so this level of maturity is not achievable in most large organizations. However, with proper investigation, the fruits of intelligence organizations' labor can benefit the HPH sector immensely.

For a review of Healthcare specific sharing organizations consider reviewing HSCC's Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO).[85]

8.L.C: Incident Response Orchestration

NIST Framework Ref: PR.IP-9

Many specialized tools exist to provide organizational cybersecurity. It can become complicated to leverage all these tools at once. Examples include SIEMs, user behavior analytics, deception technologies, email protection platforms, and EDR technologies. Though tools like SIEMs are designed to ingest information from multiple sources and provide context, this capability is dependent on the extensibility of log data, as well as the workflow and process capabilities of the SIEM technology.

SIEMs are good at developing alerts and notifying security resources about emergent issues, but they are generally not as robust in their execution of IR playbooks. This is where IR orchestration tools come in handy. When playbooks have been created and approved, IR orchestration tools ensure that playbook execution is consistent. Without IR orchestration, cybersecurity personnel must manage IR consistency. IR orchestration tools enable cybersecurity personnel to focus on the incident, rather than on the consistent execution and documentation of a response play.

84 MITRE ATT&CK®, https://attack.mitre.org/.

85 "Health Industry Cybersecurity — Matrix of Information Sharing Organizations (HIC-MISO)," HSCC (Accessed May 31, 2022), https://healthsectorcouncil.org/hic-miso/.

In addition to monitoring workflow, IR orchestration tools can pull data from system security stacks and present it to the incident responder in a centralized dashboard. Examples of data that may be pulled into this dashboard include: SIEM, log data, Dynamic Host Configuration Protocol logs, asset inventories, anti-malware consoles, vulnerability management data, threat intelligence information, identity management systems, and endpoint security technologies. Each data type provides a unique perspective on the threat that your organization is experiencing.

8.L.D: Baseline Network Traffic

NIST Framework Ref: ID.AM-3 / DE.AE-1

The network baseline is defined as a set of metrics that describe normal operating parameters. Setting the baseline enables engineers to catch changes in traffic that could indicate an application performance problem or a security breach. It also makes the "before" and "after" when a change is made clear, making it easier to measure the benefit and calculate a return on investment (ROI). Without an accurate baseline, any kind of measurement being done is basically a best guess. This can be done manually, or you can invest in technologies that can automate the process.

Taking baseline readings for your network traffic is the first step to efficiently spotting potentially fraudulent activity. Regularly monitoring network traffic will allow you to:

- Understand healthy network patterns and traffic trends.
- Evaluate network management policies compliance.
- Understand how the network resources are allocated.
- Accelerate to troubleshoot network issues (i.e., abnormal traffic and spam traffic, etc.).
- Provide data on network and security management to support decision making.
- Provide history statistics on network upgrade.

Understanding Network Performance

- ***Device availability:*** Monitor all network device availability, particularly the critical servers on your network. If an important network device such as a central server goes down, it can take down your entire network (or a significant part of it) along with it.
- ***Storage:*** Keep an eye on the storage capacity and disk space on all your critical servers. If your storage systems are getting too full, this can cause slowdowns and problems for your end users. Additionally, assuming you have good knowledge of what your storage systems parameters are, you will be better able to detect anomalous behavior.
- ***Security:*** Make sure your firewalls, AV and malware protection, and update servers are functioning and configured correctly.
- ***Traffic:*** Monitor all traffic coming in and out of the network. This will help you to establish clear baselines and identify peak periods in advance, so you can undertake appropriate capacity planning to mitigate times when large amounts of traffic are coming through.

Monitoring Unusual Network Activity

Regarding the role of baselines in network security, if there is a huge spike in traffic, that could indicate some kind of volumetric denial of service (DoS) attack. But baselines can do more than that. Consider an instance where a certain user's normal traffic patterns indicate the network is being used to access the customer relationship management (CRM) system, email, and internet. Then, suddenly, there is traffic going from the user's computer to the accounting server. This could indicate that the computer was hacked, and malware is attempting to access and compromise financial information. Any kind of traffic that deviates too far from the norm should lead to the quarantining of an endpoint. This can help mitigate risk and minimize the damage when a breach occurs. Similarly, if the accounting system was connecting to unknown sites on the internet, it could indicate malware is present on the server.

Consider these techniques to monitor unusual network activity:

- ***Compile the list of known administrative tools leveraged by your organization for remote administration.*** These tools will be installed on endpoints. Allowlist the use of those tools and then configure your EDR technologies to flag on the use of any new administrative technology that has not been previously used. (These administrative tools are not inherently malicious but could be used for malicious purposes).
- ***Determine the user accounts that are authorized to make administrative changes in the production environment.*** Allowlist those accounts for these purposes. Key on any other administrative accounts not configured in that allowlist and investigate their use. This could catch a user account that has been granted elevated privileges by a bad actor and used in a malicious manner.

Measuring Network Changes

Baselines also help measure the impact of architectural changes. For example, if a company is using a traditional Multiprotocol Label Switching (MPLS) network, it can set baselines to understand the volume of traffic flowing over the WAN links. The baseline can then be used to help the business understand whether they are spending the right amount on the network or overspending.

8.L.E: User Behavior Analytics

NIST Framework Ref: PR.PT-1 / DE.AE-1

One technique to make a SIEM more effective is leveraging User and Entity Behavior Analytics (UEBA). UEBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats. Increasingly this analysis is performed with machine learning and artificial intelligence (AI) algorithms that reduce false positives and identify potential incidents a human would not easily see. Instead of tracking devices or security events, UEBA tracks a system's users (whether it is the authorized individual or a threat actor who has compromised a valid account) and its devices. Although attackers can generate new accounts for access attempts, they are aware that most organizations monitor systems for new accounts, especially those with privileged access. The exploitation of existing accounts, however, might go unnoticed without a UEBA system in-place.

Access logs within applications like Electronic Health Record (EHR)/EMR provide a rich source of data for such UEBA. Many certified EHR/EMRs are required to create comprehensive logs but do not alert on suspicious behavior or perform trend analysis. These applications generate substantial volumes of access

logs that are often overlooked for analysis. If used proactively, they can be very useful with identifying potential insider issues.

UEBA can address a variety of use cases. The most common include inappropriate access to information (e.g., downloading an unusual number of records), account compromise, privilege account abuse, anomalous network traffic, and data exfiltration. To create actionable alerts, the UEBAs system creates a profile of baseline user and endpoint activity throughout your organization's digital ecosystem. The tool ingests the most relevant user activity logs from these systems as well as existing authentication and authorization systems and can also monitor network traffic. Activity that deviates from the user profile create alerts to system analysts or administrators or endpoint enabling IR actions to be executed according to the proper playbooks.

8.L.F: Deception Technologies

NIST Framework Ref: N/A

Deception technologies expand on the honeypot and honeynet techniques of old, scaling them for larger enterprises. These techniques place "fake systems" (a.k.a. honeypots) or "fake breadcrumbs" (a.k.a. honeytokens) throughout the digital ecosystem and wait for them to be "tripped." They work on the principle that communications should not occur in a system that serves no purpose in your organization.

Deception technologies discover attackers who have placed a foothold in your organization's network and are attempting to pivot to find targets of interest. These targets may be simple (e.g., file storage systems, email systems) or they may be complicated (e.g., EMR or imaging systems). In all cases, the goal of the attacker is to leverage access already obtained to steal data, conduct an extortion attack (i.e., ransomware), or other maleficence.

The log files of these systems should be interfaced with your organization's SOC, as defined within 8.M.A: Security Operations Center (SOC). If such communication occurs, it should be brought to the attention of the IR teams for further investigation.

Some common techniques for implementing deception technologies include:

- ***Server-based honeypot:*** Server based honeypots are designed to mimic real servers. Ideally, they will be deployed to look like known servers in your environment, such as a file server, domain controller, web server or even middleware systems. To implement in this manner, conduct port scans against your known production, test, development, or sandbox systems and configure the honeypots to mimic the services and service version levels. Deploy these systems either nearby, or in network zones where it is known that they do not serve a production value.
- ***Registry-based honeytokens:*** A registry-based honeytoken can be placed within the Windows registry nearby other target rich registry keys, such as password hashes, software installations or other registry hive information. A popular technique is to create a fictious password-hash that, if detected through use of EDR or extended detection and response (XDR) tools, could indicate the compromise of an endpoint.
- ***Account-based honeytokens:*** As with registry-based tokens, one can create an enterprise account that has no privileges in the environment. If that account is ever used for logins or other authentication measures, it would be indicative of a further compromise inside of the environment. A common

technique there is to establish a weak password without expiration, making this a "lure" for bad actors to attempt to compromise.

- ***Fake Patient Data:*** Another popular technique is to create a fake patient within an EMR, enterprise data warehouse (EDW), or other data repositories. At this point, you can configure your DLP systems to key off this fake information and signal critical alerts if it is ever transported inside or outside of your organization.

Playbooks should be established for each of these defined implementations above and run through the SOC. In all cases, it is recommended to pivot off the activity of a honeypot or honeytoken and use that to profile the bad actor and determine their specific IOCs. These could be direct remote access channels, command and control traffic, user accounts, and file hashes of interest. Once the IOCs have been determined, you can evict the bad actor from your environment and continue to monitor for more intrusive behavior.

Key Mitigated Threats

1. Social engineering
2. Loss or theft of equipment
3. Insider, accidental or malicious data loss
4. Attacks against network connected medical devices that may affect patient safety

Suggested Metrics

- ***Time to detect and respond in aggregate, measured weekly.*** The goal is that an IR protocol should kick off within *X* hours after detection of an incident, and the incident should be mitigated within *Y* hours after response. Lag time between occurrence and detection of a security incident should be fewer than *Z* days.
- ***Number of true positive incidents executed by incident category, measured weekly.*** Though there is no specific goal for this metric, it is important to monitor trends in incidents that occur in your organization. This will inform the larger security strategy over time based on actual threats in your organization.
- ***Number of backup failures, measured weekly.*** The goal is to minimize the number of backup jobs that fail and to provide continual assurance that backup jobs are executing as intended.
- ***Number of notable (or critical- and high-rated) security incidents, measured weekly.*** This will provide a profiled enumeration of each incident. Each response to a notable security incident should be executed consistently and thoroughly. Each incident should have an after-action report. The goal is to demonstrate that after-action reports and incident reports are written for each notable security incident. This will help with the development and implementation of continual improvement processes.

Cybersecurity Practice #9: Network Connected Medical Devices

Areas of Impact
PHI

Medium Sub-Practices
9.M.A Asset Management
9.M.B Endpoint Protections
9.M.C Identity and Access Management
9.M.D Network Management
9.M.E Vulnerability Management
9.M.F Contacting the FDA

Large Sub-Practices
9.L.A Security Operations and Incident Response
9.L.B Procurement and Security Evaluations

Key Threats Addressed
- Attacks against network connected medical devices that can affect patient safety

405(d) Resources
- Prescription Poster: Network Connected Medical Devices

Healthcare systems use many diagnostic and therapeutic methods for patient treatment. These range from technological systems that capture, render, and provide detailed images of scans to devices that connect directly to the patient for diagnostic or therapeutic purposes. Medical devices range from straightforward monitors, such as bedside monitors that measure vital life-sustaining activity to sophisticated multi-function machines, like infusion pumps that deliver specialized therapies and require continual drug library updates. Network connected medical devices are network-based devices that leverage networking protocols to communicate and transmit clinical information, such as Bluetooth, TCP/IP and other networks-based devices. These complex devices create and maintain copious amounts of data that affect patient safety, well-being, and privacy. Their interconnection with information systems that manage clinical decision making represent potential attack vectors in HDOs' digital systems. As such, these devices should be robustly designed and properly secured.

This section focuses on the methods that HDOs can employ to protect network connected medical devices. Specifically, it addresses the actions that HDOs are permitted to take, how to align with the Medical Device and Health IT Joint Security Plan, and how to best work with device manufacturers and the FDA.

The creation and deployment of network connected medical devices has rapidly expanded in the past few years. These online medical devices have become increasingly attractive to cybercriminals. Each device may contain hardware, software, and/or sensors that gather, store, and transmit healthcare data and confidential patient information over health system's clinical network and internet.

Many IoT devices interact with the physical world in ways conventional IT devices usually do not. The potential impact of some IoT devices making changes to physical systems and thus affecting the physical world needs to be explicitly recognized and addressed from cybersecurity and privacy perspectives. Also, operational requirements for performance, reliability, resilience, and safety may be at odds with common cybersecurity and privacy practices for conventional IT devices.

Additionally, some medical devices may only be intermittently connected to the network, or have yet to be onboarded. The problem is that these devices might still be at risk from vulnerbailities, thus it is recommended that these vulnerabilities be corrected or mitigated before being attached to the network. There is also the possibility of "rogue" medical devices getting connected to the network. These devices may be used by the healthcare provider team as part of an assessment or vendor trial or demo.

How to Prevent Spread of Security Impacts

There are four high-level goals to mitigate cybersecurity and privacy risks for IoT devices:

1. ***Protect Patient Safety and Device Effectiveness:*** Patients who are receiving care from network connected medical devices are at risk of adverse events resulting from device vulnerabilities being exploited that impact device availability and performance. Security controls internal and external to the device aim to assure the safety and effectiveness of the device.
2. ***Protect Device Security:*** Prevent a device from being used to conduct attacks, including participating in distributed denial of service (DDoS) attacks against other organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices found on the network.
3. ***Protect Data Security:*** Protect the confidentiality, integrity, and/or availability of data (including PII and PHI) collected by, stored on, processed by, or transmitted to or from the connected medical device. This goal applies to each IoT device except those without any data that needs protection.
4. ***Protect Patient Privacy:*** Individuals' privacy can be impacted by the authorized processes surrounding PII/PHI. This goal applies to all network connected medical devices that process PII/PHI or that directly or indirectly impact individuals.

Why do medical devices create unique challenges?

Confidentiality, integrity, and availability of patient data are paramount, and still breaches occur almost daily in healthcare. While impacting data is devastating to the patient and provider, compromised network connected medical device integrity can be catastrophic. Emergency room doctors rely heavily on a computed technology (CT) scanner's availability and integrity to quickly diagnose stroke patients and determine if a stroke is hemorrhagic or ischemic. Delayed care or misdiagnosis due to a compromised CT scanner could easily result in loss of motor functions, brain damage, or even death.

Many network connected medical devices interact with the physical world in ways conventional IT devices do not. Infusion pumps regulate the delivery of life-sustaining medication. Implanted cardioverter defibrillators deliver electrical shocks and restore the heart to normal rhythms. Hackers have demonstrated vulnerabilities in these types of devices which allow increasing dosages or manipulating shocks that result in sudden death. While these examples are extreme, it is clear that interfering with the stated performance of network connected medical devices negatively impacts the quality of patient care and increases the financial risk to the provider.

Traditional IT devices like workstations, servers and routers have been designed with security in mind so can be fully integrated and managed by traditional information security tools. Most medical devices, facilities management devices and some IoT devices do not share this same design and therefore create challenges for IT and Security teams.

- ***Visibility, Inventory & Device Scanning:*** The volume of medical devices ranges from 5-14 devices per bed, which creates an exponentially complex challenge for creating, maintaining and monitoring a growing, changing and mobile inventory. Network device scanning tools are considered invasive or active. These tools interact with the network device to obtain granular detail about the device. The ability to identify a computer's make, model, operating system, IP address, serial number, MAC address, etc. is standard for traditional devices. This level of detail allows traditional security tools to make determinations regarding risk levels and vulnerabilities, mitigations or remediations.

Medical devices are not designed to support active scanning. Active scanning can interfere with the performance of a medical device, which could be attached to a patient. Disrupting normal functionality or "knocking the device over" could negatively impact patient care. Identifying the medical devices on your network and gleaning the granularity of detail on each device required to make intelligent cybersecurity decisions had been a challenge for healthcare IT and Security teams.

- ***Passive Scanning & Communication Protocols:*** An optional technique for device identification is passive scanning. Like active scanning, traditional IT-based passive scanning tools can read the packets of information traveling across the network and make determinations. This becomes a challenge because traditional IT devices communicate in protocols like TCP/IP, HL7 and DICOM and traditional security tools are limited to understanding (reading packet information) written in these protocols. Medical devices, facilities devices and many IoT devices communication in unique protocols. Once again, creating a challenge in the rudimentary step of identifying what devices are on the network.
- ***Medical Device Risk Management:*** How can your organization determine the device vulnerabilities, the environmental risk posed by or to the device, the device risk level and appropriate controls required to reduce risk safely and effectively if your organization has no visibility on the devices and their details?
- ***Device Monitoring & Network Policy Management:*** NAC systems are commonly used to manage traditional endpoint devices: servers, desktops, laptops, and portables. NAC can manage traditional network endpoints because they have visibility on these devices. However, most NACs have inadequate contextual information about medical device use, traffic flows or operational status. There are two main challenges with network policy management:
    - ***Determining Policies:*** Without accurate identification of the device and a full understanding of the other network devices it is communicating with, creating network communication restriction on medical devices, potentially providing life-saving care, requires a tremendously labor-intensive effort in mapping. Therefore, many network policies have little or no restrictions on these devices and they are simply put in an unrestricted VLAN with other unknown devices with unknown risks.
    - ***Operationalization:*** When network communication policies can be identified, converting those logical communication restrictions into the network software is also labor-intensive. Programming and testing restrictions are critical to maintain and protect clinical device performance.
- ***Legacy Devices:*** These are defined as a device that cannot be reasonably protect against current cybersecurity threats.[86] Traditional IT device lifecycles are two to four years. Medical device lifecycles can extend beyond 15 years. Clinical Engineering departments work hard to maintain and extend the life of devices. But most health organizations utilize the devices beyond the EOS for the operating systems and other components within the device. Management of legacy technologies in healthcare is a multi-faceted challenge. Although the functional or maintenance obsolescence, or even device safety risks because of device EOS, are not new problems, the inclusion of cybersecurity considerations heightens the frequency of such events and increases the urgency of addressing them.

86 "Principles and Practices for Medical Device Cybersecurity," IMDRF Medical Device Cybersecurity Working Group (March 2020), https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf.

- ***Remote Access:*** Manufacturers may need to access the medical devices remotely over the network for updates or to mitigate vulnerabilities. This functionality is built into the device which causes challenges in monitoring communications, managing access, and determining restrictions. Leveraging a device's remote access capabilities is a primary vector for bad actors to enter the network.
- ***Risk Analysis & Electronic Public Health Information (ePHI):*** The HIPAA Security Rule requires an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate. While MDS^2 forms can identify which devices have ePHI, it is a static variable that is not being identified within the context of network communication. How are organizations determining if data stored or transmitted by medical devices is encrypted? The volume of devices combined with the complexity of identifying ePHI on the network is compounded when factoring in the risk of the device. All of which is required under the HIPAA Security Rule for compliance.
    - NIST SP 800-66r2 ipd Implementing the Health Insurance Portability and Accountability Act states:[87]

      Prepare for the Assessment: Before beginning the risk assessment, the regulated entity should understand where ePHI is created, received, maintained, processed, or transmitted. Identify where ePHI is generated within your organization, where and how it enters your organization (e.g., web portals), where it moves and flows within your organization (e.g., to specific information systems), where it is stored, and where ePHI leaves your organization. Is ePHI transmitted to external third-parties, such as cloud service providers or other service providers? The scope of a risk assessment should include both the physical boundaries of a regulated entity's location and a logical boundary that covers any devices or media that contain ePHI, including electronic networks through which ePHI is transmitted, regardless of its location.
- ***High Knowledge/Limited Resources:*** Cybersecurity for medical devices creates new complexities related to personnel resources and departmental alignments. Clinical Engineering is responsible for the devices and often the only individuals licensed to repair/configure them under compliance requirements. The IT and Security teams are versed in risk mitigation and how the device operates on the network. These departments will need to work more collaboratively, and some organizations have created new positions that focus on spanning the Cybersecurity for Medical Device channel.

But medical device cybersecurity risk management is evolving. Progressive HDOs are increasing collaboration, implementing a device security plan, exploring leading-edge solutions, and leveraging additional resources to bring the healthcare sector into the 21st century.

Asset Discovery and Security (ADS) monitoring solutions can automate many of the tasks surrounding the implementation of controls, additionally they can collect device specific and network ecosystem data. Sophisticated and health industry specific deep packet inspection, combined with machine learning and AI based systems, can classify and profile all medical devices on the network. While an ADS can automate discovery, monitoring, analysis, and onboarding of devices, integration with a Computerized Maintenance Management Systems (CMMS)/Configuration Management Database (CMDB) can operationalize

87 *NIST Special Publication NIST SP 800-66r2 ipd Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide*, NIST (July 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf.

maintenance and remediation workflows, and coordinate security orchestration and incident response. Together, both tools create an efficient, effective, and scalable solution.

Given the highly regulated nature of medical devices and the specialized skills required to modify them, HDOs should take great care in making configuration changes without utilizing technical support documentation or service programs endorsed by the device manufacturer. Doing so may put the HDO at risk of voiding warranties, resulting in legal liability, or at worst, harm to the patient. Therefore, traditional security methods used to secure assets should be carefully reviewed prior to being deployed or applied to medical devices. For example, one cannot simply apply a patch to a vulnerable component of the operating system that runs a medical device without fully assessing the impact on the operation or capabilities of the medical device.

Medical Device Management

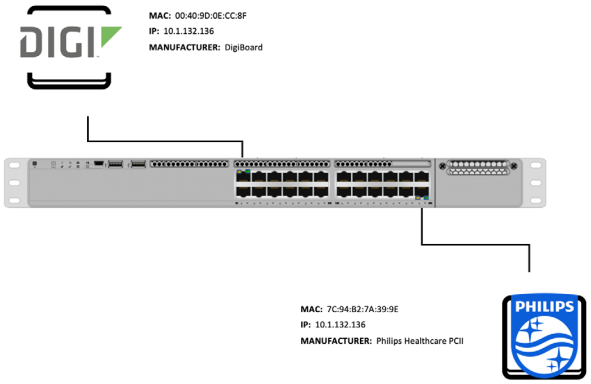
Medical devices that can connect to the internet are a specialized type of IoT device, specific to providing clinical diagnosis or treatment within HDOs. Nevertheless, cybersecurity for medical devices requires many of the cybersecurity practices already discussed in this document:

- Cybersecurity Practice #2: Endpoint Protection Systems
- Cybersecurity Practice #3: Identity and Access Management
- Cybersecurity Practice #5: IT Asset Management
- Cybersecurity Practice #6: Network Management
- Cybersecurity Practice #7: Vulnerability Management
- Cybersecurity Practice #8: Security Operations Center and Incident Response

Rather than recreating these cybersecurity practices, HDOs are encouraged to extend the relevant cybersecurity practice from each section, implementing it appropriately for medical device management. The following sections expand on how the practices listed above apply in the specialized case of medical devices.

Medical devices typically connect to larger information systems or applications. For example, a CT scanner may connect to a picture archiving and communication system (PACS), which, in turn, is connected to specialized image-reading workstations.[88] In such environments, the practices listed below are important, not only for the medical device itself (in the case the CT scanner), but also for the larger information systems and connected endpoints. Consider all these safeguards, as applicable.

Figure 3. Last Generation Technology—Limited Viability



88 *NIST Special Publication 1800-24: Securing Picture Archiving and Communication Systems (PACS): Cybersecurity for the Healthcare Sector*, NIST (December 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf.

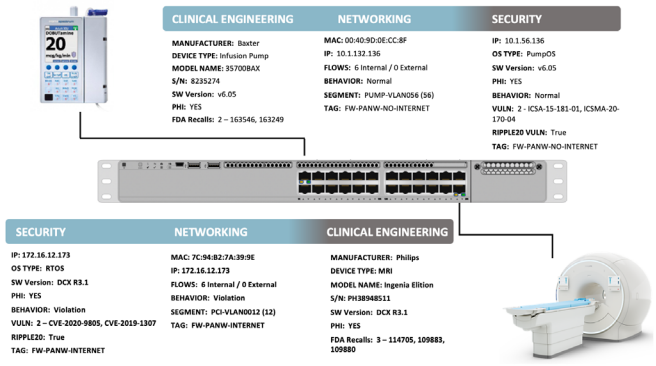
Sub-Practices for Medium-Sized Organizations

9.M.A: Asset Management

NIST Framework Ref: ID.AM, ID.AM-1, PR.IP-6

When feasible, medical devices should have the following controls enabled:

Figure 4. Next Generation Tools—Actionable Device Data



- ***Inventory, hardware:*** All medical devices should be added to an inventory that can reflect the core components of the devices themselves. You may use your general ITAM inventory, as described in Cybersecurity Practice #5: IT Asset Management. Alternatively, you may need to employ specialized tools designed specifically for tracking the lifecycle of medical devices. Such systems can be useful for maintaining preventative maintenance schedules.
- ***Inventory, software:*** Implement a software component inventory for your medical devices. Manufacturers should be able to deliver to the HDO a full listing of software components (including operating systems and software application components developed by vendors, as well as components licensed from third-parties), with at least major version information. Such lists are sometimes referred to as "bills of materials." Information about software components should be maintained in a scalable database managed by the HDO and updated as part of the standard device management practices.
- ***Wiping:*** When a medical device is slated for decommissioning, it is crucial to ensure that all data on the device are wiped. Typically, these devices are returned to the vendor and potentially resold or delivered to other organizations for destruction. Federal and state requirements for the protection and disposal of hardware and media that contain PII prohibit the allowing the data to be accessed by these other parties.

Within the medical technology discipline, it is recommended to store the results of these inventories into CMMS. These systems are like ITAM systems for IT assets but contain specialized fields for the tracking of maintenance, recalls, and other key attributes specific to medical devices.

Automated Asset Discovery

It is common for an HDO to have hundreds to thousands of medical devices deployed throughout the system. As such, conducting these hardware and software inventories manually is likely to be inefficient. Automated tools, called ADS monitoring systems, exist to assist with this issue. These ADS tools can automate many control implementation tasks while collecting device specific and network ecosystem data. Sophisticated machine learning and AI based systems can classify and profile all medical devices on the network.

While an ADS can automate discovery, monitoring, analysis, and onboarding of devices, integration with a CMMS to operationalize maintenance and remediation workflows, and coordinate security orchestration and IR. Together, both tools create an efficient, effective, and scalable solution.

Scanning results of ADS tools may include detailed insights into what type of device is detected, its make, capabilities, location, application/port, and behaviors. ADS applications can solve the fundamental inventory problem by searching, with little to no human intervention, the healthcare organization's network and identifying all the network devices. The solutions will also continually scan the network for new devices that are added.

While this feature will solve the inventory problem, there are additional requirements and considerations needed for the solution to reach cybersecurity and asset management efficiency. Additional data details need to be collected:

- How many devices are connected?
- What types of devices are they?
- Which other devices on the network are they communicating with?
- Is the device behavior normal with respect to other similar devices?
- What is the device type, manufacturer, model, modality, serial number, operating system, etc.?

Figure 4 represents the limited data obtained from medical devices when using traditional IT security network monitoring tools. Too often discovery only yields the information on the network interface card connecting the device to the network or non-descript information about the device.

Many devices are only intermittently connected to the network or have not yet been deployed. No amount of automated ADS tool discovery can see these devices, yet most still possess vulnerabilities that need to be corrected. As noted by HIPAA Security Rule, mitigations for these vulnerabilities will come in the form of physical, administrative and technical safeguards. For example, a portable electrocadriogram (ECG) machine not connected to the network (and contains thousands of patient records) is still at risk for physical theft, and therefore needs controls implemented to help reduce this risk's impact.

The combination of a CMMS tool integrated with an ADS solution allows for the cybersecurity management of connected and non-network connected medical devices.

With ADS tools designed for medical devices, machine learning, AI and deep packet inspection can be leveraged to provide dozens of data points that can be integrated into a CMMS and used to improve the management of devices by device, model and fleet

ADS tools can scan the network for medical devices, but they use a different approach than traditional vulnerability scanners which can negatively impact patient safety. Instead of actively interacting with the device, Medical Device Security (MDS) tools leverage "passive" scanning. This approach watches the network communications between devices, servers and network equipment. This technique is sometimes called computer learning, deep packet inspection (DPI), and AI.

DPI may capture device make, model, OS, embedded software, communication protocols, clinical functionality, Manufacturer Disclosure Statement for Medical Device Security (MDS^2) data and connectivity. Opening and reading these proprietary packets of information is complex, but it may provide rich contextual data on every device.

Once the basic device identification has been obtained, the device behavior is tracked and analyzed. ADS tools can create a communications profile consisting of a variety of unprecedented data elements: Volume, protocols, geography/location, traffic frequency, source (external or internal).

From these communications profiles the system can establish baselines for normal behavior based on device type. Devices that are similar are grouped for easier and more efficient management. Devices deviating from this normal behavior will be considered anomalous and flagged for inspection. Profiling and grouping devices provide for an efficient and scalable approach for managing the volume of assets and vulnerabilities related to medical devices.

Any solution designed to mitigate and remediate the vulnerabilities of medical devices across an enterprise will need to operate efficiently and effectively. The ability to scale and apply controls at the fleet level or correlate preventative maintenance activities with security maintenance will be a direct result of enhanced visibility into the details of each device on the network.

9.M.B: Endpoint Protections

NIST Framework Ref: PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1

As with authentication, most endpoint protection services are focused on agent-based approaches which assume that software and patches can be installed on the devices and managed through local or centralized servers. However, many medical devices that connect to the network lack support for agents such as AV, antimalware, host intrusion, or even basic patching to protect them from known and zero-day threats.

ADS solutions support a zero trust model (see **2.L.E: Micro-Segmentation/Virtualization Strategies**) to ensure access to any resource is validated and authorized. Zero trust incorporates the principle of least privileges. The principle of least privileges is that each device or user has a specific role and function and that access to data and services should be limited to the absolute minimum required to carry out that role or function. Even when granted minimal access based on proper authorization, trusted devices and users must be monitored to detect abuse of said privileges.

While restricting outbound access to remote systems and data, it is also necessary to protect individual devices and users from incidental or deliberate access-leading to data theft, service disruption/manipulation, ransomware, or attack proliferation. To this end, layered security is typically implemented to restrict both inbound and outbound access to devices at various levels in the network and application stack. If compromised, the principle of least privileges has critical relevance. A medical device such as a blood pressure monitor should only be connected to the technologies it needs to function. For example, the blood pressure monitor should not be connected to the HVAC system because an attacker could leverage the HVAC system to gain access to PII or PCI data.

Where feasible, medical devices should have the following controls enabled and responsibility for these controls may be a mix between the MDM and the HDO. For more defined responsibility information, check out HSCC documentation Model Contract-Language for Medtech Cybersecurity (MC2):[89]

- ***AV software:*** In most cases, the MDM should directly support AV software when the device uses a commercial (non-embedded) operating system (i.e., Windows, Linux). Ensure that a compliant AV technology is enabled. If AV cannot be implemented, compensating controls should enforce an AV scan whenever the device is serviced prior to reconnecting to the device network.

89 *Model Contract-language for Medtech Cybersecurity (MC2)*, Healthcare & Public Health Sector Coordinating Councils (HSCC) (March 2022), https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/.

- ***Local firewalls:*** Medical devices should be configured to communicate only with required systems, if supported by the MDM. Unused devices and ports should be disabled if they are supported by the manufacturer as they are only protected at the device level beneath a local firewall.
- ***Encryption:*** If supported by the manufacturer, medical devices should be encrypted at rest by default. This will ensure the confidentiality and integrity of the data in case the device is lost or stolen.
- ***Application allowlist:*** Configure medical devices, or implement software, to only allow known processes and executables to run on the devices. This control alone can significantly reduce the exploitability of devices.
- ***Default password changes:*** If supported by the manufacturer, default passwords, especially those enabling privileged access, should be changed to long, complex passwords used only for the medical device. Do not tie unique device credentials to any general systems management credential, as you do not want general credential compromises to affect the medical device. It is the MDM's responsibility to design devices not to use hardcoded or default passwords and to require a password change on the first use and it is the HDO's responsibility to change passwords consistent with HDO access management policies.
- ***Routine patching:*** The MDM and HDO share the responsibility in routine patching. The MDM's responsibility is to design devices to have secure, reliable update capabilities (e.g., digital signatures for software/firmware) and to communicate when updates are available. The HDO's responsibility is to monitor, deploy, and track updates to devices at their facility.

9.M.C: Identity and Access Management

NIST Framework Ref: PR.AC, PR.AC-7, PR.AC-4

As much as possible, medical devices should have controls for authentication, vendor support passwords, and remote access.

Authentication

Foundational to any IAM solution is to ensure accurate detection and tracking of each asset and user that connects to the network for identity validation. This core requirement has mature solutions related to managed devices and users. An explicit credential is produced to ascertain identity including certificates, username/passwords, tokenization, and other methods that attempt to link a device/user to a trusted entity. Many of these methods entail the use of agents or installation of software to validate identity. However, a significant percentage of the devices and users that connect to the network do not support agents or explicit identity credentials. These include the ever-expanding list of IoT and other devices that lack a user presence to submit a trusted credential at the point of entry. Even for managed devices with an associated user, the device itself is often not authenticated (just the user of the device), which leaves a gap in the trust of the device itself.

Common NAC systems address these gaps using MAC or IP-based authentication. The bypass of true authentication using only the MAC or IP address is a weak attempt to uniquely track non-authenticating devices. This leaves many organizations exposed to high risk, as there is a weak trust relationship and exposure to spoofing and inability to truly identify and audit the actual devices that are connected to the network. ADS solutions may be able to fingerprint devices that connect to the network including a synopsis into a device's hardware (manufacturer, model, serial number), software (operating system,

version, firmware revisions), device type and function, as well as a security assessment for vulnerabilities and risk. ADS device discovery and classification is passive and requires no agents.

Once a device is identified, these solutions continually monitor its communications for both flow data as well as deep inspection of the communication protocols and applications to check for spoofing, threat activity, and behavioral anomalies. This ensures that even if devices can circumvent authentication, threats are detected and can be blocked from the network.

In addition to authentication, other device context such as **time, location, vulnerabilities, and posture compliance** often factor into network access decisions. ADS solutions augment the tracking of these other elements for a comprehensive understanding of each network-connected device and to allow more accurate access decisions based on governance and security policies.

Vendor Support Passwords

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

Remote Access

If remote access is required to manage medical devices, MFA capabilities should be deployed. The HDO must accept the system access mode to be used. Depending on the deployment scenario, the device manufacturer may be required to support remote access capabilities. Otherwise, such capabilities should be deployed on a separate component of your existing MFA system to limit exposure if the MFA system is compromised.

If leveraging a vendor's remote access tool, be sure to evaluate the risk of "unattended sessions". These are sessions by which the vendor is permitted to access your network or medical device without any prior authorization from the HDO. This is a useful back channel for malicious actors to leverage to unauthorized access into enterprise information systems. If the vendor's remote access tools are to be activated, insist that these sessions always be "attended". This means for any remote access connection that will be made, there must be a HDO sponsor authorizing the access. Otherwise, the request access will be denied.

Remote access can be broken down into basic categories: 1) extended branch/remote office, 2) user to campus, and 3) user to cloud. ADS solutions do not typically monitor direct communications between a remote user and a cloud service but do play an active role in the first two categories. For extended branch/remote office, ADS provides the same set of rich device discovery, classification, and security analytics as devices connected to an enterprise campus network. For remote users that connect to a campus network (and resources over a VPN or similar service), ADS provides comprehensive visibility into all connected IPs, monitors them for risk and unexpected behaviors, and tracks access to both authorized as well as unauthorized or high-risk targets. ADS solution's traffic analysis allows network and security administrators to visually monitor remote access communications by location and subnet and track them for safe and approved behavior and quickly detect exceptions. They also monitor threat activity in expected flows through intrusion detection services, and correlate communications to at-risk sites through its extensive threat and reputation feeds.

9.M.D: Network Management

NIST Framework Ref: PR.AC-5

As much as possible, HDOs should ensure the following network management controls are enabled for the medical devices in their networks:

- ***Segmentation:*** Given the critical nature of medical devices and your organization's general inability to configure them to reduce vulnerabilities, it is crucial to segment these devices separately from general access or data center networks. The ability to restrict access to the device is essential to its safe operation.
  Dedicated, highly-restricted networks should be set up. The only traffic allowed on these networks should be profiled based on required operation of the devices connected to that network. Access to device management systems should be heavily restricted to limit its exposure. Lastly, it is important to ensure that these networks are segmented such that any vulnerability scanning systems are not permitted access in a clinical setting. Given the delicate nature of medical devices, execution of a rogue vulnerability scan could disrupt the devices.
- ***Micro-segmentation:*** This takes segmentation one step further by protecting devices from other systems in the same network segment in addition to systems outside of their network. It is based on defense in depth and, if supported, may be the most effective way to protect devices from network-based attacks. Medical devices are purpose-built devices that adhere to a predefined set of limited communication patterns. They are well suited to be protected by micro-segmentation, preventing attackers who penetrate a traditional segment from moving laterally because all unessential traffic is restricted.
  While this security strategy is effective, operationalizing micro-segmentation can be cost prohibitive. It requires network engineers to determine the restrictions and then program those rules/policies into the network components. With tens of thousands of devices, manually implementing and maintaining micro-segmentation is not achievable.

ADS tools can automatically and intelligently create network policies/rules based on the monitoring of device communication whereby devices are never trusted, and the environment is assumed to be hostile. This approach accomplishes the most granular level of micro-segmentation: zero trust architecture (ZTA). ZTA operates on the premise that both internal and external networks are untrustworthy with no distinction between them. Additionally, all device access requests and communications with a device are always verified based on the behavioral analytics obtained during the baselining process. ZTA, however will not protect unconnected devices, or devices yet to be onboarded. ZTA is difficult to manage without a dedicated team of IT resources. If security events or vulnerabilities are identified, these unconnected devices must be remediated too.

Once generated, these policies can be implemented manually by staff or automatically by integration with the target system (e.g., Cisco ISE, Firewall API, etc.). Policies can likewise be automatically created to isolate or quarantine devices with high levels of risk or signs of compromise.

Devices with vulnerabilities, recalls, weak passwords, or signs of threats can be tagged for remediation, and optionally protected or isolated to limit exposure. Policies/rules can be enforced based on the connected medical device's observed risk, known vulnerabilities, signs of IOC and their context with the unique network itself. Mission critical devices or high-valued assets may have more stringent restrictions.

ADS solutions are designed to approach medical device security dynamically because the context of the clinical network environment is always changing. Trust can change for a session or a device between one login and the next. New devices are constantly being added and removed which introduce different vulnerabilities to the environment. ADS solutions can identify new devices, changes in device behavior and new IOCs.

HDOs realize several benefits from micro-segmentation:

- ***Isolation:*** During cyber-attacks, network traffic is isolated, limiting access between segments.
- ***Monitoring:*** Monitoring of Internal communications, inter-segment communications, log events and irregular device behavior.
- ***Compliance:*** Reduction of the number of systems subjected to regulation.
- ***Access Control:*** Limited access to sensitive data, prevention of privilege escalation, and lateral movement.

As part of the segmentation strategy, review data flows and interfaces between the medical devices and their connected systems. Be sure not to limit the essential functionality of the medical device, including its ability to be patched remotely, if required. Device manufacturers may require installation of their own physical networks in your organization. In these cases, access to the manufacturer's physical network should be limited with the same restrictions as if the HDO were implementing its own segmentation strategy. For more defined responsibility, check out HSCC documentation Model Contract-Language for Medtech Cybersecurity (MC2).[90]

9.M.E: Vulnerability Management

NIST Framework Ref: ID.RA-1, PR.IP-12, ID.RA-5, RS.CO-5, DE.CM-8

As much as possible, medical devices should have the following vulnerability management processes implemented:

- Vulnerability and risk categorization
- Contract negotiation
- Vulnerability disclosure programs
- Software bill of materials (SBOM) and vulnerability lookups
- Vulnerability scanning

Vulnerability and Risk Categorization

In 2016, the FDA issued the Postmarket Management of Cybersecurity in Medical Devices guidance.[91] This guidance document presents components for the proper management of medical devices after they have been deployed in an HDO. Focusing on the risk to patient safety, this guidance stipulates manufacturers should implement vulnerability and risk-management practices to categorize risks according to the exploitability of the cybersecurity vulnerability and the potential to cause harm to the patient.

90 *Model Contract-language for Medtech Cybersecurity (MC2)*, Healthcare & Public Health Sector Coordinating Councils (HSCC) (March 2022), https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/.

91 *Postmarket Management of Cybersecurity in Medical Devices*, Food and Drug Administration (FDA) (October 1, 2018), https://fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

HDOs should work with device manufacturers to arrive at a common understanding of the framework for the risk categorizations. Upon disclosure of a high risk, HDOs should take escalated action to secure the device.

Utilizing a risk-based approach to vulnerability management which permits flexibility can address the problem of scarce resources on tasks that mitigate and reduce risk to your organization.

The Common Vulnerabilities and Exposures (CVE) is a list of publicly known cybersecurity vulnerabilities and exposures maintained by MITRE Corporation. The U.S. National Vulnerability Database is fully synchronized with the MITRE CVE list. When a CVE is found and identified, a software company releases a patch so users can download it and repair the vulnerability. Many HDO's have a patch-management solution to address patching systems in their network; however, they lack a patch validation view and knowledge about the completeness of the patching event. CVE entries can be very helpful in identifying vulnerable devices in the HDO environment.

With ADS tools designed for medical devices, machine learning, AI and deep packet inspection can be leveraged to provide dozens of data points that can be integrated into a CMMS and used to improve the management of devices by device, model and fleet.

ADS tools can scan the network for medical devices, but they use a different approach than traditional vulnerability scanners which can negatively impact patient safety.

Instead of actively interacting with the device, MDS tools leverage "passive" scanning. This approach watches the network communications between devices, servers and network equipment. This technique is sometimes called computer learning, deep packet inspection (DPI), and AI.

Once the basic device identification has been obtained, the device behavior is tracked and analyzed. ADS tools can create a communications profile consisting of a variety of unprecedented data elements: volume, protocols, geography/location, traffic frequency, and source (external or internal).

From these communications profiles the system can establish baselines for normal behavior based on device type. Devices that are similar are grouped for easier and more efficient management. Devices deviating from this normal behavior will be considered anomalous and flagged for inspection. Profiling and grouping devices provide for an efficient and scalable approach for managing the volume of assets and vulnerabilities related to medical devices.

Any solution designed to mitigate and remediate the vulnerabilities of medical devices across an enterprise will need to operate efficiently and effectively. The ability to scale and apply controls at the fleet level or correlate preventative maintenance activities with security maintenance will be a direct result of enhanced visibility into the details of each device on the network.

Table 13. ADS Use Cases

Use Cases	Monitor	Analyze	Secure
Undesired Traffic	Watch risky ports (e.g., 3389)	Assess appropriateness	Block ports or segment
Vulnerabilities	Correlate known vulnerabilities with existing assets (e.g., Ripple 20, Deja Blue)	Evaluate, discuss with vendors, and determine mitigation	Patch, block ports or segment
Unsupported OS	Identify risky devices	Assess traffic—necessary and unnecessary	Upgrade OS, replace device or segment
Device Behavior	Determine "normal activity" baseline	Assess traffic—necessary and unnecessary	Block unnecessary traffic

ADS tools can analyze each device in terms of potential risk to your organization, as seen in Table 13 above. This analysis can include a wide range of device traits including the identification of high-value devices, devices with known vulnerabilities, devices that have been recalled, devices using weak or open passwords, and weak TLS ciphers or expired certificates. For example, devices that process sensitive information such as PHI can be identified automatically. This can be extremely efficient in supporting a HIPAA-required risk analysis.

ADS tools can also discover signs of compromise using both known and behavioral IOC. Known indicators can include interaction with known malicious IP addresses or domains. Alternatively, these new systems can recognize behavioral anomalies within devices based on observed baselines in the network or deviations from norms for a particular device profiled.

Vulnerability Disclosure Programs

Each device manufacturer should have a program that informs HDOs of vulnerabilities in their devices. These programs should have a communication channel to report information and inform parties. HDOs should work with the manufacturers so that all parties understand the respective points of contact between the manufacturer and the HDO.

In addition to direct communications from manufacturers, other channels exist for the disclosure of medical device vulnerabilities. These include the CISA National Cybersecurity and Communication Integration Center, the Health Sector Cybersecurity Coordination Center (HC3), and the Industrial Control Systems—Computer Emergency Response Team (ICS-CERT); manufacturers can include these as part of their vulnerability releases, as can ISACs or ISAOs with which the manufacturers participate.[92]

The HDO should have a program in place to accept inbound vulnerability disclosures, evaluate the HDO's exposure to these vulnerabilities, and identify, alongside the manufacturers, response actions to remediate or mitigate each vulnerability according to its level of risk.

With a well-established vulnerability disclosure program, medical device manufacturers and HDOs will have bidirectional communication for managing medical device vulnerabilities. Communication is key

92 "Health Sector Cybersecurity Coordination Center (HC3)," HHS.gov (March 31, 2022), https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts.
"ICS-CERT Advisories," CISA (Accessed June 2, 2022), https://www.cisa.gov/uscert/ics/advisories.

to maintaining patient safety. **Table 14** provides a general rule for the response timeframes (including interim compensating controls) for medical device vulnerabilities; this general rule is in line with expectations in the Postmarket Management of Cybersecurity for Medical Devices guidance.[93]

Table 14. Timeframes for Resolving Medical Device Vulnerabilities

Vulnerability Criticality	Days
Uncontrolled Risk	
• Vendor communicates to HDO; HDO determines interim mitigation step	30 days
• Vendor produces a risk remediation solution; HDO implements solution	60 days
Controlled Risk	As defined by routine patching and preventative maintenance

Software Bill of Materials (SBOM) and Vulnerability Lookups

Most medical devices include open-source software components and libraries. Many of these medical devices ship with vulnerable or out-of-date software components that may never be updated, according to the Department of Commerce's National Telecommunications and Information Administration (NTIA).

Using SBOMs registered in your organization's ITAM, CMMS or other systems, the HDO can compare data from the NVD against data in your organization's software libraries. This comparison provides the HDO with information on current potential vulnerability postures in the medical device space.

A simple search of the NVD can be conducted by using the web interface located on NIST's website.[94] This search tool allows HDOs to look up vulnerabilities in products that they currently have. It does not require SBOM material to be preregistered.

To support the development of an automated solution, in July 2018, the U.S. National Telecommunications and Information Administration (NTIA) launched a multi-stakeholder initiative to improve software component transparency across myriad industries, including medical device technology.[95] Their goal is to standardize the process for sharing the data on the components within devices. There is little visibility into the supply chain which is problematic for security. President Biden's Executive Order on Improving the Nations Cybersecurity signed in May of 2021 specifically promotes the continued development of the NTIA SBOM initiative.[96]

A proof of concept is being tested to address this issue. Prestigious academic medical centers using ADS solutions and CMMS tools have worked with renowned medical device manufacturers under the direction of the NTIA in a public/private partnership to automate the creation and ingestion of a SBOM. MDM's now can produce SBOMs containing medical device component detail, which can then be automatically

93 *Postmarket Management of Cybersecurity in Medical Devices*, Food and Drug Administration (FDA) (October 1, 2018), https://fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

94 "National Vulnerability Database," NIST (Accessed June 2, 2022), https://nvd.nist.gov/.

95 "NTIA Software Component Transparency," National Telecommunications and Information Administration (NTIA) (April 28, 2021), https://www.ntia.doc.gov/SoftwareTransparency.

96 Executive Order No. 14028, (May 12, 2012), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

parsed and ingested from a vulnerability source into the ADS or CMMS technology solutions which provide indexes to devices within the HDO's clinical network. Advancements like this will have an unprecedented impact on reducing the risk of vulnerabilities like Ripple 20 (which identifies the Vxworks operating system within 2 billion devices, many of which are medical devices).

Vulnerability Scanning

WARNING: UNLESS APPROVED BY THE DEVICE VENDORS, THIS ACTION SHOULD BE TAKEN WITH EXTREME CAUTION DUE TO THE POTENTIAL IMPACTS ON MEDICAL DEVICES WITHIN THE PRODUCTION ENVIRONMENT. HDOS SHOULD NOT ATTEMPT TO CONDUCT VULNERABILITY SCANS UNLESS ABSOLUTELY CERTAIN THAT THE MEDICAL DEVICE IS NOT IN PRODUCTION, IS NOT CURRENTLY IMPLEMENTED IN A CLINICAL SETTING, AND IS NOT CONNECTED TO PATIENT.

The final action an HDO can take to understand its vulnerability posture is to conduct vulnerability scans against the medical devices.

The primary opportunities to conduct vulnerability scans against medical devices are:

- When the device is first procured and tested before deployment in the production environment
- When a device is taken offline for preventative maintenance and routine patching
- During the utilization of an ADS tool

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

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

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

9.M.F: Contacting the FDA

NIST Framework Ref: RS.AN-5

If an HDO discovers (or is notified) of a high-risk cybersecurity vulnerability and cannot receive support from the medical device manufacturer to mitigate this risk, the HDO has recourse to contact the FDA directly to file a complaint concern about the vulnerability. FDA contact should be limited to critical or high-risk scenarios, especially those with the potential to cause harm to patients.

The Center for Devices and Radiological Health emergency contact information is provided below:

Email: CyberMed@fda.hhs.gov

Phone: (301) 796-8240 (24 hours x 7 days per week)

Sub-Practices for Large Organizations

9.L.A: Security Operations and Incident Response

NIST Framework Ref: PR.IP-9, DE.CM-8, DE.CM-1, DE.CM-7

Expanding on the SOC and IR processes found in **Cybersecurity Practice #8: Security Operations Center and Incident Response**, HDOs can provide additional monitoring, detection, and response activities around their medical device ecosystems. HDOs should monitor for malicious activity into and within the segment using the segmentation strategy outlined previously. To provide visibility into the daily operations of the medical device systems, the following sources should be configured to send activity and access logs to the HDO's log management systems, SIEMs, or both:

- Firewalls providing segmentation to the medical device network segment
- Information systems that control the operation of the medical devices
- The full context of possibly impacted devices, including devices only intermittently connected or yet to be onboarded (as these devices are still susceptible to vulnerability if left uncorrected)
- Netflow data from the medical device network segment
- Intrusion prevention systems in front of the medical device network segment
- Logs from any deception technology deployed in the medical device network segment

Security Orchestration and Automated Response (SOAR)

HDOs should strive to consolidate all device information into one cloud-based CMMS. By replacing multiple maintenance management systems and databases containing disparate data elements into on CMMS, an HDO can position itself for a single device inventory that is integrated with ADS solutions to orchestrate the remediation of cybersecurity events. This includes preventative maintenance, corrective maintenance, contract, cost of ownership, capital planning, asset discovery, security data, and events.

This CMMS of consolidated data are used to correlate events and vulnerabilities against device records from the NIST Cybersecurity Framework 1.1, NVD, CPE, and Mitre CWE.[97] For additional preparedness information refer to the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook.[98]

Security events can be provided in a shared view to healthcare technology management (HTM) and IT teams, showing the device(s) affected, the device owner and the device location, and the latest software and firmware versions. Rules-based identification algorithms can correlate all affected devices by the event or vulnerability and information like whether the device generates PHI data or stores PHI data.

Just as the clinical engineering team responds to preventative maintenance work orders in the CMMS system, HTM and network engineers can respond to a CMMS' security maintenance work orders.

97 *Cybersecurity Framework Version 1.1*, NIST (April 2018), https://www.nist.gov/cyberframework/framework.
"National Vulnerability Database," NIST (Accessed June 2, 2022), https://nvd.nist.gov/.
"Common Platform Enumerations (CPE)," NIST National Vulnerability Database (NVD) (Accessed June 2, 2022), https://nvd.nist.gov/products/cpe/search.
"Common Weakness Enumeration (CWE)," MITRE (Accessed June 2, 2022), https://cwe.mitre.org/.

98 "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook," MITRE (October 2018), https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and.

Coordinated remediation processes (via workflow management) provides security context and event impact, including what patch, configuration change, or mitigating controls are required to then determine the remediation priority.

Baselining Devices

Practice **8.L.D: Baseline Network Traffic** specified the need for understanding device communications. Monitoring the communications of medical devices is imperative to establishing their security. Once an HDO has identified all connected medical device assets, determining its purpose in the enterprise and understanding its normal behavior patterns is the next step in effective asset management. Mapping communications patterns and baselining device behavior is crucial to identifying anomalous behaviors. The behavior of each device must be understood to ascertain the degree of exposure to internal and external threats. These pieces of data are extremely difficult to obtain without automated tools..

Network Behavior

- Does the device communicate with the manufacturer for updates and patches?
- With what other devices is it communicating?
- Is the device type isolated to communication within the VLAN?
- Are communications normal for this device type?

Understanding the clinical context with respect to medical device cybersecurity is imperative. Beyond security, devices containing ePHI are required to be identified as a part of a HIPAA Risk Assessment. Consider the following:

Clinical Context

- Does the device transfer or store PHI?
- What is the consequence of failure—inappropriate therapy or misdiagnosis?
- What is the equipment class? Diagnostic?
- Which connections are clinical and non-clinical?

Security efforts must avoid interfering with critical clinical dataflows. However, once organizations can recognize these clinical workflows, the cybersecurity or HTM will be able to identify anomalies that could negatively impact patient care (resulting in direct patient harm).

Profiling and Grouping Devices

Managing devices at a group level is necessary to effectively manage tens of thousands of medical device requirements. Healthcare organizations need to collect a wide range of data on every connected device to group and compare devices on the network. This includes decoding dozens of device and industry-specific protocols to analyze detailed application-level behavior. Traditional security tools are limited to traditional protocols. Determining normal communications is challenging.

Determining normal communications within a device type by comparing communication flows is near impossible with traditional security tools. As an example, XYZ Health Systems has 100 Infusion Pumps, 99 of which are talking to the manufacturer in India and 1 is communicating with someone in Kiev.

ADS solutions are helping healthcare organizations reduce their attack surface by providing a clear understanding of what is on the network and controlling unnecessary communications and services. By passively monitoring device communications, organizations can associate attributes to the device: ports,

services, and protocols. These new attributes, or data elements, can be used to index and better manage the hardware assets in the asset inventory.

Organizations can automatically baseline the behavior of devices in the network as well as known behavior of similar devices. ADS solutions can baseline what other assets with which a device needs to communicate to accomplish its function. It can understand which protocols are used, verifying the communications are safe and not part of threat activity. Cybersecurity or HTM can create detailed policies/rules that will limit a device's communication to only those required to perform its given function. See the **Segmentation** section of **9.M.D: Network Management** for more detail on creating policies and rules.

Mapping the device communication flow allows ADS solutions to provide actionable insights across millions of devices within healthcare's hyper-connected enterprise. To accomplish this, it requires comprehensive real-time collection, correlation, and analysis of vast amounts of information about each device.

Deep Packet Inspection

Data packets transmitted throughout networks contain far more contextual than merely the sender and recipient devices. Captured network traffic is analyzed by ADS tools to retrieve rich data from devices, including:

- Device classification/grouping: manufacturer, device type, model, modality, and serial number
- Operating system information: software version, patches, components, and antivirus software
- Network information: VLAN/subnet, wireless access points, connectivity, switch ports, and comparisons between peer devices

Analysis of device communication data from deep packet inspection can reveal the transmission "flows" to and from each device monitored by the ADS. Such granularity allows IT and HTM personnel to visualize device interactions from varying levels or perspectives, such as:

- ***Device level flow:*** location, connection attempts, last connection, usage, sessions, and data rate
- ***Communications flow:*** baseline behavior, group comparisons, and anomalies
- ***Internal communications:*** malware signatures
- ***External communications:*** real-time comparison of device patterns, and communication with hostile sites

ADS solutions are designed to collect and analyze device and system data from multiple sources within the enterprise, including:

- Network infrastructure data from switches, routers, WLAN controllers, NAC solutions, etc.
- On-demand vulnerability scans for onboarding as well as information collected from other periodic vulnerability scan reports
- Device probes like Simple Network Mapping Protocol (SNMP) for inherent device information from various MIB repositories
- Protocol decodes of proprietary protocols like DICOM, Modbus, and patient monitoring systems
- User and location information (including Active Directory users with roles and privileges, and location feeds, etc.)

- Full packet capture data from backbone core routers) including all file transfers, HTTP sessions, peer-to-peer traffic, client-server traffic, and application-level interactions)
- Network layer control plane protocols (e.g., Dynamic Host Configuration Protocol [DHCP])
- Utilization and performance data like frequency and duration of operation and connection attempts
- Parsing results from well-known data plane signatures from security vendors

Using these logs as a source, plays can be enumerated and added into IR playbooks, as described below in Table 15.

Table 15. Incident Response Plays for Attacks Against Medical Devices

Play Category	Play	Description	Source Data
Reconnaissance	Vulnerability scanning sweep of medical device segment	Scan large numbers of vulnerabilities across the medical device network. May involve scanning a single server over multiple ports or scanning multiple servers over a single port.	• Medical device management system • IDS/IPS logs in front of the medical device network, configured to detect vulnerability scanning • Firewall logs in front of the medical device network • Netflow data from within the medical device network
Lateral Movement	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).	• Firewall logs in front of the medical device network • Network data from within medical device network
Lateral Movement	Triggered decoy within medical device network	Respond to decoy triggers being communicated from within or across the medical device network segment. These communications should not occur; they indicate malicious or broken processes.	• Deception technology logs from within the medical device network • Firewall logs in front of the medical device network • Network data from within the medical device network

If an HDO experiences a security incident and requires the assistance of the manufacturer, the HDO should leverage their contact information. This should have been established as part of the vulnerability disclosure program, outlined within sub-practice 9.L.A: Security Operations and Incident Response above.

9.L.B: Procurement and Security Evaluations

NIST Framework Ref: ID.SC

HDOs should establish a set of cybersecurity requirements during the acquisition of medical devices. These requirements should be memorialized in your organization's contracting processes and implemented through the supply chain and procurement functions. Cybersecurity requirements should be incorporated into prospective procurements through vendor requests for information (RFIs) or requests for proposals (RFPs). These requirements should include high-value items such as supported and patchable operating systems, AV or allowlisting, no hardcoded or default passwords, and minimal use of administrative privileges.

Organizations should set policies and procedures that require procurements of technology and integrations (including medical devices) to undergo security evaluations as part of the HDO's supply chain process. Implementing cybersecurity evaluation as part of the supply chain process provides an opportunity for your organization to understand, evaluate, and mitigate cyber risks prior to technology deployment. When a security evaluation is undertaken, the scope of the assessment should include all the other devices required for the device to perform its clinical functions. As an example, an assessment of an infusion pump system would evaluate both the infusion pump and the server to which it connects for the formulary update. Another example would an instance where the assessment of an MRI device would place the specialized workstations that control its operation in scope.

Security Evaluation

An initial phase of the medical device acquisition process should be a security evaluation of the device. This evaluation should uncover any risks or flaws in the current design of the medical device and establish transparent communications between stakeholders from the supply chain, clinical engineering, and manufacturing functions. The HDO should insist on receiving a MDS^2.[99] The MDS^2 is an industry standard format developed by the Health Information Management and Systems Society and the American College of Clinical Engineering that has been adopted by most manufacturers. It provides a list of comprehensive cybersecurity questions for medical devices, with responses from the manufacturer of the device in question. Questions in the MDS^2 include the following:

- Can this device display, transmit, or maintain private data (including electronic PHI/PII)?
- Can the medical device create an audit trail?
- Can users be assigned different privileged levels within an application based on 'roles' (e.g., guests, regular users, power users, administrators)?
- Can the device owner/operator reconfigure product security capabilities?

A copy of the latest MDS^2 can be found on the Association of Electrical Equipment and Medical Imaging Manufacturers' website.[100] Answers to these questions assist the HDO in completing a meaningful evaluation of the medical device. The HDO should also consider requesting an SBOM and an Enterprise Architecture Diagram to create a complete Vendor Assessment Package.

99 *Manufacturer Disclosure Statement for Medical Device Security*, NEMA (October 28, 2019), https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.

100 *The Association of Electrical Equipment and Medical Imaging Manufacturers (MDS^2) form HN 1-203, rev.2019*, NEMA (2019), https://www.nema.org/Standards/ComplimentaryDocuments/MDS2-Worksheet.xlsx.

The HTM collaborates with the security team to triage each device during the intake process. It is often beneficial to break the type of request into four categories:

- New Device—Unknown Risk
- Repeat Purchase—Unknown Risk
- Repeat Purchase—Known Risk
- No Security Assessment Required

This will allow the HDO to identify mitigating controls determined to stop new risk being entered into the environment. By focusing the HDO's limited resources on devices with "unknown risk", this process will focus efforts to reduce the new entering the system risk during the onboarding process. The product of the risk assessment process should be a profile of remediation plans to reduce each risk associated with that specific device.

Risk Scoring

Current methods for analyzing identified cyber vulnerabilities tend to apply to traditional IT and focus on the impact to a system's confidentiality, integrity, and availability (CIA) to discern end-user risks. The CVSS score is designed to provide an overall measurement that can be used for making HTM decisions helping to prioritize mitigation efforts in a consistent and measurable manner. Although sufficient for evaluating traditional IT systems, this scoring system fails to consider the operational ramifications for complex systems-of-systems like those found in a clinical environment.

The risk scoring system does not adequately consider the context of the environment for identified vulnerabilities. Consequently, organizations may improperly prioritize mitigation efforts. For example, while the CVSS evaluates the severity of an identified vulnerability in the context of system impact, for medical devices, it does not take into consideration the impact to patient safety—the true indicator of the severity of the vulnerability.

ADS solutions should be considered since they provide a multi-factorial risk score for every device on the network. These factors include the probability of a compromise, criticality, CVE, device properties, connectivity, etc. These factors are combined into a comprehensive, clinical network aware, context sensitive vulnerability management platform based on the needs of each device.

Contract Negotiation

Contracts are an essential component of good risk reduction when it comes to medical devices. It is beneficial for the HDO's cybersecurity team to review and provide input towards the contract with the manufacturer. This should occur in tandem with the supply chain and legal. Negotiations should highlight key security requirements from the HDO. These requirements should reference the FDA's *Postmarket Management of Cybersecurity for Medical Devices* guidance and industry standards describing components that are critical for the safe operation of the devices.[101] Armed with the results of the cybersecurity evaluation, scenarios to resolve any unmitigated risks should be included in the contracting process to limit the HDO's liability, especially with constraints around the HDO's ability to alter the medical devices. The Health Sector Coordinating Councils' Joint Security Workgroup released a publication titled *Model*

101 *Postmarket Management of Cybersecurity in Medical Devices*, Food and Drug Administration (FDA) (October 1, 2018), https://fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

Contract-language for Medtech Cybersecurity (MC2).[102] In this publication, HDOs and MDMs provide agreed upon contract language and a maturity model. This is designed to assist purchase contract negotiations providing a clearer reference for obligations, accountability, and liability.

Additionally, procurement should be notified of device performance and risks discovered after the contracting process when a device is in use. Mechanisms for communication of these vulnerabilities found in existing devices should be conveyed back to procurement to include in the front-end security evaluation and standard contract language.

SBOM

The HDO should request an SBOM as part of the procurement process. The SBOM is a list of software components that the medical device comprises. It can be thought of as a list of software libraries that make up the device, like the ingredients of a recipe. Understanding the software libraries that make up the device allows the HDO to comprehend the impact of vulnerabilities announced by the NVD.

End of life (EOL)/End of support (EOS)

Over time, the effectiveness of medical devices will diminish, especially as hardware and software ages and is eventually decommissioned. As part of the evaluation of these devices, manufacturers should disclose to the HDO their life expectancy, which forms part of the HDO's cybersecurity management plan. The plan should include an expectation for when the EOL and EOS of the devices will occur. If there are no EOLs or EOSs established, as best practice, the manufacturers should try to provide the HDO at least three years in advance of EOL or EOS. HDOs are responsible for making risk-based decisions about devices nearing EOL or EOS. In most cases, when a device becomes unsupported, or legacy, the device should be replaced as part of established asset refresh cycles. In some cases, it is not possible to replace legacy devices due to financial or other resource constraints. If this is the case, the HDO should implement compensating controls- with the understanding that the devices will no longer be supported by the manufacturer, and their decommissioning should be strategically planned.

In 2019, the Health Sector Coordinating Council released a new publication, the Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM).[103] This publication describes processes and techniques for managing all third-party risk. The techniques provided will also assist HDOs in medical device procurement.

Key Mitigated Threats

1. Attacks against network connected medical devices

102 *Model Contract-language for Medtech Cybersecurity (MC2)*, Healthcare & Public Health Sector Coordinating Councils (HSCC) (March 2022), https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/.

103 *Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)*, Healthcare & Public Health Sector Coordinating Councils (HSCC) (September 2020), https://healthsectorcouncil.org/hic-scrim-v2/.

Suggested Metrics

- ***Number of medical devices not currently segmented on wireless or wired networks, measured monthly.*** The goal is to limit medical devices on the general access network, data center network, or other locations that do not meet the requirements of specific network segmentation strategies.
- ***Number of unmitigated high-risk vulnerabilities on network connected medical devices, measured monthly.*** The goal is to reduce the number of unmitigated risks to as near zero as possible. Each high-risk vulnerability should have a remediation action plan, as defined in **Cybersecurity Practice #7: Vulnerability Management**.
- ***Number of medical devices procured that did not receive security evaluation, measured monthly.*** The goal is to reduce the number of procurement actions without security evaluation to as near zero as possible. Share this metric with your supply chain and clinical engineering departments to ensure the procure process is executing as intended.
- ***Number of medical devices that do not conform to basic endpoint protection cybersecurity practices, measured weekly.*** The goal is to reduce the number of medical devices that do not meet basic hygiene management practices or to implement practices for these devices. It is not always possible to reduce this number to zero. Mitigating factors should be employed to keep it as low as possible.
- ***Number of devices that have unknown risks due to lack of manufacturer-disclosed information, measured monthly.*** The goal is to ensure that device manufacturers have vulnerability disclosure programs and that your organization is privy to them.

Cybersecurity Practice #10: Cybersecurity Oversight and Governance

Areas of Impact
N/A

Medium Sub-Practices
10.M.A Policies
10.M.B Cybersecurity Risk Assessment and Management
10.M.C Security Awareness and Training

Large Sub-Practices
10.L.A Cyber Insurance

Key Threats Addressed
- Social engineering
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that may affect patient safety

405(d) Resources
- Prescription Poster: Cybersecurity Policies

Cybersecurity policies must be established for the workforce to understand how they are expected to behave with regard to cybersecurity. These policies should be written for the various user audiences that exist in your organization. It is important to recognize the differences between the general workforce user, IT user, and high-profile or high-risk users (e.g., finance, HR, or health information management).

To set proper expectations, organizational policies should support new cybersecurity hygiene controls. Without such policies, it may be unclear to the workforce what level of adherence is required and what activities put your organization at risk for the threat types discussed in this document.

Several policy templates have been provided in the HICP package's Resources and Templates document.

Sub-Practices for Medium-Sized Organizations

10.M.A: Policies

NIST Framework Ref: ID.GV-1

All organizations should maintain a baseline of core cybersecurity policies. These policies will define the expected behaviors of employees within your organization as it relates to cybersecurity practices. The policies should be reviewed periodically (and at regular intervals), defined by your organizational policy governance processes. A sample set of core policies is noted below in **Table 16**.

Table 16. Example Cybersecurity Policies for Consideration

Policy Name	Description	User Base
Roles and Responsibilities	Define all cybersecurity roles and responsibilities throughout your organization. This includes who will establish policy and who will implement and conduct security practices.	• All users
Education and Awareness	Define the mechanisms that will be used to train the workforce on cybersecurity practices, threats, and mitigations. Ensure education includes common cyber-attacks (such as phishing), lost/stolen devices, and methods for reporting suspicious behavior on individual computers.	• All users • Cybersecurity department
Acceptable Use/ Email Use	Describe actions that users are permitted and not permitted to take. Explicitly define how email is to be used.	• All users
Data Classification	Define how data are to be classified, with usage parameters around those classifications.	• All users
Personal Devices	Define your organization's position on the use of personal devices (i.e., BYOD). If these are permitted, establish expectations for how the devices will be managed.	• All users
Laptop, Portable Devices, and Remote Use	Define policies for the security of mobile devices and how they are to be used in a remote setting.	• All users • IT department
Incident Reporting and Checklist	Define user requirements to report suspicious activities within your organization. Define the responsibilities of the cybersecurity department for managing incidents.	• All users • Cybersecurity department
Disaster Recovery Plan (DRP)	Define the standard practices for recovering IT assets in the case of a disaster, including backup plans.	• IT department
IT Controls Policies	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
IT Acquisition Policy	Define the actions that must be taken to ensure proper identification and protection of all IT assets purchased by your organization.	• Supply chain/ procurement users • IT department
Social Media	Define what information about employee job they can include on accounts such as LinkedIn and others. Include recommendations for personal security settings.	• All users

10.M.B: Cybersecurity Risk Assessment and Management

NIST Framework Ref: ID.GV-1

A cybersecurity risk assessment helps your organization measure the likelihood of known threats and vulnerabilities compromising data and information assets. The risk assessment is a tool an organization can leverage to prioritize mitigation, addressing gaps in cybersecurity safeguards. This is used to put controls in place, reducing the risk to an acceptable level. A risk assessment is an important step in protecting your workers and organization, as well as complying with the law. A risk assessment helps you focus on the risks that really matter and prepare for what could go wrong. A risk assessment can help your organization understand potential risks, identify, and prioritize the risks that need to be addressed. This should not be done in a silo, rather as an organizational collaborative effort.

Managing the security risks associated with the healthcare industry's growing reliance on IT is a continuous challenge. HIPAA Security Rule, Centers for Medicare and Medicaid (CMS) Promoting Interoperability Program (formerly known as 'Meaningful Use'), and several states' data protection requirements for PII require healthcare organizations to conduct a formal risk analysis.

There are several frameworks available when conducting a risk assessment. The Office for Civil Rights (OCR) identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve. There are numerous methods of performing risk analysis and there is no single method or "best practice" that guarantees compliance with the HIPAA Security Rule.[104] Some examples of steps that might be applied in a risk analysis process are outlined in the NIST 800-30 Guide for Conducting Risk Assessments and the NIST Cybersecurity Framework.[105] Key to the effectiveness of the risk assessment is to identify all IT assets across your organization that handles PHI; and, to ensure the scope of the risk assessment captures the threats or vulnerabilities that could jeopardize the confidentiality, integrity, and availability of PHI. To do this, be sure to document:

- the threats and vulnerabilities to the information system;
- the potential impact and the effectiveness of existing safeguards and controls; and
- the likelihood that the threat or vulnerability could compromise data or information system assets.

It's important to remember that performing a risk assessment is an ongoing process and one in which an organization:

- regularly reviews its records to track access to PHI and detect security incidents;
- periodically evaluates the effectiveness of security measures that are in place; and
- regularly evaluates potential threats and vulnerabilities to PHI.

Healthcare organizations have struggled to find effective ways to ensure cybersecurity threats affecting their operations (driven by human action, mother nature, or technology flaw), are fully implemented

104 "Security Rule Guidance Material: Guidance on Risk Analysis," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

105 *SP 800-30 Rev. 1; Guide for Conducting Risk Assessments*, NIST (September 2012), https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.
"Cybersecurity Framework," NIST (Accessed June 1, 2022), https://www.nist.gov/cyberframework.

with appropriate controls to mitigate the risks. Enterprise Risk Management (ERM) can help identify, communicate, and categorize an organization's top risk areas.[106]

What do cybersecurity and privacy leaders need to know about the requirement for a risk assessment?

1. An RA should be the first requirement in any security program or framework. It informs and measures how well controls are working to mitigate risk and reduce liability. Not having an effective RA is like not having a foundation to your home. Without a risk assessment, you are making decisions based on an incomplete picture. In addition, both HIPAA Security Rule, and in some cases, state law requires cybersecurity management. The risk assessment is a good starting point to meeting your regulatory requirements.
2. An organization's leadership team plays a central role in ensuring resources are properly allocated to the most vulnerable areas of your organization. Proactive risk management will preserve and protect your organization's financial viability and human assets. Risk management processes should be put in place to protect your organization's limited budget and resources.
3. Understanding risk, policy imperatives, and architecture are the three pillars that any successful cybersecurity program should be built upon. Without each leg, the stool becomes unbalanced and falls.
4. Risk assessment informs and measures how well controls are working when mitigating risk and reducing lability. When performed correctly, it is the most useful tool for managing and reducing costs.
5. The risk assessment is almost always the first document requested by an investigator in an audit, compliance review or investigation of a breach. It answers two questions: did you know the risk in advance of the investigation; and did you plan to do anything about it?
6. Risk assessment is most beneficial when objectively conducted with due diligence.
7. Have a multi-disciplinary team to identify risks in an organization. A cross section of leaders will add value and identify something that others may not be aware of.
8. Calculate a risk rating for each threat to create a grading of risk (high, medium, low) relative to the overall impact and likelihood should the threat be activated.
9. A risk assessment is a tool for building trust in other third-party relationships and business partnerships. Being able to demonstrate your organization has completed a risk assessment is part of building trusted partnerships.
10. A risk assessment will foster effective customer communications regarding quality and safety issues, thereby reducing potential financial losses associated with claims.

Conducting a risk assessment correctly and periodically is critical to having and building an informed security program. Done well, it can reap many benefits from saving dollars, to avoiding compliance issues, and mitigating potential causes of disruption. Simply put, it helps protect your business and your investment.

106 Enterprise Risk Management is an effective organization-wide approach to addressing the full spectrum of your organization's significant risks by understanding the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos." See "Circular No. A-11." Executive Office of the President Office of Management and Budget (OMB). Section 260. August 2022. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf.

For more information on risk assessments, review the Security Risk Assessment (SRA) Tool from HHS ONC.[107]

Additionally, NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM) published in October 2020 is a comprehensive reference.[108]

10.M.C: Security Awareness and Training

NIST Framework Ref: ID.GV-1

Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for cybersecurity and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting cybersecurity awareness events.[109] Also consider creating a cyber champion program within your organization. This is a great way to increase engagement across your organization.

One method for establishing a Security Awareness Program is to designate key stakeholders within your organization as Cybersecurity Change Leaders, or Cybersecurity Ambassadors. It's recommended to select stakeholders who are engrained in the culture of your organization and have a passion for cybersecurity. Program elements might include the following:

- An onboarding and training program, with outlined roles and responsibilities of the stakeholder
- Development of cybersecurity awareness materials for delivery and distribution by the Cybersecurity Change Leader
- Regular touch points with Cybersecurity Change Leaders (either in a group setting or individually), to promote communication and maintain relationships
- Encouragement of feedback from the Cybersecurity Change Leader to the awareness team. Adjustment of outreach based on these recommendations, with special attention dedicated to understanding the best channels of cybersecurity awareness content

Please also refer to **Cybersecurity Practice #1: Email Protection Systems**, **1.M.D: Workforce Education**, for additional information on awareness and training programs.

107 "Security Risk Assessment Tool," Office of the National Coordinator for Health Information Technology (ONC) (February 15, 2022), https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

108 Kevin Stine, Stephen Quinn, and Robert Gardner, *NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)*, NIST (October 2020), https://csrc.nist.gov/publications/detail/nistir/8286/final.

109 "NIST Risk Management Framework: SP 800-53 Controls and SP 800-53B Control Baselines Resources for Implementers," NIST (Updated May 26, 2022), *https://csrc.nist.gov/Projects/risk-management/sp800-53-controls*.

Sub-Practices for Large-Sized Organizations

10.L.A: Cyber Insurance

NIST Framework Ref: ID.GV-1

Cyber insurance is no longer about risk transference through the purchase of a policy that an organization will hopefully never use. Due to the increase in ransomware attack impacts, cyber insurance providers have undertaken a significantly more proactive approach to both protect their businesses and the organizations they underwrite. The relationship has changed from a transactional activity to an ongoing relationship.

This approach aligns with the ongoing lifecycle of improving and maturing cybersecurity programs. Before the numerous ransomware attack payouts, insurance company questionnaires asked basic questions about system security, PCI-DSS compliance, and whether there were any reportable data breaches. They did not ask detailed questions on cybersecurity, or specific projects being undertaken to address threats. The cyber market is ever-changing. New countermeasures should be considered as cyber-attacks continue. In this new ongoing relationship, underwriters will ask more detailed questions about controls to address specific threats related to recent attacks (e.g., SolarWinds breach). You should expect to see the level of depth and scrutiny to continue to evolve. As such, it's recommended to consider the practices outlined in HICP as a starting place to prepare for underwriter questioning.

The threat of ransomware has now caused cyber insurance underwriters to consider numerous specific countermeasures to address threats before issuing coverage, including:

- MFA for offline and privileged access
- Email security that prevents harm from social engineering and/or malicious attachments and links
- Privileged access separation and management
- Air-gapped backups
- Continual vulnerability management
- Effective network segmentation of IoT and legacy devices
- EDR software
- Continual monitoring and threat response
- Drilling tabletop exercises
- Building and implementing downtime procedures for critical processes
- Frequency and level of detail of risk assessments
- Delivery of a continual risk management process
- Specific compliance standards (e.g., PCI-DSS)

What this means is that a relationship with an insurance provider is a good idea because it can help provide continual assurance in these areas. It is no longer possible to transfer all cyber risk via insurance because that presents too much risk to the insurance companies. However, working in partnership with them can help augment your organization's practices to address security requirements, while effectively managing premium costs.

When making the decision on coverage, consideration of the following is recommended:[110]

- How much coverage will be offered?
- Will there be coverage from several providers based on escalating costs, or just one provider?
- What is the deductible based on the coverage?
- What other services does your organization provide to complement the policy?
- Based on a risk assessment of your organization, how much will a computer systems failure cost? Many organizations that have had cyber-attacks were forced to pay tens of millions out of pocket because their insurance premium did not cover the costs.
- Do sub-limits apply for social engineering, ransomware attacks, reputational loss, or business loss due to system failures?

These services can include:

- ***Tabletop Exercise Facilitation:*** The broker can help facilitate services to conduct tabletop exercises to determine readiness in case of an attack.
- ***Digital Forensics/Incident Response (DFIR) Panel:*** A list of pre-approved companies to choose from to conduct DFIR services. However, unlike in the past, you will have to separately contract with these firms to reserve services. This is because the demand for qualified DFIR professionals is so high that unless you prepay for hours, you may not be able to get the professionals you need. You most likely will not be able to add your firm of choice to this list.
- ***Legal Panel:*** A list of pre-approved law firms to use in case of an incident. Pay close attention to these firms, who they have on staff and what experience that staff has in cybersecurity and healthcare.
- ***Security Risk Assessments:*** The broker can partner with (or provide themselves) security risk assessment services to help determine areas for improvement, and most importantly, determine what the premium should ideally be.

In summation, cyber insurance is an ongoing partnership used to continually improve your organization and ensure that needed services are present and available.

What Should Your Cyber Insurance Policy Cover?

Consider coverage for:

- Data breaches (like incidents involving theft of personal information)
- Cyber-attacks on your data held by vendors and other third-parties
- Cyber-attacks (like breaches of your network)
- Cyber-attacks that occur anywhere in the world (not only in the United States)
- Cyber-attacks determined to be nation-state attackers
- Cyber-attacks aided by insiders both intentional and unintentional
- Cyber-attacks that lead to extortion (ransomware attacks)
- Terrorist acts
- Cyber warfare

110 "Cyber Insurance," Federal Trade Commission (FTC) (Accessed June 1, 2022), https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/cyber-insurance.

Also, consider whether your cyber insurance provider will:

- Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- Provide coverage in excess of any other applicable insurance you have
- Offer a breach hotline that's available 24x7x365
- Provide access to third-party breach specialists, including forensics, independent legal counsel working on your behalf, not the cyber insurance provider, and incident remediation firms
- Require you to use specific vendors for IR
- Provide coverage for notification costs including printing, mailing, phone centers, and PR assistance
- Loss of business coverage or revenue

Key Mitigated Threats

1. Social engineering
2. Ransomware attacks
3. Loss or theft of equipment or data
4. Insider, accidental or malicious data loss
5. Attacks against network connected medical devices that may affect patient safety

Suggested Metrics

- ***Number of policies reviewed over a specified timeframe, suggested every three years.*** The goal is to establish a standard practice to review policies and to monitor compliance with this standard.
- ***Number of workforce members who review and sign off after reading policies over a specified timeframe, suggested yearly.*** The goal is to establish a standard practice for workforce members to review applicable policies and attest to the review, and for your organization to monitor compliance with this standard.

Appendix A: Acronyms and Abbreviations

Table 17. Acronyms and Abbreviations

Acronym/Abbreviation	Definition
ABAC	Attribute Based Access Control
AHIP	America's Health Insurance Plans
ASL	Assistant Secretary for Legislation
ASPR	Administration for Strategic Preparedness and Response
ASTM	American Society for Testing and Materials
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
AV	Antivirus
BYOD	Bring Your Own Device
CAB	Change Advisory Board
C2	Command and Control
CEO	Chief Executive Officer
CHIO	Chief Health Information Officer
CIO	Chief Information Officer
CIRT	Cybersecurity Incident Response Team
CISO	Chief Information Security Officer
CISSP	Certified Information Security Systems Professional
CMS	Centers for Medicare and Medicaid
CNSSI	Committee on National Security Systems Instruction
COO	Chief Operations Officer
CSA	Cybersecurity Act
CT	Computed Tomography
CVSS	Common Vulnerability Scoring System
DCC	Distributed Checksum Clearinghouse
DEP	Device Enrollment Program
DICOM	Digital Imaging and Communications in Medicine
DKIM	Domain Key Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication Reporting and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSRBL	Domain Name System Real-time Blackhole List
DoD	Department of Defense
DOS	Denial of Service
DRP	Disaster Recovery Plan

Acronym/Abbreviation	Definition
DSM	Direct Secure Messaging
EDR	Endpoint Detection and Response
EHR	Electronic Health Record
EMR	Electronic Medical Record
ePHI	Electronic Protected Health Information
ERP	Enterprise Resource Planning
FDA	Food and Drug Administration
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GINA	Genetic Information Nondiscrimination Act
HCIC	Health Care Industry Cybersecurity
HDO	Health Delivery Organization
HIDS	Host Based Intrusion Detection Systems
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Based Intrusion Prevention Systems
HIT	Health Information Technology
HITECH	Health Information Technology Economic and Clinical Health Act
HL7	Health Level Seven
HMO	Health Maintenance Organization
HPH	Health Care and Public Health
HR	Human Resources
HRSA	Health Resources and Services Administration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAM	Identity and Access Management
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICU	Intensive Care Unit
IDS	Intrusion Detection System
IHI	Individually Identifiable Health Information
INFOSEC	Information Security
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Intellectual Property or Internet Protocol

Acronym/Abbreviation	Definition
IPS	Intrusion Prevention Systems
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITAM	Information Technology Asset Management
LAN	Local Area Network
LANMAN	Local Area Network Manager
LIS	Laboratory Information Systems
LLC	Limited Liability Corporation
MAC	Media Access Control
MACRA	Medicare access and the Children's Health Insurance Program Reauthorization Act
MDM	Mobile Device Management
MDS2	Manufacturer Disclosure Statement for Medical Device Security
MFA	Multi-Factor Authentication
MIB	Management Information Base
MITRE	The MITRE Corporation
MRI	Magnetic Resonance Imaging
NAC	Network Access Control
NCI	National Cancer Institute
NIST	National Institute of Standards and Technology
NNCOE	NIST National Cybersecurity Center of Excellence
NVD	National Vulnerability Database
OCIO	Office of the Chief Information Officer
OCR	Office for Civil Rights
ONC	Office of the National Coordinator (for Healthcare Technology)
OS	Operating System
PCI-DSS	Payment Card Industry Data Security Standard
PCS	Patient Care Service
PHI	Protected Health Information
PII	Personally Identifiable Information
RADIUS	Remote Authentication Dial-In User Service (RADIUS)
RBAC	Rule Based Access Control
RDP	Remote Desktop Protocol
ROM	Read Only Memory
SAMHSA	Substance Abuse and Mental Health Services Administration

Acronym/Abbreviation	Definition
SBOM	Software Bill of Materials
SIEM	Security Incident and Event Management
SMB	Server Message Block
SME	Subject Matter Expert
S/MIME	Secure Multi-Purpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSN	Social Security Number
SSO	Single Sign On
STIX	Structure Threat Information eXpression
SVP	Senior Vice President
TAXII	Trusted Automated eXchange of Indicator Information
TLS	Transport Layer Security
TXT	Text
UBA	User Behavior Analytics
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
VAR	Value Added Reseller
VP	Vice President
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B: References

"4.1.9 Federal Information Security Management Act," NIH, https://grants.nih.gov/grants/policy/nihgps/html5/section_4/4.1.9_federal_information_security_management_act.htm.

2020 Data Breach Investigations Report (DBIR), Verizon, 2020, https://www.verizon.com/business/resources/reports/dbir/2020/.

"2021 Data Breach Investigations Report," Verizon, 2021, https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.

Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, *NIST Special Publication 800-167: Guide to Application Whitelisting*, National Institutes of Science and Technology (NIST), October 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

"Attribute Based Access Control," NIST Computer Security Resource Center, February 13, 2013, https://csrc.nist.gov/Projects/Attribute-Based-Access-Control.

"Bad Practices," CISA (Accessed June 2, 2022), https://www.cisa.gov/BadPractices.

Bill Mathers et al., "Implementing Least-Privilege Administrative Models," Microsoft Windows IT Pro Center, May 31, 2017, https://docs.microsoft.com/en-us/windows-server/identity/ad- ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

Brandon Vigliarolo, "Report: The IT Response to WannaCry," TechRepublic, July 25, 2017, https://www.techrepublic.com/article/report-the-it-response-to-wannacry/.

"California Consumer Privacy Act (CCPA)," State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.

"CIS Benchmarks," Center for Information Security, September 24, 2018, https://www.cisecurity.org/cis-benchmarks/.

"CIS Control 1: Inventory and Control of Hardware Assets," Center for Information Security Controls,d September 24, 2018, https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/.

"CIS Control 2: Inventory of Authorized and Unauthorized Software," Center for Internet Security Controls, September 24, 2018, https://www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-software/.

"CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers," Center for Information Security Controls, September 24, 2018. https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/.

"CIS Critical Security Control 12: Network Infrastructure Management," Center for Information Security Controls, June 2, 2022, https://www.cisecurity.org/controls/boundary-defense/.

"CIS Critical Security Control 18: Penetration Testing," Center for Internet Security, September 24, 2018, https://www.cisecurity.org/controls/penetration-testing.

"CISA Tabletop Exercises Packages," CISA, May 31, 2022, https://www.cisa.gov/cisa-tabletop-exercises-packages.

"CommHIT Information Sharing & Analysis Centers (ISACs)," CommunityHealth IT, May 31, 2022, https://www.communityhealthit.org/isacs/.

"Common Platform Enumerations (CPE)," NIST National Vulnerability Database (NVD), June 2, 2022, https://nvd.nist.gov/products/cpe/search.

"Common Vulnerability Scoring System version 3.1: Specification Document," FIRST, June 2, 2022, https://www.first.org/cvss/specification-document.

"Common Weakness Enumeration (CWE)," MITRE, June 2, 2022, https://cwe.mitre.org/.

"Controlling Root Access," Redhat Customer Portal, September 24, 2018, https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec- controlling_root_access.

"Cyber Hygiene Services," CISA, June 2, 2022, https://www.cisa.gov/cyber-hygiene-services.

"Cyber Insurance," Federal Trade Commission (FTC), June 1, 2022, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/cyber-insurance.

"Cybersecurity," FDA, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

Cybersecurity Framework Version 1.1, NIST, April 2018, https://www.nist.gov/cyberframework/framework.

"Cybersecurity Framework," NIST, June 1, 2022, https://www.nist.gov/cyberframework.

"Cyber Storm: Securing Cyber Space," CISA, May 26, 2022, https://www.cisa.gov/cyber-storm-securing-cyber-space.

David Swift, *Successful SIEM and Log Management Strategies for Audit and Compliance*, The SANS Institute, November 9, 2010, https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528.

"DEP Guide," Apple, October 2015, https://www.apple.com/business/site/docs/DEP_Guide.pdf.

"DHS Cyber Tabletop Exercise (TTX) for the Healthcare Industry [Exercise Materials]," Homeland Security Digital Library, 2013, https://www.hsdl.org/?abstract&did=789781.

"Does the Security Rule allow for sending electronic PHI (e-PHI) in an email over the Interent? If so, what protections must be applied?," HHS OCR. July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html.

Erika McCallister, Tim Grance, and Karen Scarfone, *NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

Erik Decker, et al., "Toolkit for Developing and Identity and Access Management (IAM) Program," EDUCAUSE May 7, 2013, https://library.educause.edu/resources/2013/5/toolkit-for-developing-an-identity-and-access-management-iam-program.

Executive Order No. 14028, May 12, 2012, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

"Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule," SAMHSA, https://www.samhsa.gov/newsroom/press-announcements/202007131330.

"Family Educational Rights and Privacy Act (FERPA)," US Department of Education, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

"Field Offices," FBI. May 31, 2022, https://www.fbi.gov/contact-us/field-offices.

"Fraud & Abuse Laws," HHS Office of Inspector General, https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/#:~:text=The%20Physician%20Self%2DReferral%20Law%2C%20commonly%20referred%20to%20as%20the,relationship%2C%20unless%20an%20exception%20applies.

Gavin O'Brien et al., *NIST Special Publication 1800-8: Securing Wireless Infusion Pumps In Healthcare Delivery Organizations*, NIST. August 2018. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.

"General Data Protection Regulation: GDPR," Intersoft Consulting, https://gdpr-info.eu/.

"Genetic Information," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html.

Gordon Fraser, "A Practical Example of Incident Response to a Network Based Attack," The SANS Institute. August 16, 2017. https://www.sans.org/white-papers/37920/.

"Gramm-Leach-Bliley Act," FTC, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

Health-ISAC (H-ISAC), https://h-isac.org/.

Healthcare Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent, Healthcare & Public Health Sector Coordinating Council (HSCC). June 2019. https://healthsectorcouncil.org/workforce-guide/.

Health Industry Cybersecurity — Matrix of Information Sharing Organizations (HIC-MISO), HSCC. Accessed May 31, 2022. https://healthsectorcouncil.org/hic-miso/.

Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM), Healthcare & Public Health Sector Coordinating Councils (HSCC). September 2020. https://healthsectorcouncil.org/hic-scrim-v2/.

"Health Sector Cybersecurity Coordination Center (HC3)," HHS.gov. March 31, 2022. https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts.

"HITECH Act Enforcement Interim Final Rule," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

"ICS-CERT Advisories," CISA. June 2, 2022. https://www.cisa.gov/uscert/ics/advisories.

IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software, ISO, September 2021, https://www.iso.org/standard/72026.html.

"Incident Response Training," CISA. May 26, 2022. https://www.cisa.gov/incident-response-training#.

ISAO Standards Organization, https://www.isao.org/.

KC Cross, Denise Vangel, and Meera Krishna, "Use DMARC to Validate Email in Office 365," Microsoft TechNet. October 8, 2017. https://technet.microsoft.com/en- us/library/mt734386(v=exchg.150).aspx.

KC Cross and Denise Vangel, "Configure Your Spam Filter Policies," Microsoft TechNet. December 13, 2017. https://technet.microsoft.com/en- us/library/jj200684(v=exchg.150).aspx.

Keith Ferrazzi, "7 Ways to Improve Employee Development Programs," Harvard Business Review. July 31, 2015. https://hbr.org/2015/07/7-ways-to-improve-employee-development-programs.

Kevin Stine, Stephen Quinn, and Robert Gardner, *NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)*, NIST. October 2020. https://csrc.nist.gov/publications/detail/nistir/8286/final.

"Learn the Process," The Joint Commission, https://www.jointcommission.org/accreditation-and-certification/become-accredited/learn-the-process/.

"MACRA," Centers for Medicare and Medicaid Services (CMS), https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/MACRA-MIPS-and-APMs/MACRA-MIPS-and-APMs#:~:text=The%20Medicare%20Access%20and%20CHIP,clinicians%20for%20value%20over%20volume.

Manufacturer Disclosure Statement for Medical Device Security, NEMA. October 28, 2019. https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.

Medical Device and Health IT Joint Security Plan, HSCC. January 2019. https://healthsectorcouncil.org/the-joint-security-plan/.

Michael Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet February 2, 2015. https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

Michael Stone et al., *NIST Special Publication 1800-5b: IT Asset Management*, NIST. October 2015. https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5b-draft.pdf.

"Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0," HHS Guidance Portal, https://www.hhs.gov/guidance/document/minimum-acceptable-risk-standards-exchanges-mars-e-20.

MITRE ATT&CK®. May 26, 2022. https://attack.mitre.org/.

Model Contract-language for Medtech Cybersecurity (MC2), Healthcare & Public Health Sector Coordinating Councils (HSCC). March 2022. https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/.

Murthy Raju, "Using RBL and DCC for Spam Protection," Linux.com. June 14, 2007. https://www.linux.com/news/using-rbl-and-dcc-spam-protection.

"National Vulnerability Database," NIST. June 2, 2022. https://nvd.nist.gov/.

"National Vulnerability Database: CVSS," NIST. Accessed September 24, 2018. https://nvd.nist.gov/vuln-metrics/cvss.

"NIST Risk Management Framework: SP 800-53 Controls and SP 800-53B Control Baselines Resources for Implementers," NIST. May 26, 2022. *https://csrc.nist.gov/Projects/risk-management/sp800-53-controls*.

"NTIA Software Component Transparency," National Telecommunications and Information Administration (NTIA) April 28, 2021. https://www.ntia.doc.gov/SoftwareTransparency.

NIST Special Publication NIST SP 800-66r2 ipd Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide, NIST. July 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf.

NIST Special Publication 1800-24: Securing Picture Archiving and Communication Systems (PACS): Cybersecurity for the Healthcare Sector, NIST, December 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf.

ONC's Cures Act Final Rule, https://www.healthit.gov/curesrule/.

"OWASP Top 10 - 2017: Ten Most Critical Web Application Security Risks," OWASP, 2017, https://raw.githubusercontent.com/OWASP/Top10/master/2017/OWASP%20Top%2010-2017%20(en).pdf.

Patrick Kral, "The Incident Handlers Handbook," The SANS Institute, February 21, 2012, https://www.sans.org/white-papers/33901/.

Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *NIST Special Publication 800-63: Digital Identity Guidelines*, NIST (June 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.

Paul A. Grassi et al., *NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

Paul Cichonski et al., *NIST Special Publication 800-61r2: Computer Security Incident Handling Guide*, NIST August 2012, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

"PCI DSS v4.0 Resource Hub," PCI Security Standards Council, https://www.pcisecuritystandards.org/.

Peter Czanik and BalaBit, "The 6 Categories of Critical Log Information," S!NS Technology Security Laboratory, last modified 2013, February 4, 2018, https://www.sans.edu/cyber-research/security-laboratory/article/sixtoplogcategories.

Postmarket Management of Cybersecurity in Medical Devices, Food and Drug Administration (FDA) October 1, 2018, https://fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

"Principles and Practices for Medical Device Cybersecurity," IMDRF Medical Device Cybersecurity Working Group, March 2020, https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf.

"Ransomware Guide," MS-ISAC and CISA, September 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

"Registration Requirements," SAMHSA, https://www.samhsa.gov/grants/applying/registration-requirements.

"SAFER Guide: Contingency Planning," ONC HealthIT, July 2016, https://www.healthit.gov/sites/default/files/safer/guides/safer_contingency_planning.pdf.

"Security Risk Assessment Tool," Office of the National Coordinator for Health Information Technology (ONC), February 15, 2022, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

"Security Rule Guidance Material: Guidance on Risk Analysis," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

"Security Technical Implementation Guides (STIGs)," Information Assurance Support Environment (IASE), September 24, 2018, https://public.cyber.mil/stigs/.

SP 800-30 Rev. 1; Guide for Conducting Risk Assessments, NIST, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

StopRansomware.gov, CISA, May 31, 2022, https://www.cisa.gov/stopransomware.

The Association of Electrical Equipment and Medical Imaging Manufacturers (MDS2) form HN 1-203, rev.2019, NEMA, 2019, https://www.nema.org/Standards/ComplimentaryDocuments/MDS2-Worksheet.xlsx.

"The HIPAA Privacy Rule," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.