Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

Resources and Templates

Table of Contents

Appendix A: Glossary of Terms

Definitions from Division N, Title 1, Section 102 of the Cybersecurity Information Act of 2015[1]

Cybersecurity threat - An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term ``cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber threat indicator - Information that is necessary to describe or identify:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- any combination thereof.

Defensive measure - An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term ``defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by:

- the private entity operating the measure; or
- another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

Federal entity - A department or agency of the United States or any component of such department or agency.

[1] https://www.congress.gov/bill/114th-congress/house-bill/2029/text

Information system - Has the meaning given the term in section 3502 of title 44, United States Code; and includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

Local government - Any borough, city, county, parish, town, township, village, or other political subdivision of a State.

Malicious cyber command and control - A method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

Malicious reconnaissance - A method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

Monitor - To acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

Non-federal entity - Any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof). The term ``non-Federal entity'' includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States. The term ``non-Federal entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Private entity - Any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof. The term ``private entity'' includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services. The term ``private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Security control - The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security vulnerability - Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Tribal - The term ``tribal'' has the meaning given the term ``Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

Other Terms

Asset - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. *Source(s): CNSSI 4009-2015*

Breach - A breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident." OMB M-18-02 and subsequent OMB Guidance: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. *Source: Department of Homeland Security DHS Directives System Instruction Number: 047-01-006 Revision Number: 00 Issue Date: DECEMBER 4, 2017*

Business Continuity Plan – The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. *Source(s): NIST SP 800-34 Rev. 1; CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)*

Capacity Planning - Systematic determination of resource requirements for the projected output, over a specific period. *Source(s): businessdictionary.com*

Category - The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes." *Source(s): NIST Cybersecurity Framework*

Client-Side Attacks - Client-side attacks occur when vulnerabilities within the 190 endpoint are exploited.

Controls (Also see Security Controls) - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. *Source(s): FIPS 200 (FIPS 199); FIPS 199; CNSSI 4009-2015 (FIPS 199); NIST SP 800-128 (FIPS 199); NIST SP 800-137 (FIPS 199); NIST SP 800-18 Rev. 1 (FIPS 199); NIST SP 800-34 Rev. 1 (FIPS 199); NIST SP 800-37 Rev. 1 (FIPS 199); NIST SP 800-39 (FIPS 199, CNSSI 4009); NIST SP 800-60 Vol 1 Rev. 1 (FIPS 199); NIST SP 800-30 (FIPS 199, CNSSI 4009); NIST SP 800-82 Rev. 2 (FIPS 199)*

Critical Infrastructure - Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. *Source(s): Presidential Policy Directive Critical Infrastructure Security and Resilience (*PPD-21)

Cyber Risk - Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system.

Cybersecurity - The process of protecting information by preventing, detecting, and responding to attacks. *Source(s): NIST Framework*

Defense-in-depth - Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. *Source(s): CNSSI 4009-2015 (NIST SP 800-53 Rev. 4); NIST SP 800-39 (CNSSI 4009); NIST SP 800-53 Rev. 4; NIST SP 800-30 (CNSSI 4009)*

Denial of Service Attack (DOS) - Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed. *Source(s): NIST SP 800-24*

Disaster Recovery – A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. *Source: SP 800-34.* Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan. *Source: CNSSI-* **Disaster Recovery Plan (DRP) –** A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. *Source(s): NIST SP 800-34 Rev. 1; CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)*

Endpoint Protection Platform (or End-Point Protection Platform) - Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.). *Source(s): NIST SP 800-128*

Event - Any observable occurrence on a system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). *Source: NIST Framework*

Firmware - Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. *Source(s): Techterms.com*

Framework - A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework." *Source(s): NIST Framework*

Impact – Consequence; to have direct effect on. In cybersecurity, the effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations, its assets, on individuals, other organizations, or on national interests. *Source(s): DHS Risk Lexicon, National Infrastructure Protection Plan, NIST SP 800-53 Rev 4*

Incident - An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. *Source(s): NIST Framework*

Internet of Things (IoT) – In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems. *Source: Strategic Principles for Securing the Internet of Things DHS: November 15, 2016*

Mobile Device - A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device. *Source(s): CNSSI 4009-2015 (Adapted from NIST SP 800-53 Rev. 4)*

Multi-factor Authentication - MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. *Source: Back to basics: Multi-factor authentication (MFA) NIST.gov*

Network Access - Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). *Source(s): NIST SP 800-53 Rev. 4*

Overlay - A fully specified set of security controls, control enhancements, and supplemental guidance derived from tailoring a security baseline to fit the user's specific environment and mission. *Source(s): NIST SP 800-53 Rev. 4*

Patch - A software update comprised code inserted into the code of an executable program. Patches may do things such as fix a software bug or install new drivers.

Port - The entry or exit point from a computer for connecting communications or peripheral devices. *Source(s): NIST SP 800-82*

Profile - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. *Source(s): NIST Framework*

- Target Profile - the desired outcome or 'to be' state of cybersecurity implementation
- Current Profile – the 'as is' state of system cybersecurity

Protocol - A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. *Source(s): NIST SP 800-82*

Remote Access - Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). *Source(s): NIST SP 800-53*

Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. *Source(s): NIST SP 800-82*

Risk Management - The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. *Source(s): FIPS 200*

Risk Tolerance - The level of risk that the organization is willing to accept in pursuit of strategic goals and objectives. *Source(s): NIST SP 800-53*

Router - A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. *Source(s): NIST SP 800-82*

Security Control - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. *Source(s): NIST SP 800-82*

Supporting Services - Providers of external system services to the organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. *Source(s): NIST SP 800-53*

Switch - A network device that filters and forwards packets between LAN segments. *Source(s): NIST SP 800-47*

Third-Party Relationships - Relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties.
Source(s): DHS

Third-party Providers - Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. *Source: NIST Special Publication 800-53 (Rev. 4)*

Threat - A possible danger to a computer system. *Source(s): NIST SP 800-28 Version 2*

Thresholds - A value that sets the limit between normal and abnormal behavior.

Source(s): NIST SP 800-94

Vulnerability - A security weakness in a computer. *Source(s): NIST SP 800-114*

Appendix B: CSA 405(d) Steering Committee Members

Last Name	First Name	Organization
Barrett	Matt	NIST
Bastani	Bob	HHS/ASPR
Bollerer	Chris	HHS/OCIO/OIS
Bradsher	Kris	HHS/ASL
Csulak	Emery	HHS/CMS
Cummings	Stacy	DoD Program Office
Curren	Steve	HHS/ASPR
Dar	Cristina	HHS/FDA
Hall	Bill	HHS/ASPA
Heesters	Nick	HHS/OCR
Jackson	Helen	DHS
Lemott	Sonja	DoD Program Office
Mosely-Day	Serena	HHS/OCR
Niemczak	Stephen	HHS/OIG
Nsahlai	Rose-Marie	HHS/ONC
O’Connor	Kerry	DHS
Ross	Aftin	HHS/FDA
Schwartz	Suzanne	HHS/FDA
Todd	Nickol	HHS/ASPR
Vantrease	Scott	HHS/OIG
Wolf	Laura	HHS/ASPR

Appendix C: Task Group Membership

Last Name	First Name	Title	Organization
Adams	Kenneth	Director, Federal Advisory	KPMG
Alicea	Michael	Chief Information Officer (CIO)	Synergy Healthcare Services, LLC
Alvarez	Bayardo	Director, Information Technology (IT)	Boston PainCare Center
Anastasiou	Peter	Director, Security Strategy	Tufts Health Plan
Anderson	Carl	Vice President (VP)	HITRUST
Barrera	Connie	Director, Information Assurance (IA) and Chief Information Security Officer (CISO)	Jackson Health System
Barrett	Lee	Executive Director	Electronic Healthcare Network (EHNAC)
Barrett	Matthew	Cybersecurity Framework Lead	NIST
Becknel	Damon	CISO	Horizon Blue Cross Blue Shield of New Jersey
Belfi	Catherine	Manager – Emergency Management and Enterprise Resilience	New York University Langone Medical Center
Blanchette	Karen	Executive Director	PAHCOM
Blass	Gerard	President and Chief Executive Officer (CEO)	ComplyAssistant
Bollerer	Chris	Supervisory IT Specialist	HHS/OIS
Bontsas	Jeff	VP and CISO	Ascension Information Services
Bowden	Daniel	CISO	Sentara Healthcare
Branch	Robert	Director, Information Systems and Technology	Munroe Regional Medical Center
Carr	Joseph	CIO	New Jersey Hospital Association
Castillo	Janella	Junior Information Security Analyst	HITRUST
Chaput	Robert	CEO	Clearwater Compliance LLC
Chua	Julie	HHS Security Risk Management Division Manager	HHS/OCIO/OIS
Cline	Bryan	VP, Standards and Analytics	HITRUST
Cofran	Wendy	CIO	Natick VNA/Century Health Systems
Coughlin	Jeff	Senior Director, Federal and State Affairs	HIMSS
Coyne	Andrew	CISO	Mayo Clinic
Csulak	Emery	CISO	HHS/CMS
Cullen	Mike	Senior Manager, Cybersecurity and Privacy	Baker Tilly
Cummings	Allana	CIO	Children’s Healthcare of Atlanta

Curran	Sean	Senior Director	West Monroe Partners
Curren	Stephen	Director, Division of Resilience	HHS/ASPR
Curtiss	Rich	CISO	Clearwater Compliance LLC
Dar	Cristina	Research Officer	HHS/FDA
Davis	Cynthia	CHIO	Methodist Le Bonheur Healthcare
Decker	Erik	Chief Security and Privacy Officer	University of Chicago Medicine
Donat	Terry	Surgeon and Illinois Professional Emergency Manager	CGH Medical Center
Dunkle	Stephen	CISO	Geisinger Health
Durbin	Kenneth	Strategist, Certified Information Systems Security Professional (CISSP)	Symantec
Echols	Mike	CEO	IACI - International Association of ISAOs
Edmonson	Vladimir	Chief Privacy Officer & Senior Compliance Director	Ohio Health
Etherton	Anna	IT Specialist (INFOSEC)	DHS/CS&C
Farabella	Helena	National Chairperson	PAHCOM
Finn	David	Health IT Officer	Symantec
Fleet	Eli	Director of Federal Affairs	HIMSS
Frederick	Michael	VP Operations	HITRUST
Goldman	Julian	Clinician: Attending Anesthesiologist, Massachusetts General Hospital / Harvard Medical School	Harvard Med
Goldstein	Eric	Branch Chief, Partnerships and Engagement	DHS CS&C
Gomez	John	CEO	Sensato
Gorme	Craig	IT Security Manager	UF Health and Shands Hospital
Grillo	Jorge	CIO/VP Facilities, Safety, Security, Construction and EVS	St Lawrence Health System
Heesters	Nicholas	Health Information Privacy Security Specialist	HHS/OCR/HIPAA
Hicks	Andrew	Managing Principal	Coalfire
Hinde	William	Managing Director	West Monroe Partners
Holtzman	David	VP, Compliance Strategies	CynergisTek, Inc.
Jackson	Helen	Program Analyst	DHS/CS&C
James	Bruce	Director of Cybersecurity Architecture	Intermountain Healthcare

Jarrett	Mark	Chief Quality Officer, Association Chief Medical Officer	Northwell Health
Jobes	Kathy	VP and CISO	Ohio Health
Kacer	Wendy	Sr. Director, Cybersecurity Governance, Risk and Compliance	Dignity Health
Kim	Lee	Director of Privacy and Security	HIMSS
Klein	Sharon	Partner	Pepper Hamilton
Krigstein	Leslie	VP, Congressional Affairs	CHIME
Lacey	Darren	CISO	Johns Hopkins
Lee	Wayne	Chief Cybersecurity Architect	West Monroe Partners
Levy	Leonard	VP and CIS	Spectrum Health
Love	Talvis	Senior Vice President (SVP), Enterprise Architecture, eCommerce and CISO	Cardinal Health
Maksymow	Michael	VP and CIO	Beebe Healthcare
Marquette	Casey	Sr. Director, Information Security (INFOSEC)	CVS Health
McAllister	Guy	VP and CIO	Tift Regional Medical Center
McDonald	Blair	IT INFOSEC Analyst	HHS/OS/OCIO
McLendon	John	VP and CIO	Johns Hopkins All Children's Hospital
Nonneman	Lisa	IT Director	Mary Lanning Healthcare
Nordenberg	Dale	Executive Director	MDISS
Palmer	Dennis	Sr. Assurance Associate	HITRUST
Quinn	Jessica	SVP, Chief Compliance Officer	Ohio Health
Quinn	Matthew	Sr. Advisor, Health Technology	HRSA
Riethmiller	Erika	Director, Corporate Privacy Incident Program	Anthem
Ross	Aftin	Senior Science Health Advisor	FDA.HHS/OCIO/OIS
Royster	Curtis	IT Specialist	DC Government/Department of Health Care Finance
Savickis	Mari	VP, Federal Affairs	CHIME & AEHIS
Savoie	Don Savoie	Chief Operating Officer (COO)	Meridian Behavioral Health Center
Schwartz	Suzanne	Associate Director for Science and Strategic Partnerships	FDA.HHS/OCIO/OIS
Shaikh	Munzoor	Director	West Monroe Partners
Siler	Kendra	President	CommunityHealth IT

Skinner	Rich	Head of Strategy and Business Development-Cyber Security	West Monroe Partners
Smith	Philip	President	MedMorph LLC
Stephens	Timothy	Sr. Advisor	Biologics Modular
Stevens	Deborah	VP and CISO	Tufts Health Plan
Stine	Kevin	Chief of the Applied Cybersecurity Division	NIST
Tennant	Rob	Director, HIT Policy	Medical Group Management Association
Teyf	Daniel	Security Architect	Colorado Governor's Office of IT, Office of Information Security, CISO
Thomas	Mitchell	Chief Security Officer	HealthSouth Inc.
Tierney	Logan	Project Manager	Greater New York Hospital Association
Todd	Nickol	Deputy Director, Division of Resilience	HHS/ASPR
Voigt	Leah	Chief Privacy and Research Integrity Officer	Spectrum Health
Wang	May	Chief Technology Officer and Co-founder	ZingBox
Watson	Kelli	Cybersecurity Operative and Researcher	Sensato
Webb	Tim	Partner	InfoArch Consulting, Inc.
West	Karl	CISO	Intermountain Healthcare
Wheatley	Cathleen	System Chief Nurse Executive and VP of Clinical Operations	Wake Forest Baptist Health
Willis	David	Medical Director	Heart of Florida Health Center
Wilson	Chad	Director of Information Security	Children's National Health System
Wilson	Kafi	Principle/CEO	KWMD LLC
Wivoda	Joe	Sr. Director of Healthcare at Analysts	Analysts
Wolf	Laura	Supervisory Program Analyst	HHS/ASPR
Worzala	Chantal	VP, Health Information Policy	American Hospital Association
Wright	Michael	Sr. Manager	Baker Tilly
Zigmund-Luke	Marilyn	Sr. Counsel	America's Health Insurance Plans (AHIP)

Appendix D: Practices and the NIST Cybersecurity Framework

The 405(d) Task Group identified the following ten most effective Practices to mitigate common threats across the large, complex U.S. health care sector:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Each practice is aligned to the NIST Cybersecurity Framework (NIST Framework). The NIST Framework articulates a consistent structure with five cybersecurity functions: identify, protect, detect, respond, and recover. It describes the intended cybersecurity outcome. With the practices **identified** in this document, organizations are encouraged to embark on the **protective**, **detective**, **responsive**, and **recovery** activities in each of the 10 Practice areas.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy

🟦		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

For example, Practice #1: Email Protection Systems, outlines a series of steps to protect the organization from phishing, ransomware, and data leakage. These practices align to the Protect function of the NIST Framework. Specifically, they map back to the PR.AC-1, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-2, PR.DS-5, and PR.PT-4.

Within the two technical volumes, each of the ten practices has a set of sub-practices, which vary depending on the size of the organization. For each practice, Table 2 identifies the number of sub-practices provided for small, medium and large organizations. Large organizations will benefit from sub-practices for both medium and large organizations.

NIST Framework Mapping

Small Organization Sub-Practices Mapped to NIST Framework Sub-Categories

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
E-mail Protection Systems	1.S.A	E-mail System Configuration	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)
E-mail Protection Systems	1.S.A	E-mail System Configuration	PR.DS-2	Data-in-transit is protected
E-mail Protection Systems	1.S.A	E-mail System Configuration	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)
E-mail Protection Systems	1.S.A	E-mail System Configuration	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
E-mail Protection Systems	1.S.A	E-mail System Configuration	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)
E-mail Protection Systems	1.S.A	E-mail System Configuration	PR.DS-2	Data-in-transit is protected
E-mail Protection Systems	1.S.B	Education	PR.AT-1	All users are informed and trained

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
E-mail Protection Systems	1.S.C	Phishing Simulation	PR.AT	The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	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)
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	PR.IP-12	A vulnerability management plan is developed and implemented
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	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)
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	PR.DS-1	Data at rest is protected
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	PR.DS-2	Data-in-transit is protected
Endpoint Protection Systems	2.S.A	Basic Endpoint Protection	PR.AC-3	Remote access is managed
Access Management	3.S.A	Basic Access Management	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Access Management	3.S.A	Basic Access Management	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Access Management	3.S.A	Basic Access Management	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Access Management	3.S.A	Basic Access Management	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Access Management	3.S.A	Basic Access Management	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Access Management	3.S.A	Basic Access Management	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
Access Management	3.S.A	Basic Access Management	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)
Access Management	3.S.A	Basic Access Management	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Access Management	3.S.A	Basic Access Management	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Data Protection and Loss Prevention	4.S.A	Policy	ID.GV-1	Organizational cybersecurity policy is established and communicated

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Data Protection and Loss Prevention	4.S.A	Policy	ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
Data Protection and Loss Prevention	4.S.B	Procedures	ID.GV-1	Organizational cybersecurity policy is established and communicated
Data Protection and Loss Prevention	4.S.B	Procedures	PR.AT-1	All users are informed and trained
Data Protection and Loss Prevention	4.S.B	Procedures	PR.DS-2	Data-in-transit is protected
Data Protection and Loss Prevention	4.S.B	Procedures	PR.DS-5	Protections against data leaks are implemented
Data Protection and Loss Prevention	4.S.B	Procedures	PR.AT-1	All users are informed and trained
Data Protection and Loss Prevention	4.S.B	Procedures	PR.DS-1	Data at rest is protected
Data Protection and Loss Prevention	4.S.B	Procedures	PR.IP-6	Data is destroyed according to policy
Data Protection and Loss Prevention	4.S.B	Procedures	ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
Data Protection and Loss Prevention	4.S.C	Education	PR.AT	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Asset Management	5.S.A	Inventory	ID.AM-1	Physical devices and systems within the organization are inventoried
Asset Management	5.S.B	Procurement	ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
Asset Management	5.S.C	Decommissioning	PR.IP-6	Data is destroyed according to policy
Asset Management	5.S.C	Decommissioning	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition
Network Management	6.S.A	Network Segmentation	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.S.A	Network Segmentation	PR.AC-3	Remote access is managed
Network Management	6.S.A	Network Segmentation	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Network Management	6.S.A	Network Segmentation	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
Network Management	6.S.B	Physical Security and Guest Access	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Network Management	6.S.B	Physical Security and Guest Access	PR.AC-2	Physical access to assets is managed and protected
Network Management	6.S.B	Physical Security and Guest Access	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Network Management	6.S.B	Physical Security and Guest Access	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.S.C	Intrusion Prevention	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	7.S.A	Vulnerability Management	PR.IP-12	Vulnerability management plan is developed and implemented.
Incident Response	8.S.A	Incident Response	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
Incident Response	8.S.B	ISAC/ISAO Participation	ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources
Medical Device Security	9.S.A	Medical Device Security	PR.PT	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Cybersecurity Policies	10.S.A	Policies	IG.GV-1	Organizational cybersecurity policy is established and communicated
Cybersecurity Policies	10.S.A	Policies	ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Cybersecurity Policies	10.S.A	Policies	PR.AT	The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Cybersecurity Policies	10.S.A	Policies	PR.AT-1	All users are informed and trained
Cybersecurity Policies	10.S.A	Policies	RS.CO-1	Personnel know their roles and order of operations when a response is needed

Medium Organization Sub-Practices Mapped to NIST Framework Sub-Categories

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.DS-2	Data-in-transit is protected
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.DS-2	Data-in-transit is protected
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	DE.CM-4	Malicious code is detected
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
E-mail Protection Systems	1.M.A	Basic E-mail Protection Controls	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)
E-mail Protection Systems	1.M.B	Multifactor Authentication for Remote E-mail Access	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)
E-mail Protection Systems	1.M.C	E-mail Encryption	PR.DS-2	Data-in-transit is protected
E-mail Protection Systems	1.M.D	Workforce Education	PR.AT-1	All users are informed and trained
Endpoint Protection Systems	2.M.A	Basic Endpoint Protection Controls	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)
Endpoint Protection Systems	2.M.A	Basic Endpoint Protection Controls	DE.CM-4	Malicious code is detected
Endpoint Protection Systems	2.M.A	Basic Endpoint Protection Controls	PR.DS-1	Data-at-rest is protected
Endpoint Protection Systems	2.M.A	Basic Endpoint Protection Controls	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)
Endpoint Protection Systems	2.M.A	Basic Endpoint Protection Controls	PR.IP-12	Vulnerability management plan is developed and implemented.

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Endpoint Protection Systems	2.M.A	Basic Endpoint Protection Controls	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Access Management	3.M.A	Identity	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Access Management	3.M.B	Provisioning, Transfers and De-Provisioning Procedures	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Access Management	3.M.C	Authentication	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Access Management	3.M.D	Multi-Factor Authentication (MFA) for Remote Access	PR.AC-3	Remote access is managed
Access Management	3.M.D	Multi-Factor Authentication (MFA) for Remote Access	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Data Protection and Loss Prevention	4.M.A	Classification of Data	ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
Data Protection and Loss Prevention	4.M.B	Data Use Procedures	ID.GV-1	Organizational cybersecurity policy is established and communicated

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Data Protection and Loss Prevention	4.M.C	Data Security	PR.DS	Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
Data Protection and Loss Prevention	4.M.C	Data Security	PR.DS-1	Data-at-rest is protected
Data Protection and Loss Prevention	4.M.C	Data Security	PR.DS-2	Data-in-transit is protected
Data Protection and Loss Prevention	4.M.C	Data Security	PR.IP-6	Data is destroyed according to policy
Data Protection and Loss Prevention	4.M.C	Data Security	PR.DS-5	Protections against data leaks are implemented
Data Protection and Loss Prevention	4.M.D	Backup Strategies	PR.IP-4	Backups of information are conducted, maintained, and tested
Data Protection and Loss Prevention	4.M.E	Data Loss Prevention	PR.DS-5	Protections against data leaks are implemented
Asset Management	5.M.A	Inventory of Endpoints and Servers	ID.AM-1	Physical devices and systems within the organization are inventoried
Asset Management	5.M.B	Procurement	ID.AM	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.
Asset Management	5.M.C	Secure Storage for Inactive Devices	PR.AC-2	Physical access to assets is managed and protected
Asset Management	5.M.D	Decommissioning Assets	PR.IP-6	Data is destroyed according to policy

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Asset Management	5.M.D	Decommissioning Assets	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition
Network Management	6.M.A	Network Profiles and Firewalls	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.M.A	Network Profiles and Firewalls	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Network Management	6.M.B	Network Segmentation	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.M.C	Intrusion Prevention Systems	DE.CM-1	The network is monitored to detect potential cybersecurity events
Network Management	6.M.D	Web Proxy Protection	PR.AC-3	Remote access is managed
Network Management	6.M.D	Web Proxy Protection	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.M.E	Physical Security of Network Devices	PR.AC-2	Physical access to assets is managed and protected
Vulnerability Management	7.M.A	Host/Server Based Scanning	DE.CM-8	Vulnerability Scans are performed
Vulnerability Management	7.M.B	Web Application Scanning	DE.CM-8	Vulnerability Scans are performed
Vulnerability Management	7.M.C	System Placement and Data Classification	ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Vulnerability Management	7.M.D	Patch Management, Configuration Management, and Change Management	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	7.M.D	Patch Management, Configuration Management, and Change Management	PR.IP-3	Configuration change control processes are in place
Vulnerability Management	7.M.D	Patch Management, Configuration Management, and Change Management	PR.IP-12	A vulnerability management plan is developed and implemented
Incident Response	8.M.A	Security Operations Center	RS.RP	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Incident Response	8.M.B	Incident Response	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
Incident Response	8.M.B	Incident Response	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
Incident Response	8.M.B	Incident Response	RS.AN-1	Notifications from detection systems are investigated
Incident Response	8.M.B	Incident Response	RS.MI-1	Incidents are contained
Incident Response	8.M.B	Incident Response	RS.MI-2	Incidents are mitigated

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Incident Response	8.M.B	Incident Response	RC	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
Incident Response	8.M.C	Information Sharing/ISACs/ISAOs	ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources
Medical Device Security	9.M.A	Medical Device Management	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Medical Device Security	9.M.B	Endpoint Protections	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Medical Device Security	9.M.B	Endpoint Protections	DE.CM-4	Malicious code is detected
Medical Device Security	9.M.B	Endpoint Protections	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Medical Device Security	9.M.B	Endpoint Protections	PR.DS-1	Data-at-rest is protected
Medical Device Security	9.M.B	Endpoint Protections	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Medical Device Security	9.M.B	Endpoint Protections	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)

Practice	Sub-Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Medical Device Security	9.M.C	Identity and Access Management	PR.AC	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Medical Device Security	9.M.C	Identity and Access Management	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Medical Device Security	9.M.C	Identity and Access Management	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Medical Device Security	9.M.C	Identity and Access Management	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Medical Device Security	9.M.D	Asset Management	ID.AM	Physical access to assets is managed and protected
Medical Device Security	9.M.D	Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried
Medical Device Security	9.M.D	Asset Management	PR.IP-6	Data is destroyed according to policy
Medical Device Security	9.M.E	Network Management	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Cybersecurity Policies	10.M.A	Policies	ID.GV-1	Organizational cybersecurity policy is established and communicated

Large Organization Sub-Practices Mapped to NIST Framework Sub-Categories

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
E-mail Protection Systems	1.L.A	Advanced and Next Generation Tooling	PR.DS-2	Data-in-transit is protected
E-mail Protection Systems	1.L.A	Advanced and Next Generation Tooling	DE.CM-5	Unauthorized mobile code is detected
E-mail Protection Systems	1.L.A	Advanced and Next Generation Tooling	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
E-mail Protection Systems	1.L.B	Digital Signatures	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity
E-mail Protection Systems	1.L.B	Digital Signatures	PR.DS-2	Data-in-transit is protected
	1.L.B	Digital Signatures	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
E-mail Protection Systems	1.L.C	Analytics Driven Education	PR.AT-1	All users are informed and trained
Endpoint Protection Systems	2.L.A	Automate the Provisioning of Endpoints	PR.DS-5	Protections against data leaks are implemented
Endpoint Protection Systems	2.L.B	Mobile Device Management	PR.AC-3	Physical access to assets is managed and protected
Endpoint Protection Systems	2.L.C	Host Based Intrusion Detection/Prevention Systems	PR.DS-5	Protections against data leaks are implemented
Endpoint Protection Systems	2.L.D	Endpoint Detection and Response	PR.DS-5	Protections against data leaks are implemented
Endpoint Protection Systems	2.L.D	Endpoint Detection and Response	RS.AN-1	Notifications from detection systems are investigated

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Endpoint Protection Systems	2.L.E	Application Whitelisting	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity
Endpoint Protection Systems	2.L.E	Application Whitelisting	ID.AM-2	Software platforms and applications within the organization are inventoried
Endpoint Protection Systems	2.L.F	Micro-segmentation/Virtualization Strategies	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Access Management	3.L.A	Federated Identity Management	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Access Management	3.L.B	Authorization	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Access Management	3.L.B	Authorization	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Access Management	3.L.C	Access Governance	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Access Management	3.L.D	Single-Sign On	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Data Protection and Loss Prevention	4.L.A	Advanced Data Loss Prevention	PR.DS-5	Protections against data leaks are implemented

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Data Protection and Loss Prevention	4.L.B	Mapping of Data Flows	ID.AM-3	Organizational communication and data flows are mapped/
Data Protection and Loss Prevention	4.L.B	Mapping of Data Flows	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
Asset Management	5.L.A	Automated Discovery and Maintenance	PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
Asset Management	5.L.A	Automated Discovery and Maintenance	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Asset Management	5.L.A	Automated Discovery and Maintenance	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition
Asset Management	5.L.B	Integration with Network Access Control	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Asset Management	5.L.B	Integration with Network Access Control	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Asset Management	5.L.B	Integration with Network Access Control	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Network Management	6.L.A	Additional Network Segmentation	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Network Management	6.L.A	Additional Network Segmentation	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
Network Management	6.L.A	Additional Network Segmentation	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.L.A	Additional Network Segmentation	PR.PT-4	Communications and control networks are protected
Network Management	6.L.B	Command and Control Monitoring of Perimeter	DE.CM-1	The network is monitored to detect potential cybersecurity events
Network Management	6.L.B	Command and Control Monitoring of Perimeter	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Network Management	6.L.C	Anomalous Network Monitoring and Analytics	DE.CM-1	The network is monitored to detect potential cybersecurity events
Network Management	6.L.C	Anomalous Network Monitoring and Analytics	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Network Management	6.L.D	Network Based Sandboxing / Malware Execution	DE.CM-5	Unauthorized mobile code is detected
Network Management	6.L.D	Network Based Sandboxing / Malware Execution	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Network Management	6.L.E	Network Access Control	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
Network Management	6.L.E	Network Access Control	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Network Management	6.L.E	Network Access Control	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege
Vulnerability Management	7.L.A	Penetration Testing	ID.RA-1	Asset vulnerabilities are identified and documented
Vulnerability Management	7.L.A	Penetration Testing	PR.IP-12	A vulnerability management plan is developed and implemented
Vulnerability Management	7.L.A	Penetration Testing	DE.CM-8	Vulnerability scans are performed
Vulnerability Management	7.L.A	Penetration Testing	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	7.L.B	Remediation Planning	PR.IP-12	A vulnerability management plan is developed and implemented
Incident Response	8.L.A	Advanced Security Operations Centers	N/A	N/A
Incident Response	8.L.B	Advanced Information Sharing	ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources
Incident Response	8.L.C	Incident Response Orchestration	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Incident Response	8.L.D	Baseline Network Traffic	ID.AM-3	Organizational communication and data flows are mapped
Incident Response	8.L.D	Baseline Network Traffic	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
Incident Response	8.L.E	User Behavior Analytics	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Incident Response	8.L.E	User Behavior Analytics	DE.AE-1	/ A baseline of network operations and expected data flows for users and systems is established and managed
Incident Response	8.L.F	Deception Technologies	N/A	N/A
Medical Device Security	9.L.A	Vulnerability Management	ID.RA-1	Asset vulnerabilities are identified and documented
Medical Device Security	9.L.A	Vulnerability Management	PR.IP-12	A vulnerability management plan is developed and implemented
Medical Device Security	9.L.A	Vulnerability Management	ID.RA-1	Asset vulnerabilities are identified and documented
Medical Device Security	9.L.A	Vulnerability Management	ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
Medical Device Security	9.L.A	Vulnerability Management	RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
Medical Device Security	9.L.A	Vulnerability Management	ID.RA-1	Asset vulnerabilities are identified and documented

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Medical Device Security	9.L.A	Vulnerability Management	PR.IP-12	A vulnerability management plan is developed and implemented
Medical Device Security	9.L.A	Vulnerability Management	DE.CM-8	Vulnerability scans are performed
Medical Device Security	9.L.B	Security Operations and Incident Response	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
Medical Device Security	9.L.B	Security Operations and Incident Response	DE.CM-8	Vulnerability scans are performed
Medical Device Security	9.L.B	Security Operations and Incident Response	DE.CM-1	The network is monitored to detect potential cybersecurity events
Medical device Security	9.L.B	Security Operations and Incident Response	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Medical device Security	9.L.C	Procurement and Security Evaluations	ID.SC	The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks
Medical device Security	9.L.D	Contacting the FDA	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)

Practices	Sub – Practice		NIST Sub-Category Unique Identifier	NIST Unique Identifier Description
Cybersecurity Policies	N/A	N/A	N/A	N/A

Appendix E: Practices Assessment, Roadmaps, and Toolkit

Within this document, there are a total of 88 practices. It would be a daunting task to implement all these practices at once. In some cases, an identified practice may not be the best option for your organization. An evaluation methodology is provided below to assist you with selecting and prioritizing the practices of greatest relevance.

Assessment Methodology

As stated during the introduction, this document is focused on the five most prevailing threats currently impacting our sector. These five threats, summarized in Table 1, should be front of mind as you assess which practices to implement first.

Many models exist to help enumerate priority and criticality based on risk. Below is a simple model that may be followed:

- Step 1: Enumerate and Prioritize Threats
- Step 2: Review Practices Tailored to Mitigate Threats
- Step 3: Determine Gaps Compared to Practices
- Step 4: Identify Improvement Opportunity and Implement
- Step 5: Repeat for Next Threats

Step 1: Enumerate and Prioritize Threats

The first step in implementing a threat centric approach to mitigate cyber-attacks is to evaluate and prioritize the threats that are listed below. Organizations may have different perspectives on their threat susceptibility, causing variations in the threats to be mitigated.

Full details of conducting a threat assessment can be found within NIST Special Publication 800-30. For the purposes of this document, one should review the impacts these threats can cause to determine which is of the highest priority. *Source(s): NIST SP 800-30*

Threat #	Threat Description	Impact of Attack
A	Email Phishing Attack	Potential to deliver malware or conduct credential attacks. Both attacks lead to further compromise of the organization.
B	Ransomware Attack	Potential to lock up assets (extort) and hold them for monetary "ransom." May result in the permanent loss of patient records.
C	Loss or Theft of Equipment or Data	Potential for equipment to be lost or stolen and lead to a breach of sensitive information. This may lead to identity theft of patients.
D	Accidental or Intentional Data Loss	Potential for data to be intentionally or unintentionally removed from the organization. May lead to a breach of

		sensitive information.
E	Attacks Against Connected Medical Devices and Patient Safety	Potential for patient safety to be impacted by a potential cyberattack. May could cause adverse safety events to the patient.

Table 1: Top 5 Threats to Healthcare Sector

Step 2: Review Practices Tailored to Mitigate Threats

Once you have selected the first threat to mitigate, the next step is to review the series of practices that exist to mitigate that threat. Table 2 correlates threats mitigated to health care cybersecurity systems and practices.

Practice #	Cybersecurity Systems and Practices	Threats Mitigated
1	Email Protection Systems	A, B, D
2	Endpoint Protection Systems	B, C
3	Access Management	B, C, E
4	Data Protection and Loss Prevention	B, C, D
5	Asset Management	B, C, D, E
6	Network Management	B, C, D, E
7	Vulnerability Management	B, C, E
8	Incident Response	A, B, C, D, E
9	Medical Device Security	E
10	Cybersecurity Policies	A, B, C, D, E

Table 2: Cybersecurity Systems and Practices Mapped to Threats Mitigated

As the practices in this document mitigate multiple threats, it is advisable to consider the practices that provide the best breadth of protection, followed by the practices that provide the most depth to mitigate the threat.

For example, if your first start is protection against Phishing attacks, then a logical path would be to begin with Practice #10: Policies, followed by Practices #1: Email Protection Systems. This approach ensures the policy is established when you update your email protection capabilities.

Step 3: Determine Gaps Compared to Practices

Now that you have selected the practices to mitigate identified threats, the next step is to review the sub-practices associated with these selections, comparing the sub-practice to the current state of your existing safeguards. Identify any gaps between the existing state and the identified practice.

Step 4: Identify Improvement Opportunity and Implement

Assess each identified gap to determine if the reviewed practices will provide sufficient protection for your organization considering the projected cost to implement them. If it is determined to be a cost-effective solution, then identify the practice for implementation.

Leveraging common project management methodologies is ideal to ensure effective implementation of complicated practices.

Step 5: Repeat for Next Threats

After you have successfully iterated through the first prioritized threat, repeat Steps 1 through 4 for the next threats. In doing so, you create a roadmap to implement practices that fit within your organization's resource and cost constraints.

Example Assessment

The five-step process is described in an example for a fictitious small provider practice in Table 3.

Step	Analysis	Outcome
Step 1: Threat Assessment	Reviewed all threats. Threat most likely to occur is Phishing.	Determined that phishing attacks could cause the most damage to the organization. Start here.
Step 2: Review Practices	Reviewed all 10 Practices.	Identified three practices that would help mitigate this threat: Email Phishing Protection, Security Operations Center / Incident Response (SOC/IR), Policies and Procedures
Step 3: Determine Gaps	Reviewed the sub-practices identified within the three practices.	Email phishing protection controls are sufficient. No education or phishing simulation conducted.
Step 4: Identify Improvement Opportunities and Implement	Phishing education comes with no direct costs. Phishing simulations would be too expensive for the small practice.	Deferred the implementation of Phishing simulation. Established a workforce phishing education program and implemented.
Step 5: Repeat	Reviewed additional 4 threats, determined next most critical is ransomware.	Start the process anew.

Table 3. A Small Provider Practice Applies the Five-Step Process to a Phishing Attack Scenario

Cybers Security Practices Assessment Toolkit

See CSA 405(d) website for download

Appendix F: Resources

Below is a list of free resources with supplemental information for the threats and concepts addressed in this document. This list is not intended to be comprehensive or complete.

U.S Department of Health and Human Services (HHS) Resources

- **Security Risk Assessment Tool**
  - **Link:** https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
  - **Description:** Security Risk Assessment Tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program
  - # of pages: N/A
- **Risk Management Handbook (RMH) Chapter 08: Incident Response**
  - **Link:** https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf
  - **Description:** "The intent of this document is to describe standard operating procedures that facilitate the implementation of security controls associated with the Incident Response (IR) family of controls taken from the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations and tailored to the CMS environment in the CMS ARS."
  - # of pages: 116
- **Incident Report Template**
  - **Link:** https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template.html?DLPage=4&DLEntries=10&DLSort=0&DLSortDir=ascending
  - **Description:** Template for reporting a computer security incident
  - # of pages: 7
- **Cybersecurity || FDA General Page**
  - **Link:** https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm
  - **Description:** FDA's Cybersecurity page
  - # of pages: 2-3
- **Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health**
  - **Link:** https://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhreports/ucm604500.htm
  - **Description:** FDA's Medical Device Safety Action Plan
  - # of pages: 18
- **HHS Office for Civil Rights Cybersecurity Page**
  - **Link:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
  - **Description:** This web page includes most of OCR's general cybersecurity resources (cybersecurity incident checklist, ransomware guidance, cybersecurity newsletters, HIPAA Security Rule to NIST CSF Crosswalk, etc.).
  - # of pages: 1+ (multiple links to various pages)
- **HIPAA Security Rule Guidance Material**
  - **Link:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

    - **Description:** This site focuses on the HIPAA Security Rule and includes OCR's HIPAA guidance on administrative, physical, and technical safeguards as well as for risk analysis and risk management (it also includes some security focused NIST documents).
    - # of pages: 1+ (multiple links to various pages)
- **Privacy, Security, & HIPAA**
    - **Link:** https://www.healthit.gov/topic/privacy-security-and-hipaa
    - **Description:** ONC's Privacy, Security, and HIPAA resources page
    - # of pages: 1+ (multiple links to various pages)
- **HHS Cybersecurity Task Force Report**
    - **Link:** https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx
    - **Description:** Report on improving cybersecurity in the health care industry, mandated in the Cybersecurity Act of 2015, Section 405(C)
    - # of pages: 96
- **Critical Infrastructure Protection for the Healthcare and Public Health Sectors**
    - **Link:** https://www.phe.gov/preparedness/planning/cip/Pages/default.aspx
    - **Description:** Text
    - # of pages: 1+ (multiple links to various pages)
- **My entity just experienced a cyber-attack! What do we do now? A Quick-Response Checklist** from the HHS, Office for Civil Rights (OCR)
    - **Link:** https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf
    - **Description:** A checklist of things to do if your organization experiences a cyber-attack.
    - # of pages: 2
- **Cyber-Attack Quick Response**
    - **Link:** https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif
    - **Description:** An infographic on responding to a cyber-attack.
    - # of pages: 1
- **FACT SHEET: Ransomware and HIPAA**
    - **Link:** https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es
    - **Description:** A fact sheet on ransomware and HIPAA.
    - # of pages: 8
- **Cybersecurity Awareness Training**
    - **Link:** https://www.hhs.gov/sites/default/files/fy18-cybersecurityawarenesstraining.pdf
    - **Description:** Cybersecurity awareness training leveraged by HHS employees, contractors, interns, and other.
    - # of pages: 61
- **Security 101 for Covered Entities**
    - **Link:** https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es
    - **Description:** Seven papers on specific topics related to the Security Rule.
    - # of pages: 11
- **Guidance on Risk Analysis Requirements under the HIPAA Security Rule**
    - **Link:** https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
    - **Description:** A document that assists organizations with implementing safeguards to secure ePHI.

    - # of pages: 9
- **Protecting the Healthcare Digital Infrastructure: Cybersecurity Checklist**
    - **Link:** https://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-checklist.pdf
    - **Description:** An introductory checklist that outlines several hardware, software, and cybersecurity educational items organizations should consider and implement to protect their digital infrastructure.
    - # of pages: 2

U.S. Department of Homeland Security (DHS) Resources

- **Department of Homeland Security Component Overview**
    - **Link:** https://www.dhs.gov/sites/default/files/publications/DHS%20Cybersecurity%20Overview_2.pdf
    - **Description:** An overview of the Department of Homeland Security components.
    - # of pages: 2
- **(US-Cert) Cybersecurity Framework**
    - Link: https://www.us-cert.gov/ccubedvp/cybersecurity-framework
    - **Description:** A cybersecurity framework with the core functions: Identify, Protect, Detect, Respond, and Recover.
    - # of pages: 1
- **(ICS-CERT) Standard and References**
    - **Link:** https://ics-cert.us-cert.gov/Standards-and-References#plan
    - **Description:** A list of and link to the Industrial Control Systems Cyber Emergency Response Team standards and references.
    - # of pages: 1+
- **DHS Stop.Think.Connect. Campaign**
    - **Link:** https://www.dhs.gov/stopthinkconnect
    - **Description:** A page explaining and expanding on the STOP.THINK.CONNECT. campaign.
    - # of pages: 1+
- **Report on Ongoing SamSam Ransomware Campaigns, 03/30/2018, Healthcare Cybersecurity and Communications Integration Center (HCCIC), HHSHCCIC@HHS.gov**
    - **Link:** https://content.govdelivery.com/attachments/USDHSCIKR/2018/04/06/file_attachments/986231/HCCIC-2018-002W-SamSam%2BRansomware%2BCampaign.pdf
    - **Description:** A report expanding on recent dealings with the ransomware known as SamSam.
    - # of pages: 11

- **Cyber Resilience Review**
    - **Link:** https://www.us-cert.gov/ccubedvp/assessments
    - **Description:** The Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization’s operational resilience and cybersecurity practices.

    Through the CRR, your organization will develop an understanding of its ability to manage cyber risk during normal operations and times of operational stress and crisis.
    - # of pages: 1+ (main page plus multiple downloads)

- Automated Indicator Sharing
    - **Link:** https://www.us-cert.gov/ais
    - **Description:** Automated Indicator Sharing (AIS) enables the exchange of cyber threat indicators between the Federal Government, SLTT governments, and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender's address of a phishing email. AIS is part of a DHS effort to create a cyber ecosystem where as soon as a stakeholder observes an attempted compromise, the cyber threat indicator of compromise (IOC) will be shared in real time with all partners, protecting everyone from that particular threat.
    - # of pages: 1+ (main page plus multiple downloads)
- Cybersecurity Evaluation Tool
    - **Link:** https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
    - **Description:** The Cyber Security Evaluation Tool (CSET) is a no-cost, voluntary desktop stand-alone application that guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices. Using the tool organizations are able to evaluate their cybersecurity posture against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
    - # of pages: 1+ (main page plus multiple downloads)
- The Cybersecurity Workforce Development Toolkit
    - **Link:** https://niccs.us-cert.gov/workforce-development/cybersecurity-resources/cybersecurity-workforce-development-toolkit
    - **Description:** The toolkit helps organizations understand their cybersecurity workforce and staffing needs to protect their information, customers, and networks better. The toolkit includes cybersecurity career path templates and recruitment resources to recruit and retain top cybersecurity talent
    - # of pages: 17
- NICCS Education and Training Catalog
    - **Link:** https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework#
    - **Description:** The catalog is a central location of over 3,000 cybersecurity related courses from over 125 different providers. The catalog can be searched by course location, preferred delivery method (i.e., online or in-person), specialty area, and proficiency level. Courses are designed for participants to add a skillset, increase their level of expertise, earn a certification, or transition to a new career. Strict vetting criteria for course providers ensure that the courses listed in the catalog are offered by organizations that are recognized as providing quality resources. Each course has been mapped to at least one specialty area within the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.
    - # of pages: 1+ (main page plus multiple downloads)

- **External Dependencies Management Assessment**
    - **Link:** For more information, or to schedule an EDM Assessment, contact cyberadvisor@hq.dhs.gov.

    - **Description:** The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization’s management of their dependencies. Through the EDM assessments, organizations can learn how to manage risks arising from external dependencies within the information and communication technology (ICT) supply chain.
    - # of pages: N/A
- **Cyber Infrastructure Survey**
    - **Link:** For more information, or to schedule a CIS, contact cyberadvisor@hq.dhs.gov.
    - **Description:** The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. CIS provides an assessment of the organization’s cybersecurity practices in place for a critical service.
    - # of pages: N/A
- **Phishing Campaign Assessment**
    - **Link:** For more information, or to get started, contact nccicсustomerservice@hq.dhs.gov.
    - **Description:** The Phishing Campaign Assessment (PCA) is a no cost six-week engagement offered to federal, state, local, tribal and territorial (SLTT) governments, as well as critical infrastructure and private sector companies, that evaluates an organization’s susceptibility and reaction to phishing emails of varying complexity. The PCA’s results provide guidance, measure effectiveness, and justify resources needed to defend against spear-phishing and increase user training and awareness.
    - # of pages: N/A
- **Risk and Vulnerability Assessment**
    - **Link:** For more information, or to schedule an RVA, contact ncciccustomerservice@hq.dhs.gov.
    - **Description:** A Risk and Vulnerability Assessment (RVA) is a no-cost offering that combines national threat and vulnerability information with data collected and discovered through onsite assessment activities to provide customers with actionable remediation recommendations prioritized by risk. Engagements are designed to determine whether and by what methods an adversary can defeat network security controls. Components of the assessment can include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration reviews of servers and databases, and evaluation of an organizations detection and response capabilities.
    - # of pages: N/A
- **Vulnerability Scanning**
    - **Link:** For more information, contact ncciccustomerservice@hq.dhs.gov.
    - **Description:** DHS offers vulnerability scanning (formerly known as Cyber Hygiene scanning) of internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation’s overall resiliency.
    - # of pages: N/A

- **Validated Architecture Design Review**
    - **Link:** For more information, contact ncciccustomerservice@hq.dhs.gov.

    - **Description:** The Validated Architecture Design Review (VADR) is a voluntary, no-cost assessment based on standards, guidelines, and best practices. The assessment encompasses architecture and design review, system configuration, and log file review, and sophisticated analysis of network traffic to develop a detailed representation of the communications, flows, and relationships between devices and most importantly to identify anomalous (and potentially suspicious) communication flows. This offering provides a sophisticated analysis of the asset owner's network.
    - # of pages: N/A
- **Enhanced Cybersecurity Services**
    - **Link:** For more information about the program and ECS service provider contact information, please visit www.dhs.gov/ecs.
    - **Description:** The Enhanced Cybersecurity Services (ECS) program facilitates the protection of IT networks by offering intrusion detection and prevention services through approved service providers. All U.S.-based public or private entities, including State, Local, Tribal, and Territorial (SLTT) organizations are eligible to participate.
    - # of pages: N/A
- **Malware Analysis**
    - **Link:** To submit malware for analysis, visit www.malware.us-cert.gov. For further questions or requests, contact ncciccustomerservice@hq.dhs.gov.
    - **Description:** The Advanced Malware Analysis Center provides 24/7 dynamic analysis of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining analysis results. Experts detail recommendations for malware removal and recovery activities. This service can be performed in conjunction with incident response services if required.
    - # of pages: N/A
- **Information Products: National Cyber Awareness System**
    - **Link:** To subscribe to select products, visit **https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new**
    - **Description:** NCCIC offers no-cost, subscription-based information products to stakeholders through the www.us-cert.gov and www.ics-cert.gov websites. NCCIC designed these products—part of the National Cyber Awareness System (NCAS)—to improve situational awareness among technical and non-technical audiences by providing timely information about cybersecurity threats and issues and general security topics. Products include technical alerts, control systems advisories and reports, weekly vulnerability bulletins, and tips on cyber hygiene best practices. Subscribers can select to be notified when products of their choosing are published.
    - # of pages: N/A

National Institute of Standards and Technology (NIST) Resources

- **SP 800-30 Risk Management Guide for Information Technology Systems**
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01
    - **Description:** (see abstract)
    - # of pages: 65
- **SP 800-39 Managing Information Security Risk: Organization, Mission, Information System View**
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-39/final
    - **Description:** (see abstract)

    - # of pages: 88
- SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
    - **Description:** (see abstract)
    - # of pages: 53
- SP 800-28 Version 2. Guidelines on Active Content and Mobile Code
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-28/version-2/final
    - **Description:** (see abstract)
    - # of pages: 62
- SP 800-114 User's Guide to Securing External Devices for Telework and Remote Access
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-114/archive/2007-11-01
    - **Description:** (see abstract)
    - # of pages: 47
- SP 800-177, Trustworthy Email
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-177/final
    - **Description:** (see abstract)
    - # of pages: 97
- SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-181/final
    - **Description:** (see abstract)
    - # of pages: 144
- SP 800-184 – Guide to Cybersecurity Event Recovery
    - **Link:** (https://csrc.nist.gov/publications/detail/sp/800-184/final
    - **Description:** (see abstract)
    - # of pages: 53
- SP 800-63-3, Digital Identity Guidelines
    - **Link:** https://csrc.nist.gov/publications/detail/sp/800-63/3/final
    - **Description:** (see abstract)
    - # of pages: 74

Appendix G: Templates

DISCLAIMER: This document, and this section specifically are in no way recommending or suggesting the purchase of vendor materials or endorsing particular vendor materials, but instead offers samples that were donated or otherwise made available to this initiative by the following organizations

About Templates and How to Use Them

This section provides practical document templates that can be used by providers to aid in strengthening the privacy, security and cybersecurity protocols of their practice. This section is not meant to provide all policies and procedures required to be in place for covered entities and business associates subject to various federal and state privacy and security requirements. However, a sampling of templates are provided for cybersecurity protection and related topics. Future editions of this document may include additional templates and checklists.

The following templates ARE:

- Available to be used at no charge
- Designed to be carefully reviewed and revised by the provider (by merging technical system and office staff policy and workflow into the documents) so that they reflect business practice
- Representing different levels of content and style which may be more suited for small, medium, large organizations

ARE NOT:

- Representative of a complete set of privacy and/or security Policies and Procedures
- Including required state/federal laws and regulations. Each provider/practice is responsible to understand how sensitive information such as Protected Health Information (PHI) and/or Personally Identifiable Information (PII) is handled and to gain and maintain compliance with required laws/regulations separate from this section

4.1 How to Use These Templates-Policy Template Instructions

Using templates

Highlight the desired section/template. Copy the file to your hard drive. You may copy the Template file for your own use and cut sections from it to paste into your own documents, or start with these if current documentation is not in place.

Carefully review the language and assure it is applicable to your practice and business operation. Modify it as necessary to assure language is easy for your workforce members to understand.

4.2 How Policy Templates are Organized

This section includes various templates with a wide variety of style. However, in general, Policy and Procedures often have key sections. Below is a description of methods of organization. Choose the format that works best for your organization.

Sections – Think about the overall grouping of topics for your documentation. For example, you may choose to group together those policies that address workforce behavior. These may include topics like Acceptable Use and Workstation protocols. Another category often grouped together would be those policies governing HIPAA Security that are the responsibility of the Security Officer (versus those types of policies applying to all workforce members (like Email Usage). It may be helpful to group together the technical systems specific policies, and/or those dealing with Incident Response and Reporting and Breach Notification. This is an attempt to organize the material in a logical sequence, to make it easier for a user to find a particular template, and to facilitate ease in the next step of the compliance life cycle – which is training. Users may want to adopt a similar organizational format for their policy manuals. Keeping policies and procedures current becomes an ongoing process so choosing one format makes the revision and educational processes easier to manage.

Policy Template Structure – Templates are often divided into several parts, as follows:

Responsibility: Generic titles for personnel responsible for implementing the policy should be listed. If your chosen template has this section, users should change the titles to match their organization's terminology, organizational structure and division of duties. It is not practical to list individual names, but tying together the titles of those responsible for certain functions assures that all reading the document understand the individual(s) accountable for assuring the policy is in place.

Background: Some templates do not contain a background section. However, those that do, offer this as this section describes what the policy is trying to accomplish. Users should consider including background descriptions in their final policies, as a guide to understanding the issues and concepts behind the policy.

Policy: Provides suggested wording for the policy. The templates included herein are written to incorporate the relevant regulatory requirements in the policy section. Due to the detailed nature of some of the regulations, this sometimes results in very detailed policy statements. However, keeping a distinction between requirements (policy) and options to accomplish the requirements (procedure) is a good way to assure the documents are representative of your practice, but maintain their alignment with the required regulation or law for which they are written. Users are strongly cautioned to understand the overall regulations for which a policy is needed prior to making substantive changes to the policy sections of template documents.

Procedure: The policy can be thought of as the "What." The procedure is the "How." Users should augment and/or modify the procedure sections of these templates as necessary to fit their organization/department's way of doing things.

Notes. Notes are included in some templates. When notes are available, they are to provide further guidance and explanation in applying the policy.

Definitions. Understanding definitions is an essential part of a complete set of policies and procedures. Users should be sure to include a Definitions section in their final privacy, security/cyber security documentation.

Revision History. Once compliance is gained, being able to keep the document in alignment with your organization's practices and to prove ongoing revision, having a Revision History is key. A routine annual review for possible revisions is suggested as a Best Practice. Frequency may be more often as necessary due to systems and operational changes. A good example of a history block is apparent in the examples that follow from SANS.

4.3 Information about These Templates

In order to provide a sampling of policy and procedure templates that may be more appropriate for smaller versus larger organizations, template samples have been donated by some companies that provide HIPAA Privacy and Security Toolkits. This document, and this section specifically are in no way recommending or suggesting the purchase of vendor materials, but instead offering samples that are available from the following organizations:

- Federal Communications Commission Cyber Security Planning Guide - https://transition.fcc.gov/cyber/cyberplanner.pdf. While this Planning Guide does not offer specific "templates", it does include a depth of information which may pertain directly to small provider offices to the degree they serve as a small business environment. Be sure to review the section on Preventing Phishing, and potentially leverage the Definitions and Security Links (for Training and other Cyber Security Reporting information).
- Health IT Gov - https://www.healthit.gov/node/289 - Security Policy Templates were gathered as the Regional Extension Centers assisted Primary Care Providers to gain HIPAA/HITECH compliance. A series of templates and forms are available at no charge. A helpful on-line "Top 10 Tips on Cyber-Security" specific to providers can be found at https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf.
- The Office of the National Coordinator has recently published a draft document on "Trusted Exchange Framework and Common Agreement" with goals and principles to be voluntarily adopted as our industry continues to increase shared information. To aid the providers for which this document is provided, a "Do's and Don't's Template for Trusted (data) Exchange" has been provided which mirrors these principles. It can be used as a handy desk reference to aid in healthcare/information technology business decision making processes. More information can be found at https://www.healthit.gov/newsroom/21st-century-cures-act-trusted-exchange-framework-and-common-agreement-webinar-series
SANS – Specific to Security, this suite of templates from The SANS Institute is available at no charge and can be downloaded at https://www.sans.org/security-resources/policies.

Small Provider Example – Portable Devices

To customize this template document, replace all of the text that is presented in brackets (i.e. "[" and "]") with text that is appropriate to your organization and circumstances. Many of the procedure statements below represent "best practices" for securing mobile computing. These may not be feasible or available for your practice. Be sure this document reflects the actual practices and safeguards currently in place!

Laptop, Portable Device, and Remote Use Policy and Procedure

[Organization name]

Purpose: This organization considers safeguarding its electronic information, personally identifiable information, intellectual property and any patient information, e.g. "sensitive information" of paramount importance. [Organization name] has developed a series of privacy and security policies and procedures as well as a series of computer and internet use policies and procedures.

Certain employees and contractors of [organization] use portable and mobile computing devices including [Insert as applicable]:

- Laptop Computers
- Tablet Computers
- iPADs or their equivalent
- Smartphones
- Other mobile devices [specify]

For work related tasks while traveling or at home. This sometimes entails remote access to our networks, to our applications that create, store, maintain or transmit ePHI, or to websites that create, store, maintain or transmit ePHI.

It is the policy of [organization] that all remote use and/or access will be done with established security safeguards.

Procedure:

1. Laptops and [insert type of device(s)-for example, "Smartphone and Tablet"] that are assigned to individuals for remote use will be accounted for on a computer asset inventory.
2. Laptops and [insert type of device(s)-for example, "Smartphone and Tablet"] must be configured with the standard configuration prior to use remotely.
3. The standard laptop and if available [insert type of device(s)-for example, "Smartphone and Tablet"] configuration will require a unique user login ID and password complexity equal to that of the network if feasible. The current policy on password strength and change will be in force.
4. The standard laptop and [insert type of device(s)-for example "Smartphone and Tablet"] configuration will require the laptop to automatically log off after a period of [enter timeout period-portable devices should have a lower timeout than devices secured in your medical practice because they are more susceptible to theft] minutes of inactivity.
5. The standard configuration will require documents to be written to the [organization] server where possible. [Organization] will use appropriate technology tools to synchronize all laptop and [insert type of device(s)-for example, "Smartphone and Tablet"] files with the network server and thus ensure the laptop files are a) resident on the server and b) part of the routine backup. Note: A variety of software

applications ensure that data on mobile devices can be automatically synchronized to your network or cloud server-such as Dropbox, Evernote, Apple iCloud, Microsoft Office 365 or other synchronization tools and so forth.

6. The standard configuration will require network drive folder level passwords where feasible, when the files relate to confidential or proprietary information.
7. Laptops and [insert type of device(s)-for example, "Smartphone and Tablet"], will be encrypted at either the entire drive or solid-state memory level, or with a partition encryption where the partition contains ePHI.
8. Encryption keys will be separate from the device and maintained with appropriate complexity by the Security Official or their designee. NOTE: Organizations are required by HIPAA to appoint a Privacy and Security Officer. However depending upon the size and complexity of the organization, this official may be the Office Manager, Physician in charge or "responsible security individual".
9. Screenshots with ePHI shall not be saved to laptops or [insert type of device(s)-for example, "Smartphone and Tablet"] unless encryption is enabled.
10. The standard configuration will require malicious software protection to be enabled on the laptop and [insert type of device(s)-for example, "Smartphone and Tablet"], along with automatic live updates. Note: Smartphones, tablets and other mobile devices are also susceptible to viruses or spyware!
11. If laptops [insert type of device(s)-for example, "Smartphone and Tablet"] are used, the security official will enable automatic updating of security patches.
12. When laptop or mobile device security patches or updates are not automatically downloadable but otherwise can be downloaded from a website, the security official will notify, by email, all employees who have a laptop or [insert type of device(s)-for example, "Smartphone and Tablet"], requesting they download and install the update. The security official will request a confirmation receipt of the email and notification of the update. The security official will track responses and if necessary take possession of the device to ensure updates.
13. [Optional] Laptops or [insert type of device(s)-for example, "Smartphone and Tablet"] will be configured with remote security controls that will remotely wipe the device upon loss or theft, scan for malware, provide Global Position System (GPS) tracking, encrypt partitions or memory that stores ePHI, alert or block introduction of unauthorized Subscriber Identity Module (SIM) cards.
14. Smartphones and tablets that are used to access, receive or transmit ePHI via email shall only do so with this medical practice's secure domain mail server or [insert type of secure encrypted email system]. Email settings shall be configured to limit the number of recent or emails stored on the device.
15. Smartphones and tablets that are used to access, receive or transmit ePHI shall be configured to limit the number of text messages stored on the device. Only secure text messaging systems shall be used.
16. Laptops or [insert type of device(s)-for example, "Smartphone and Tablet"] that use wireless communications including Bluetooth will be configured to always turn off the "Discoverable Mode" to ensure the device is not viewable by unauthorized persons. Alternatively, where "Discoverable Mode" is necessary for proper pairing, the user shall be trained to disable this mode when in public places where data and conversations can be discovered by nearby unauthorized individuals.
17. Laptop and [insert type of device(s)-for example, "Smartphone and Tablet"] users will be trained and periodically reminded to pair their devices with the pairing laptop in private locations, and not public locations. Users will be trained to understand that there may be eavesdroppers who may be hacking, sniffing, or setting up malicious code.

18. Laptop and [insert type of device(s)-for example, “Smartphone and Tablet”] users are not allowed to change any setting or security rule on their laptops or [insert type of device(s)-for example, “Smartphone and Tablet”] without permission from the Security Official.
19. Laptop and [insert type of device(s)-for example, “Smartphone and Tablet”] users must adhere to the general [organization] computer and internet use policy including not downloading software, introducing foreign media, and so forth.
20. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”], when in transit, must be carried in the user’s immediate vicinity with appropriate covers or containers. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”] should not be left unattended.
21. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”] when in use at the employee/contractor’s home should be used in a secure location and only by the employee/contractor and not by family/friends or other unauthorized individuals. Users may not use their devices or remotely access ePHI in the immediate presence of any unauthorized person, family or friend who might view the information.
22. Flash drives and other media copying of ePHI will only be used if password protection is enabled and the drive or media is encrypted and provided by the Security Official.
23. All remote access to the [organization] networks or cloud-based applications with ePHI shall be done with the use of a secure access [insert the type of access; for example if you have set up a VPN].

I have read this policy and procedure and will adhere to its requirements:

_______________________________________ ____________

____

Name of Employee/Contractor Date Employer Date

Mid-Large Provider Example – Incident Reporting and Checklist; Workforce Training At-a-Glance One Page Reference Sheet

SECURITY INCIDENT PROCEDURES: RESPONSE AND REPORTING

RESPONSIBILITY: Security Official, Director of Information Systems, and Privacy Official

BACKGROUND:
Development of an internal mechanism to identify and address privacy/security incidents is required by regulations. Formal report and response procedures are an integral component of a security program. A security incident can be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Including privacy incidents or "wrongful disclosures" means the incidents can not only come from an information system, but also from paper documents or any other place across the organization where PHI is created, handled, maintained or stored.

[Note: This policy can be easily expanded to address Red Flag issues (see https://www.consumer.ftc.gov for information). Many examples under the Procedure section can also be considered triggers.]

POLICY:

1. [ENTITY] maintains a comprehensive internal security control program, which is coordinated by the Information Systems department. [ENTITY] also maintains a base compliance program which functions to keep PHI protected and addresses issues of breach of security and privacy policies and procedures by monitoring and mitigating such issues. The internal privacy/security incident reporting process is the mechanism of both the security control and compliance programs, which allows for the organization to identify, investigate, respond, and resolve known and suspected privacy and security incidents. The actual reporting of incidents occurs in two ways:
   - 1.1. Through the use of a Privacy/ Security Incident Reporting Form (Note: This is used for all of the [ENTITY] workforce members and may also be utilized by outside organizations/individuals such as contractors or business associates.)
   - 1.2. As a result of monitoring pre-configured automated system security reports, and use of internal audits and monitoring reviews to identify issues.
2. Regardless of mode of receipt, a chain of command process is used to first address and resolve the issue, report to the impacted individual or other parties (e.g. regulators) where applicable and communicate any necessary curriculum changes resulting from the incident(s) to all workforce members as a core component of training.

PROCEDURE:

1. All workforce members are trained to use the Privacy/Security Incident Reporting Form to report any suspicious privacy/security activities. Specific occurrences which will trigger the completion of the form may include but not be limited to the following:
   - 1.1. Any suspicious or known breach of privacy/security by any workforce member for any reason known to be a violation or contradiction of [ENTITY]'s philosophy of protecting and safeguarding PHI.
   - 1.2. Any suspicious or known breach of privacy/security by an external third party for any reason known to be a violation or contradiction of [ENTITY]'s philosophy of protecting and safeguarding PHI.
   - 1.3. Any suspicious activity uncovered as a result of a review of routine or random audit trail.
   - 1.4. Request for audit log review of user activity (special authorization required)

1.5. Suspected or proven violation of protection of malicious software (introduction of malicious software)
1.6. Violation of Login Attempt (Using or attempting to guess another users log in and/or password)
1.7. Sharing of passwords
1.8. Inappropriate access to the internet
1.9. Improper network activity
1.10. Improper Email Activity / Phishing
1.11. Inappropriate access by customer, client, member, contractor or business associate
1.12. Suspicious documents (inconsistent identification information, photo or physical description, suspected altered or forged signatures)
1.13. Suspicious Medical Information (Member unaware of or denies information previously collected in the medical record, or other trigger that member information is inconsistent with that previously found)
1.14. Suspicious requests (mail returned even though attempts at verifying address have occurred), patterns of usage inconsistent with previous history, frequent ID card requests or replacement requests with change of address
1.15. Personal Information Suspicious (known fraud associated with personal information, inability for person to authenticate via challenge/secret questions, personal information inconsistent with other information on file or that provided via external source, duplicate identifiers (SSN, Medicaid, Medicare cards))

Note: Consider reviewing the “Identity Theft Resource Center” compiled list of breaches as a way to identify patterns, trends and any information to better communicate examples of occurrences that should trigger workforce members to identify and complete an incident report.

2. Forms must be accurately and thoroughly completed within (XXX) hours of the incident (or sooner if the suspected or known breach causes serious risk to the organization) and forwarded immediately to the attention of the workforce member’s direct supervisor and the Privacy and Security Officers. In the event an organization or individual outside [ENTITY] provides the report, the same time frame and reporting procedure applies to the [ENTITY] workforce member in receipt of the report. [Note: This template assumes the form itself is only in hard copy form. An organization may consider the supply and use of the form in electronic mode. Additionally a procedure should be in place for workforce members to forward the incident report directly to the Privacy and Security Officers in cases when the suspect is the issuer’s direct supervisor. Telephone, anonymous hotlines and to other automated processes may exist and should be merged into this procedural section as they relate to the practice. It is also important to train members of the workforce to keep incident information confidential in order to prevent the suspect from learning of the report. This action may serve to prevent the suspect from trying to cover their tracks.] Form may be copied in duplicate in order to facilitate this process and should include at least the following information:
2.1. Date,
2.2. Name,
2.3. Title of submitter,
2.4. Reason for report,
2.5. Indication of whether or not the activity is suspected or known,
2.6. Indication of what application (s) or system(s) have been violated
2.7. Identification of the user in question if appropriate, form may include a listing of the more common reasons for completing the report (listed above) and checkbox style.

2.8. A section of the form should include date received and notes for investigation, mitigation and further actions.

3. Upon receipt of completed Security Incident Report, or automated system security report, the Privacy and Security Officers will review (and conduct superficial investigation if necessary) in order to confirm the validity and level of risk associated with the reported incident in order to place the report in priority with other reports for committee review.

4. The Security Officer, Privacy Official, Director of Information Systems, and any other affected department Director/Manager will convene within a reasonable period of time (depending upon the level of risk of the incident) and as frequently as necessary to determine the following:
   4.1. Investigate and validate the facts included in the incident report, this should include assessment of possible damage to the organization.
   4.2. Determine if the incident needs to be reported to law enforcement, other authorities or the CERT Coordination Center.
   4.3. Determine if unsecured protected health information was acquired or disclosed in a breach situation. If so, determine method to report to Secretary of DHHS (log book or direct report) see DUTY TO REPORT SECURITY OR PRIVACY BREACH, NOTIFY AND MITIGATE THE EFFECT.
   4.4. Determine application of sanctions as necessary in accordance with the Sanctions Policy.
   4.5. Lessen or mitigate any harmful effects to the extent necessary and applicable.
   4.6. Determine if issue should be evaluated as part of a larger review (such as part of ongoing risk analysis), and whether or not systems configuration and/or changes to other related [ENTITY] policies and procedures are necessary.
   4.7. Address communication and training to all affected workforce members if policies and procedures are to be implemented or modified in accordance with MAINTENANCE OF POLICIES AND PROCEDURES document.

5. All necessary actions, including outcomes, will be handled promptly and documented in accordance with [ENTITY] policy.

6. On a routine basis (quarterly or monthly) the Privacy/Security Officers should provide to the organization's senior management level representatives, aggregate reporting of all received privacy/security incident reports, and the organization's response, including level of sanctions applied, mitigation attempts, and/or resulting changes to policies and procedures. (NOTE: One may also include members of the organization's board of directors if applicable).

REFERENCE: 45 CFR §§ 164.308(a)(6)(i), (ii) NOTE: Names of other policies appearing in all CAPS should be appropriately cross-referenced to other practice policies.

Access Control Procedure for [SYSTEM NAME]

OVERVIEW

The purpose of this procedure is to ensure that the proper processes and safeguards are in place for the use of *[SYSTEM NAME]* by the *[DEPARTMENT(S) NAME]* at the *[ORGANIZATION NAME]*. This procedure outlines the requirements for the creation, deletion and review of user accounts and access for *[SYSTEM NAME],* and complies with the Enterprise Access Control, Responsibilities and Oversight, Personally Owned Device, and Electronic Media Protection Policies.

SCOPE

This procedure applies to all user accounts created within *[SYSTEM NAME]* for *[ORGANIZATION NAME] [AND EXTERNAL]* users in *[DEPARTMENT(S)]*. [*It also applies to mobile devices used to access (SYSTEM NAME)]*.

PROCEDURES

A. Roles

Information Owner	[JOB ROLE]
Information System Owner	[JOB ROLE]
IT Custodian(s)	[JOB ROLE]

B. Account Creation

1. The following roles and privileges are identified for *[SYSTEM NAME]*:

(Example:)

JOB ROLE	SYSTEM PRIVILEGES	SYSTEM ROLE
IT Custodian	Read/Write Create/Delete User Accounts	System Administrator
JOB ROLE 2 (e.g., analyst, nurse, etc.)	Read/Write	General User
External UCM/BSD User	Read Only	External User

2. All requests for internal and external user accounts must be directed to *[JOB ROLE]* by the employee's immediate manager or *[EXTERNAL CONTACT PERSON]* and submitted *[in writing, via email, through a SARF, etc.].* All requests for access to *[SYSTEM NAME]* must include the following information:

a. User's name, job title, and system job role/privileges requested
b. Detailed business justification for the type of access sought

3. *[JOB ROLE]* is responsible for communicating with *[VENDOR NAME/CONTACT PERSON]* within *[TIMEFRAME]* when a user's account should be created.

5. *[JOB ROLE]* is responsible for ensuring that accounts are created with the appropriate system privileges as outlined in Section B.

6. All user accounts created will be documented in the *[SYSTEM USER ACCESS DOCUMENT]* by *[JOB ROLE]*, including the user's name, date user account was created, job role, name of user's manager who approved system access, system privileges and system role assigned to the account.

7. Passwords for *[SYSTEM NAME]* should not be the same as users' UCM login passwords, should comply with the Access Control Policy, and consist of the following minimum requirements:

a. A minimum of 8 characters.
b. Include mixed case letters and numbers or special characters.
c. Password must be changed at least every 120 days (whether *[SYSTEM NAME]* technically enforces it or not.)
d. Passwords must not be the same as the username.
e. Passwords may not be reused until 3 additional passwords have been used.

8. If users are sent a default password when an account is created, users must be informed to change their *[SYSTEM NAME]* account password immediately, and comply with the above requirements.

C. Account Deletion

1. A user's immediate manager will notify *[JOB ROLE]* within *[TIMEFRAME] [via email, form, SARF, etc.]* when the user leaves, is terminated or is transferred to ensure access to *[SYSTEM NAME]* is deleted or disabled or privileges are changed within a timely manner.

2. *[JOB ROLE]* is responsible for communicating with *[VENDOR NAME/CONTACT PERSON]* within *[TIMEFRAME]* when a user's account should be disabled or deleted, or privileges should be changed. [JOB ROLE] will communicate changes to user accounts with *[VENDOR NAME/CONTACT PERSON] [via email/calling vendor help desk, etc.]* (OR *[JOB ROLE]* is responsible for disabling, deleting or changing privileges for user accounts within the system administrator console within *[TIMEFRAME]*of being notified of the change.)

3. *[JOB ROLE]* will follow up with *[VENDOR NAME/CONTACT PERSON]* within *[TIMEFRAME]* to ensure that the user account was deleted/disabled/changed by the vendor appropriately and within the timeframe specified.

4. All user accounts deleted, disabled, or changed will be documented in the *[SYSTEM USER ACCESS DOCUMENT].*

D. Account Review

1. *[JOB ROLE]* is responsible for monitoring account creation, deletion and privileges/roles for *[SYSTEM NAME]*.

2. Accounts should be reviewed every *[TIMEFRAME]* by *[JOB ROLE(S)]*.

a. *[JOB ROLE]* will contact *[VENDOR/CONTACT PERSON]* to receive an accounts report from *[VENDOR NAME]* for confirmation of active user accounts and privileges (or login to the Administrator console for [SYSTEM NAME] to verify active user accounts and roles).
b. Vendor reports should be compared with the *[SYSTEM USER ACCESS DOCUMENT]* in order to verify user account access and privileges.

4. Discrepancies in user account access and privileges will be addressed immediately by *[JOB ROLE]* in order to mitigate inappropriate access to the system.

E. Mobile Devices

1. The use of *[SYSTEM NAME]* on mobile devices is allowed if the following conditions are met:

a. *[JOB ROLE]* coordinates with the Help Desk to ensure that users' mobile devices are enrolled in the *[ORGANIZATION NAME]* Mobile Device Management System.
b. Mobile devices must have an antivirus application installed and running.
c. Mobile devices must be encrypted.
d. Mobile devices must be password/fingerprint/pin protected.
e. Mobile devices will have remote wipe capabilities.

2. *[JOB ROLE]* ensures that the Personally Owned Device Policy and Electronic Media Protection Policy are followed.

Date	**Revision**	**Author**
99/99/99	Created Access Control Procedures	*[AUTHOR NAME]*

Sample Privacy and Security Incident Report

NAME
<<Address>>
<<Phone>>

The Privacy/Security Incident Report form is an internal mechanism used to report suspicious privacy/security activities. Forms must be accurately and thoroughly completed within one (1) hour of the incident (or sooner if the suspected or known breach causes serious risk to the organization) and forwarded immediately to their direct supervisor. Supervisors will forward the report to the PSO who will conduct a Risk Assessment and determine whether to enter reported activities into Breach Notification and Tracking Log.

Date Incident Report completed: ______________________________

Name and Title of person reporting incident: ______________________________

A. Incident

Describe the incident (description of incident/reason for report, identification of user in question if applicable)*:

Date and time or estimate of incident*:		
Was incident suspected or known (check one)*:	Suspected	Actual/Known
List application(s)/system(s) violated:		
Location (workstation location):		
What form was the PHI? (check all that apply)	Digital	Verbally Spoken
	Hard Copy	Electronic
What happened to the PHI? (check all that apply)	Taken	Transferred
	Corrupted	Accessed

==

B. *Office Use*

Date report received*:		
Violation type (check one):	Administrative	Physical

	Technical	
Was incident considered unsecured ePHI?	Yes	No
Has incident been verified?	Yes	No
When?	By Whom?	
Who has been identified as the individual responsible for committing the incident?*		
Complete Risk Assessment Worksheet. What is the level of probability (high, medium or low) that the PHI was compromised?		
If necessary, has Notification been completed?	Yes. Date:	No
Describe the corrective action plan to mitigate:		
Are sanctions applied?	Yes	No
30 Day Tracking: Has 30 day follow up and tracking been completed?	Yes	No
Is the corrective action plan in place?	Yes	No
Are modifications needed?	Yes	No

* Required information

1. What is the nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification?

   Include specific details about the type of information:

   - Clinical, Financial and/or Demographic
   - Paper and/or Electronic
   - Spoken

   Be sure to list elements considered inherently **higher risk** such as:

   - Social security numbers
   - Financial/credit card information
   - Diagnosis of Mental Illness/Drug and Alcohol addiction
   - HIV diagnosis
   - Family planning
   - Genetic testing

   Include consideration of any types of data with enough variation to allow for someone to commit identity theft.

1.A. Was the information breached "unsecured PHI?" (Document your answer and rationale.)

1.B. Was the impermissible acquisition, access, use, or disclosure that of a "Limited Data Set" (LDS)? If so, did the LDS contain birth dates or ZIP codes? NOTE: An LDS not containing birth dates or ZIP codes has been deemed by the Secretary as an automatic "**<u>low probability</u>**."

2. Who was the unauthorized person who used the PHI or to whom the disclosure was made?

3. Was the PHI actually acquired or viewed? (Document answer and rationale.)

4. Does the incident fall under one of the exceptions of the breach definition? (Document your answer and rationale.)

5. Describe the extent to which the risk to the PHI has been mitigated.

6. Describe any other reasonable factors related to the incident.

7. What is your final conclusion based on the response of the above factors? Is the final probability that the PHI was compromised deemed **low**, **medium** or **high**?

Privacy and Security Policies
Workforce At-A-Glance Guidelines

Question	Guideline(s)	Policy References
Who is the [ABC Provider] privacy and security contact person?	Contact the [ABC Provider] Privacy/Security Official (PSO): [Name] [Address] [Phone/Email]	
Guidelines Regarding Workforce Member Set Up and Termination		
What do I need to do upon initial employment?	• Attend all [ABC Provider] privacy and security training and learn about your organization's Privacy and Security controls and guidelines for handling Protected Health Information. • Review and sign all forms and agreements provided by [ABC Provider] including but not limited to: o Acceptable Use Agreement o Remote Worker Set Up Checklist (if applicable) • Agree to keep information confidential and follow all [ABC Provider] policies regarding the protection of data and any specific client policies • Take steps to implement data backup procedures	
What do I need to do if I terminate (or change) my relationship (employment or independent contract) with [ABC Provider]?	• Back up all confidential/proprietary information and/or ePHI residing on employee or contractor computer. Saved items must be encrypted according to [ABC Provider] policies and procedures. • Relinquish keys, hardware etc. as directed by [ABC Provider] PSO. • Access to confidential/proprietary information and/or ePHI residing on [ABC Provider] network will be terminated or modified by the [ABC Provider] PSO. • Dispose of all extraneous PHI and sensitive patient information by permanently deleting (destroying) it in accordance with [ABC Provider] policies and procedures and as instructed by PSO or his/her designee.	
Guidelines on Safeguarding Sensitive Information and Protected Health Information		
How should I safeguard sensitive or protected health information residing on?	• Review and abide by [ABC Provider] policies and procedures and related resources including but not limited to: o General safeguards policy & procedures o Acceptable Use Agreement o Home Office Worker Checklist o NIST/CMS Secure Remote Access Info (safeguards)	

Question	Guideline(s)	Policy References
• Computer • Mobile device • Hardcopy • Removable media • Databases	• Never leave PHI unattended. Lock or log out of workstation before leaving it unattended. Lock away, turnover or otherwise make hard copies containing PHI inaccessible to local foot traffic. • Position computer screens so that only authorized persons can read the display • Shred paper documents when no longer needed. PHI must be rendered unusable, unreadable or indecipherable to unauthorized individuals before it can be considered disposed of properly. • Information (data) stored on removable media should be encrypted and/or password protected. Removable media should be carried separate from laptop or mobile device (when possible, keep jump-drives and other removable media separate from the laptop or other mobile device). All passwords, login instructions and authentication tools should be kept separate from the laptop or mobile device. • Do protect computer screen from others • Do use password enabled screen savers and logons • Do mask PHI when making copies or copy/pasting information into another document • Do follow home office set-up guidelines • Do encrypt (or password protect) PHI on mobile devices (PDS's, USB's, DVD's and other storage media • Do follow the organization's data retention protocols • Do advise PSO of any personal databases containing PHI • Do watch for unauthorized uses and disclosures, and advise PSO • Back up device data according to [ABC Provider] policies. Includes only retaining the amount necessary for your files to keep data-at-rest in a secure/encrypted manner. • Do *not* discuss PHI in open areas or with people who do not have a need to know • Do *not* transmit PHI by e-mail unless the sender is using a secure e-mail system. • Do *not* download PHI to a Personal Digital Assistant (PDA) without permission of the Privacy/Security Official. • Do *not* maintain a separate database containing PHI without specific permission of the Privacy/Security Official	
How should I safeguard sensitive or protected health information when sending faxes?	• Use [ABC Provider] FAX Cover Sheet • Confirm the accuracy of fax numbers by calling intended recipients to check the fax number, notify them the fax is on the way, and request verification of receipt of the fax once received. • When expecting a fax that contains PHI, schedule with the sender	

Question	Guideline(s)	Policy References
	when possible so that the fax can be collected upon arrival. - If it is discovered that PHI has been sent to the wrong fax number, the sender must immediately send a second fax to the number that was contacted in error reiterating the confidentiality message above and asking the recipient to telephone the sender immediately to arrange proper disposition of the information. - Any instance of transmitting PHI to the wrong destination number must be reported to the Privacy/Security Officer immediately	
Frequently Asked Questions		
What should I do if I'm asked to handle PHI (e.g., handling individual rights requests) outside of my usual job/project functions?	- Review non-standard activities involving the handling of PHI with [ABC Provider] PSO or his/her designee. - Refer to [ABC Provider] policies on general uses & disclosures, authorization documents, and processing individual (patient/member) rights.	
What should I do if I observe unauthorized acquisition, access, use or disclosure of PHI or other breach?	Report any suspicious privacy/security activities immediately to [ABC Provider] PSO by completing and submitting the [ABC Provider] Privacy/Security Incident Report form.	
What should I do if I receive a complaint about [ABC Provider]'s privacy policies, procedures or actions?	Inform the [ABC Provider] PSO of any privacy or security complaints immediately upon receipt of such complaint. [ABC Provider] PSO will ask that complainant complete and submit a Complaint Form.	
What should I do if I need access to information residing on [ABC Provider] network?	- Contact [ABC Provider] PSO	
What should I do if I experience data	- Avoid data loss by backing up your data according to [ABC Provider] procedures and performing ongoing computer maintenance tasks	

Question	Guideline(s)	Policy References
loss?	• Contact [ABC Provider] PSO to report your data loss and to receive instruction on data recovery from backup processes	
What should I do if I have any Privacy or Security related questions?	• Contact [ABC Provider] PSO or his/her designee. (See contact information above.)	

Do’s and Don’ts for Secure Exchange from TEFCA- One Page Chart

The following key do’s and don’ts have been extracted and simplified to create this handy one page checklist specifically for the Small Provider Practice. The Office for the National Coordinator has provided a document on the Trusted Exchange Framework Common Agreement that includes concepts and principles summarized below-https://www.healthit.gov/buzz-blog/interoperability/trusted-exchange-framework-common-agreement-common-sense-approach-achieving-health-information-interoperability/

Do’s and Don’ts

DO:

- Know the data you handle. If it is subject to HIPAA, know how it is created, received, maintained and transmitted throughout your organization. Know if it is encrypted in use, in transmit and at rest.
- Follow industry standard methods for privacy and security compliance (HIPAA/HITECH policies and procedures); for following electronic standard transactions (ASC X12N or NCPDP EDI) and for creating data for exchange with others (Consolidated Clinical Data Architecture (C-CDA) and Meaningful Use protocols) and to be provided to patients (HIPAA Privacy Individual Rights of Access, Amendment, Accounting for Disclosure, Restriction and others).
- Make sure your HIPAA compliance program is comprehensive and up to date, including ongoing training, policy review and risk assessments. Be sure the workforce members know how to identify, handle and report breach situations to business partners and to the authorities.
- Encourage your vendors to follow industry accepted methods of creating data, functionality and sharing (use of Certified Electronic Health Record Technology – Office of the National Coordinator).
- Implement technology in a manner that makes it easy to use and that allows others to connect to data sources, innovate, and use data to support better, more person-centered care, smarter spending, and healthier people.
- Conduct all exchange openly and transparently. Make terms, conditions, and contractual agreements that govern the exchange of data available.
- Clearly specific the permitted uses and disclosures of data handling.
- Ensure that data is exchanged and used in a manner that promotes patient safety, including consistently and accurately matching Health Information to an individual.
- Update clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization.
- Work collaboratively with standards development organizations (SDOs), health systems, and providers to ensure that standards, such as the C-CDA, are implemented so that data can be received and accurately rendered by the receiving healthcare organization. When required by federal or state law, appropriately capture a patients’ permission to exchange or use their PHI.
- Ensure that Individuals and their authorized caregivers have easy access to their data including having a way to learn how their information is shared and used.

DON’T:

- Don’t Support (or support your vendor’s use of) proprietary technologies and data handling and exchange.
- Don’t impede the ability of patients to access and direct their own data to designated third parties as required by HIPAA.
- Do not seek to gain competitive advantage by limiting access to individuals’ data such as by establishing internal policies and procedures that use privacy laws or regulations as a pretext for not sharing health information.
- Do not implement technology in a manner that permits limiting the sharing of data.
- Do not use methods that discourage or impede appropriate health information exchange, such as throttling the speed with which data is exchanged, limiting the data elements that are exchanged with healthcare organizations that may be a competitor, or requiring burdensome testing requirements in order to connect and share data with another trading partner.
- Do not impose limitations through internal policies and procedures that unduly burden the patient’s right to get a copy or to direct a copy of their health information to a third party of their choosing.