HEALTHCARE AND PUBLIC HEALTH SECTOR-SPECIFIC

CYBERSECURITY PERFORMANCE GOALS

STRENGTHENING THE CYBERSECURITY OF THE HEALTHCARE SECTOR AND KEEPING PATIENTS SAFE AND SECURE

HEALTHCARE AND PUBLIC HEALTH SECTOR-SPECIFIC

CYBERSECURITY PERFORMANCE GOALS

STRENGTHENING THE CYBERSECURITY OF THE HEALTHCARE SECTOR AND KEEPING PATIENTS SAFE AND SECURE

The Department of Health and Human Services (HHS) helps the Healthcare and Public Health (HPH) critical infrastructure sector prepare for and respond to cyber threats, adapt to the evolving threat landscape, and build a more resilient sector. As outlined in the HHS Healthcare Sector Cybersecurity concept paper, HHS is publishing these voluntary healthcare specific **Cybersecurity Performance Goals (CPGs)** to help healthcare organizations prioritize implementation of high-impact cybersecurity practices. The HPH CPGs are designed to better protect the healthcare sector from cyberattacks, improve response when events occur, and minimize residual risk. HPH CPGs include both *essential goals* to outline minimum foundational practices for cybersecurity performance and *enhanced goals* to encourage adoption of more advanced practices.

Linking Cybersecurity and the HPH CPGs

In March 2023, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released its Cross-Sector CPGs which serve as a national, critical-infrastructure cybersecurity baseline. HHS, in collaboration with CISA and industry, have adapted CISA's CPGs to develop voluntary HPH CPGs.

These goals are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizations in particular, can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They were built off the chassis of CISA's CPGs and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the National Cybersecurity Strategy). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as identified in the 2023 Hospital Cyber Resiliency Landscape Analysis.

These resiliency-based goals complement HHS' ongoing work to improve cybersecurity in medical devices through the Food and Drug Administration's establishment of pre-market cybersecurity requirements and recommendations for medical devices, and promote cybersecurity through the Office for Civil Rights' continuous administration and enforcement of the Health Insurance Portability and Accountability Act Privacy, Security, and Breach notification rules.

Navigating the HPH CPGs

The HPH CPGs are designed to ensure layered protection at different stages of the attack chain, or points in digital systems that can be exploited, which is crucial to mitigating the impacts of cybersecurity incidents if and when they occur. They are divided into two categories of goals:

Essential Goals to help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.

Enhanced Goals to help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

ESSENTIAL GOALS
to help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.

Mapping HPH CPGs to Health Industry Cybersecurity Practices to Facilitate Implementation

Mitigate Known Vulnerabilities
7.M.A, 7.M.B, 2.M.A

Email Security
1.M.A, 1.M.B, 1.M.D

Multifactor Authentication
3.M.A, 3.M.C, 3.M.D

Basic Cybersecurity Training
1.M.D, 10.M.C

Strong Encryption
1.M.C

Revoke Credentials
3.M.B, 3.M.C

Basic Incident Planning and Preparedness
10.M.A, 8.M.B, 4.M.D

Unique Credentials
3.M.A, 3.M.B, 3.M.C, 3.M.D

Separating User and Privileged Accounts
3.M.A, 3.M.B, 3.M.C, 3.M.D

Vendor/Supplier Cybersecurity Requirements
10.M.B

Essential Goals

The Essential Goals* are as follows:

- **Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.
- **Email Security:** Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud.
- **Multifactor Authentication:** Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet.
- **Basic Cybersecurity Training:** Ensure organizational users learn and perform more secure behaviors.
- **Strong Encryption:** Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion.
- **Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers:** Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly.
- **Basic Incident Planning and Preparedness:** Ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents.
- **Unique Credentials:** Use unique credentials inside organizations' networks to detect anomalous activity and prevent attackers from moving laterally across the organization, particularly between IT and OT networks.
- **Separate User and Privileged Accounts:** Establish secondary accounts to prevent threat actors from accessing privileged or administrative accounts when common user accounts are compromised.
- **Vendor/Supplier Cybersecurity Requirements:** Identify, assess, and mitigate risks associated with third party products and services.

*See appendix 1 for more details on the essential CPGs.

ENHANCED GOALS
to help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

Mapping HPH CPGs to Health Industry Cybersecurity Practices to Facilitate Implementation

Asset Inventory
5.M.A, 5.M.B, 5.M.C, 7.M.C

Third Party Vulnerability Disclosure
10.M.B

Third Party Incident Reporting
10.M.B, 7.M.D, 8.M.C

Cybersecurity Testing
7.L.A, 7.L.C, 8.M.C

Cybersecurity Mitigation
8.M.C, 7.M.D, 7.L.B

How to Respond to Relevant Threats
2.L.C

Network Segmentation
6.M.B

Centralized Log Collection
8.M.A, 8.M.B

Centralized Incident Planning and Preparedness
8.M.A, 8.M.B

Configuration Management
7.M.D

Enhanced Goals

The Enhanced Goals** are as follows:

- **Asset Inventory:** Identify known, unknown (shadow), and unmanaged assets to more rapidly detect and respond to potential risks and vulnerabilities.
- **Third Party Vulnerability Disclosure:** Establish processes to promptly discover and respond to known threats and vulnerabilities in assets provided by vendors and service providers.
- **Third Party Incident Reporting:** Establish processes to promptly discover and respond to known security incidents or breaches across vendors and service providers.
- **Cybersecurity Testing:** Establish processes to promptly discover and responsibly share vulnerabilities in assets discovered through penetration testing and attack simulations.
- **Cybersecurity Mitigation:** Establish processes internally to act quickly on prioritized vulnerabilities discovered through penetration testing and attack simulations.
- **Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (TTP):** Ensure organizational awareness of and ability to detect relevant threats and TTPs at endpoints. Ensure organizations are able to secure entry and exit points to its network with endpoint protection.
- **Network Segmentation:** Mission critical assets are separated into discrete network segments to minimize lateral movement by threat actors after initial compromise.
- **Centralized Log Collection:** Collection of necessary telemetry from security log data sources within an organization's network that maximizes visibility, cost effectiveness, and faster response to incidents.
- **Centralized Incident Planning and Preparedness:** Ensure organizations consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios.
- **Configuration Management:** Define secure device and system settings in a consistent manner and maintain them according to established baselines.

**See appendix 2 for more details on the enhanced CPGs.

APPENDIX 1: Essential CPGs

Essential Goals						
ID	**Goals**	**Desired Outcomes (NIST CSF V1.1)**	**HICP Practices**	**HICP Sub-Practices**	**NIST 800-53 REV5 Controls**	**Threats Mitigated**
1	**Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented **DE.CM-8:** Vulnerability scans are performed **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) **ID.RA-6:** Risk responses are identified and prioritized **PR.AC-3:** Remote access is managed	**Vulnerability Management** **Endpoint Protection**	**Host/Server-Based Scanning** 7.M.A **Web Application Scanning** 7.M.B **Basic Endpoint Protection Controls** 2.M.A	CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 RA-1, RA-3, RA-5, SI-2 CA-5, PM-4, PM-9, PM-28, RA-7 CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 AC-1, AC-17, AC-19, AC-20, SC-15	Ransomware Social engineering Insider threat Attacks on network connected devices
2	**Email Security:** Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud	**PR.DS-5:** Protections against data leaks are implemented **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction **PR.PT-4:** Communications and control networks are protected	**Email Protection Systems**	**Basic Email Protection Controls** 1.M.A **Workforce Education** 1.M.D **Multifactor Authentication for Email Access** 1.M.B	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 SC-8, SC-11 AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4 AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11	Ransomware or other malware delivered via email, spoofing email attempts Account takeover
3	**Multifactor Authentication:** Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet	**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**Identity and Access Management**	**Identity** 3.M.A **Authentication** 3.M.C **Multifactor Authentication for Remote Access** 3.M.D	AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11 IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12	Lateral movement within an environment Account takeover

Essential Goals

ID	Goals	Desired Outcomes (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
4	**Basic Cybersecurity Training:** Ensure organizational users learn and perform more secure behaviors	**PR.AT-1:** All users are informed and trained **PR.AT-2:** Privileged users understand their roles and responsibilities **PR.AT-3:** Third party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**Email Protection Systems** **Cybersecurity Oversight and Governance**	**Workforce Education** 1.M.D **Security Awareness and Training** 10.M.C	AT-2, PM-13, PM-14 AT-3, PM-13	Ransomware Social engineering Insider threat Attacks on network connected devices
5	**Strong Encryption:** Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion	**PR.DS-2:** Data-in-transit is protected **PR.DS-5:** Protections against data leaks are implemented	**Email Protection Systems**	**Email Encryption** 1.M.C	SC-8, SC-11	Inbound attack email filtering Data theft
6	**Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers:** Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**Identity and Access Management**	**Provisioning, Transfers and Deprovisioning Procedures** 3.M.B **Authentication** 3.M.C	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21	Lateral movement within an environment Account takeover
7	**Basic Incident Planning and Preparedness:** Ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents	**RS.RP-1:** Response plan is executed during or after an incident **RS.CO-1:** Personnel know their roles and order of operations when a response is needed **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**Cybersecurity Oversight and Governance** **Security Operations Center and Incident Response**	**Backup Strategies** 4.M.D **Policies** 10.M.A **Incident Response** 8.M.B	CP-10, IR-4, IR-8 CP-2, CP-3, IR-3, IR-8 CP-2, IR-4, IR-8 SI-5, PM-15	Patient safety Business continuity Unplanned operational downtime

Essential Goals

ID	Goals	Desired Outcomes (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
8	**Unique Credentials:** Use unique credentials inside organizations' networks to detect anomalous activity and prevent attackers from moving laterally across the organization, particularly between IT and OT networks	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**Identity and Access Management**	**Identity** 3.M.A **Provisioning, Transfers, and Deprovisioning Procedures** 3.M.B **Authentication** 3.M.C **Multifactor Authentication for Remote Access** 3.M.D	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12	Lateral movement within an environment
9	**Separate User and Privileged Accounts:** Establish secondary accounts to prevent threat actors from accessing privileged or administrative accounts when common user accounts are compromised	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**Identity and Access Management**	**Identity** 3.M.A **Provisioning, Transfers, and Deprovisioning Procedures** 3.M.B **Authentication** 3.M.C **MultiFactor Authentication for Remote Access** 3.M.D	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	Lateral movement within an environment Account takeover Lateral movement
10	**Vendor/Supplier Cybersecurity Requirements:** Identify, assess, and mitigate risks associated with third party products and services	**ID.SC-3:** Contracts with suppliers and third party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	**Cybersecurity Oversight and Governance**	**Cybersecurity Risk Assessment and Management** 10.M.B	SA-4, SA-9, SR-2, SR-3, SR-5	Supply chain risk

APPENDIX 2: Enhanced CPGs

Enhanced Goals						
ID	**Goals**	**Desired Outcome (NIST CSF V1.1)**	**HICP Practices**	**HICP Sub-Practices**	**NIST 800-53 REV5 Controls**	**Threats Mitigated**
11	**Asset Inventory:** Identify known, unknown (shadow), and unmanaged assets to more rapidly detect and respond to potential risks and vulnerabilities	**ID.AM-1:** Physical devices and systems within the organization are inventoried **ID.AM-2:** Software platforms and applications within the organization are inventoried **ID.AM-4:** External information systems are catalogued **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	**IT Asset Management**	**Inventory of Endpoints and Servers** 5.M.A **Procurement** 5.M.B **Secure Storage for Inactive Devices** 5.M.C **System Placement and Data Classification** 7.M.C	CM-8, PM-5 CM-8 AC-20, PM-5, SA-9 AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	Shadow assets not covered under critical process like vuln. mgmt. Shadow IT
12	**Third Party Vulnerability Disclosure:** Establish processes to promptly discover and respond to known threats and vulnerabilities in assets provided by vendors and service providers	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**Cybersecurity Oversight and Governance**	**Cybersecurity Risk Assessment and Management** 10.M.B	PM-30, SA-9, SR-1, SR-2, SR-3, SR-5 PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6	Supply chain risk
13	**Third Party Incident Reporting:** Establish processes to promptly discover and respond to known security incidents or breaches across vendors and service providers	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-3:** Contracts with suppliers and third party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	**Cybersecurity Oversight and Governance** **Vulnerability Management** **Security Operations Center and Incident Response**	**Cybersecurity Risk Assessment and Management** 10.M.B **Patch Management, Configuration Management** 7.M.D **Information Sharing and ISACs/ ISAOs** 8.M.C	SA-4, SA-9, SR-2, SR-3, SR-5 PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6	Supply chain risk Asset compromise Unplanned outages Unplanned operational downtime
14	**Cybersecurity Testing:** Establish processes to promptly discover and responsibly share vulnerabilities in assets discovered through penetration testing and attack simulations	**RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**Vulnerability Management** **Security Operations Center and Incident Response**	**Penetration Testing** 7.L.A **Attack Simulation** 7.L.C **Information Sharing and ISACs/ ISAOs** 8.M.C	CA-2, CA-7, PM-16, PM-28, RA-2, RA-3	Unplanned operational downtime

Enhanced Goals

ID	Goals	Desired Outcome (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
15	**Cybersecurity Mitigation:** Establish processes internally to act quickly on prioritized vulnerabilities discovered through penetration testing and attack simulations	**RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**Security Operations Center and Incident Response**	**Information Sharing and ISACs/ ISAOs** 8.M.C **Patch Management** 7.M.D **Vulnerability Remediation Planning** 7.L.B	CA-2, CA-7, PM-16, PM-28, RA-2, RA-3	Unplanned operational downtime
16	**Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (TTP):** Ensure organizational awareness of and ability to detect relevant threats and TTPs at endpoints, ensure organizations are able to secure entry and exit points to its network with endpoint protection	**ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **ID.RA-3:** Threats, both internal and external, are identified and documented **DE.CM-1:** The network is monitored to detect potential cybersecurity events	**Endpoint Protection Systems**	**Endpoint Detection Response** 2.L.C	PM-15, PM-16, RA-10, SI-5 PM-12, PM-16, RA-3, RA-10, SI-5 AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	Malware exploitation on endpoint devices Ransomware Lack of situational awareness of threat landscape Unplanned operational downtime
17	**Network Segmentation:** Mission critical assets are separated into discrete network segments to minimize lateral movement by threat actors after initial compromise	**PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation) **PR.PT-4:** Communications and control networks are protected	**Network Management**	**Network Segmentation** 6.M.B	AC-4, AC-10, SC-7, SC-10, SC-20 AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47	Asset compromise Ransomware Lack of situational awareness of threat landscape
18	**Centralized Log Collection:** Collection of necessary telemetry from security log data sources within an organization's network that maximizes visibility, cost effectiveness, and faster response to incidents	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**Security Operations Center and Incident Response**	**Security Operations Center** 8.M.A **Incident Response** 8.M.B	AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16	Lack of situational awareness of threat landscape

Enhanced Goals

ID	Goals	Desired Outcome (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
19	**Centralized Incident Planning and Preparedness:** Ensure organizations consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **PR.IP-10:** Response and recovery plans are tested	**Security Operations Center and Incident Response**	**Security Operations Center** 8.M.A **Incident Response** 8.M.B	CM-3, CM-4, SA-10	Lack of situational awareness of threat landscape Unplanned operational downtime
20	**Configuration Management:** Define secure device and system settings in a consistent manner and maintain them according to established baselines	**PR.IP-1:** A baseline configuration of information technology/ industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	**Vulnerability Management**	**Patch Management, Configuration Management** 7.M.D	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	Asset compromise Unplanned outages

DEPLOYING THE HPH CPGS

Below is a mapping of the HPH CPGs using the *Cyber Defense Matrix*[1] that underscores how the goals can help provide protection across an organization's IT enterprise and the cyber threat landscape. The HPH CPGs directly address common attack methods threat actors use today to attack the healthcare sector. The defense matrix organizes protections across the assets that make up an IT infrastructure in relation to which functions those protections fall within NIST's Cybersecurity Framework.

Taken together, the HPH CPGs offer a sound foundation for cyber preparedness and resiliency for healthcare organizations.

Cyber Defense Matrix Part 1: Examples, Common Vectors, and Potential Impact

	Identify	Protect	Detect	Respond	Recover	Examples	Common Attack Vectors	Potential Impact
Devices						• Laptops • Servers • Containers • Virtual Machines	• Malware run against user system • Compromised credentials used to log into devices	• Attacker can pivot from device to other IT • Devices shut down causing operational disruption
Applications						• Custom applications and open source libraries • Internet exposed web applications • Email tools and EHR	• Software supply chain attack (e.g., Log4J) • Software weakness exploited (e.g., remote code execution)	• Attackers able to disrupt services and steal data • Attackers gain foothold into network
Networks						• Cloud infrastructure (AWS, Azure) • Office WiFi /network	• Misconfiguration abused to gain access • Denial of service	• Network made unavailable for a period of time
Data						• PII or PHI • Claims data	• Stolen data • Ransomware used to encrypt data	• Patient fraud • Data unavailable during healthcare operations
Users						• Employees • Patients logging into a portal	• Social engineering / phishing • Credential theft	• Credentials used to gain unauthorized access to IT resources, enabling higher privileged attacks and wide-scale damage

1 For additional details on defense in depth, please reference the model found here: Cyber Defense Matrix.

Cyber Defense Matrix Part 2: Goals

	Identify	Protect	Detect	Respond	Recover	Essential Goals	Enhanced Goals
Devices						• Mitigate Known Vulnerabilities	• Asset Inventory • Cybersecurity Testing • Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures • Centralized Log Collection
Applications						• Revoke Credentials for Departing Workforce Members, including Employees, Contractors, Affiliates, and Volunteers • Vendor/Supplier Cybersecurity Requirements	• Third Party Vulnerability Disclosure • Cybersecurity Mitigation • Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures • Centralized Log Collection
Networks						• Basic Incident Planning and Preparedness • Unique Credentials	• Third Party Incident Reporting • Network Segmentation • Centralized Log Collection • Centralized Incident Planning and Preparedness • Configuration Management
Data						• Strong Encryption	• Centralized Incident Planning and Preparedness
Users						• Email Security • Multifactor Authentication • Basic Cybersecurity Training • Separate User and Privileged Accounts