Cybersecurity Resources for HIPAA-Regulated Entities

February 14, 2024
Latest update: March 18, 2024

This is a listing of resources (e.g., guidance, templates, tools) that regulated entities may find useful for achieving compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and improving the security posture of their organizations. This list of resources complements guidance provided to regulated entities in Special Publication (SP) 800-66r2.

For ease of use, the resources are organized by topic. This listing is not meant to be exhaustive or prescriptive, nor is there any indication of priority in the listing of resources within a topic. However, there has been an attempt to organize the resources within each topic so that foundational resources (e.g., getting started guides or tools) appear at the beginning of the topic. Regulated entities can consult these resources when they need additional information or guidance about a particular topic. Regulated entities should note that some links may lead to for-cost resources. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or resources are necessarily the best available for the purpose.

Send comments and recommendations to sp800-66-comments@nist.gov.

Topics

Risk Assessment / Risk Management	Application Security
Documentation Templates	Protection of Organizational Resources and Data
Small Regulated Entities	Incident Handling/Response
Telehealth/Telemedicine Guidance	Equipment and Data Loss
Mobile device security	Contingency Planning
Cloud services	Supply Chain
Ransomware & Phishing	Information Sharing
Education, Training, and Awareness	Access Control/Secure Remote Access
Medical device security	Telework
Internet of Things (IoT) Used in Healthcare	Cybersecurity Workforce

Risk Assessment/Risk Management: The assessment, analysis, and management of risk to electronic Protected Health Information (ePHI) provides the foundation for a regulated entity's Security Rule compliance efforts. While regulated entities are free to use any risk assessment/management methodology that effectively protects the confidentiality, integrity, and availability of ePHI, the resources listed may be helpful.

- **HPH Sector Cyber Security Performance Goals (CPGs)** (Department of Health and Human Services (HHS)) – Consists of a voluntary subset of cybersecurity practices that healthcare organizations can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety.
- **Security Risk Assessment Tool** (Department of Health and Human Services (HHS) & Office of the National Coordinator for Health Information Technology (ONC)) – Designed to help regulated entities conduct a security risk assessment as required by the HIPAA Security Rule[1].
- **Framework for Improving Critical Infrastructure Cybersecurity** (NIST) – Consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps the owners and operators of critical infrastructure manage cybersecurity-related risk.
- **Health Care and Public Health (HPH) Sector Cybersecurity Framework Implementation Guide Version 2** (HHS Administration for Strategic Preparedness & Response (ASPR)) – Intended to help HPH Sector organizations implement the NIST Cybersecurity Framework version 1.1 as an integral part of their cybersecurity and cyber risk management programs.
- **Health Industry Cybersecurity Practices (HICP) Managing Threats and Protecting Patients** (HHS/HPH Sector Coordinating Council (SCC)) – Sets forth a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cybersecurity risks for regulated entities.
- **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations** (HHS/HPH SCC) – Contains technical details for implementing cybersecurity practices. It provides an overview of cybersecurity practices that have been outlined by the industry as highly effective at mitigating risks to the healthcare industry.
- **Protecting the Healthcare Digital Infrastructure: Cybersecurity Checklist** (HPH SCC) – Outlines several hardware, software, and cybersecurity educational items that organizations should consider and implement to protect their digital infrastructure.
- **Health Sector Cybersecurity Coordination Center (HC3) Threat Briefs** (HHS) – Highlights relevant cybersecurity topics and raises the Healthcare and Public Health (HPH) sector's

[1] Regulated entities should be aware that use of the Security Risk Assessment (SRA) Tool or any risk assessment/management tool does not necessarily equate to compliance with the HIPAA Security Rule's risk analysis requirement.

situational awareness of current cyber threats, threat actors, best practices, and mitigation tactics.

- **Cybersecurity Newsletters Archive** (HHS Office for Civil Rights (OCR)) – This website contains a number of archived HHS newsletters about a variety of topics. Their goal is to help HIPAA covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues and highlighting best practices to safeguard Protected Health Information (PHI).
- **Health Sector Cybersecurity Coordination Center (HC3) Sector Alerts** (HHS) – Provides high-level, situational background information and context for technical and executive audiences. Designed to assist the sector with the defense of large-scale and high-level vulnerabilities.
- **HICP Managing Threats and Protecting Patients: Resources and Templates** (HHS) – Maps the 10 most effective practices to mitigate common threats in the healthcare sector to Subcategories of the Cybersecurity Framework. An evaluation methodology is also provided to assist regulated entities with selecting and prioritizing the practices of greatest relevance.
- **HICP Threat Mitigation Matrix** (HHS) – Assists an organization's information technology (IT) team in identifying the five key cybersecurity threats outlined in the HICP that are most pertinent to their unique organization and apply controls to mitigate those threats. The controls and sub-controls are categorized based on their applicability to the organization's size.
- **Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy** (NIST SP 800-37) – Provides a disciplined, structured, and flexible process for managing security and privacy risk.
- **Managing Information Security Risk: Organization, Mission, and Information System View** (NIST SP 800-39) – Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.
- **Top 10 Myths of Security Risk Analysis** (ONC) – Includes an informative list of common misconceptions about HIPAA and a risk assessment to help distinguish fact from fiction.
- **OCR Audit Protocol** (HHS) – Reviews the policies and procedures adopted and employed by covered entities and business associates to meet the selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.
- **MITRE ATT&CK** (MITRE) – Consists of a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies.
- **MITRE D3FEND** (MITRE) – Consists of a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques. The primary goal is to help standardize the vocabulary used to describe defensive cybersecurity technology functionality.

- **Health informatics — Information security management in health using ISO/IEC 27002** (International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC)) – Provides guidance to help regulated entities ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity, and availability of personal health information.
- **Critical Security Controls** (Center for Internet Security (CIS)) – Provides a prescriptive, prioritized, and simplified set of best practices that can be used to strengthen an organization's cybersecurity posture.
- **Integrating Cybersecurity and Enterprise Risk Management (ERM) (**NIST IR 8286**)** – Helps enterprises and their component organizations better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.
- **Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management** (NIST IR 8286A) – Describes documentation of various scenarios based on the potential impact of threats and vulnerabilities on enterprise assets.

Back to top

Documentation Templates: Regulated entities may find value in utilizing templates that facilitate the creation of required documentation.

- **Sample Business Associate Agreement (BAA) Provisions** (HHS) – Includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for a contract between a business associate and subcontractor.
- **HICP Managing Threats and Protecting Patients: Resources and Templates** (HHS) – Provides practical document templates that can be used by regulated entities to aid in strengthening the privacy, security, and cybersecurity protocols of their organizations.

Back to top

Small Regulated Entities: Smaller regulated entities with limited resources may face additional challenges in complying with the Security Rule's requirements. These resources may provide smaller organizations with the guidance needed to improve their cybersecurity posture while complying with the Security Rule.

- **Check Your Cyber Pulse: Basic Practices for Small Entities** (HHS 405(d)) - Provides healthcare organization with a quick reference for maintaining cybersecurity readiness.

- **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations** (HHS/HPH SCC) **–** Provides small healthcare organizations with a series of cybersecurity practices to reduce the impact of the five cybersecurity threats identified in *HICP Managing Threats and Protecting Patients*. Small organizations may benefit from the cybersecurity practices in both volumes.
- **Guide to Privacy and Security of Electronic Health Information** (ONC) – Aims to help small, regulated entities understand how to integrate federal health information privacy and security requirements into their practices.
- **Security Standards: Implementation for the Small Provider** (HHS) – Provides guidance concerning the implementation of the Security Rule standards, implementation specifications, and requirements as they relate to covered entities that are sole practitioners or otherwise considered small providers.
- **NIST Small Business Cybersecurity Corner** (NIST) – Provides cybersecurity resources tailored to protect small businesses and reduce their cybersecurity risks.
- **Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide** (NIST SP 1271) – Details cybersecurity activities for each Function of the Cybersecurity Framework that may be good starting points for small businesses.
- **Cybersecurity for Small Business: Protect Your Small Business** (Federal Trade Commission (FTC)) – Focuses on the basics for protecting a small business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with NIST, the U.S. Small Business Administration, and the Department of Homeland Security.
- **Cybersecurity Awareness Program Small Business Resources** (Cybersecurity and Infrastructure Security Agency (CISA)) – Describes resources and materials to keep your small business cyber secure.
- **Small Business Information Security: The Fundamentals** (NIST IR 7621) – Presents the fundamentals of a small business information security program in non-technical language.
- **Critical Security Controls** (CIS) – Provides a prescriptive, prioritized, and simplified set of best practices that can be used to strengthen an organization's cybersecurity posture.

Back to top

Telehealth/Telemedicine Guidance: Telehealth and telemedicine technologies can provide advantages to delivering patient care. However, new risks to ePHI can also be introduced. Regulated entities need to consider the security practices of the telehealth platforms that they utilize. Consideration must also be given to where telehealth meetings are taking place. Are personnel present who do not have authorization to access PHI? Are any devices (e.g., Internet of Things (IoT) devices) present that are listening and/or recording?

- **Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)** (HPH SCC) – Identifies cyber risks and best practices associated with the use of telehealth and telemedicine and summarizes the policy and regulatory underpinnings for telehealth and telemedicine cyber risk management. Its target audience includes senior executives in healthcare and IT, telehealth service and product companies, and regulators.
- **Tips for Video Conferencing** (CISA) – Details useful tips for conducting secure video conferencing that can apply to telehealth and telemedicine.
- **Guidance for Securing Video Conferencing** (CISA) – Presents cybersecurity principles and practices that individuals and organizations can follow to video conference more securely.

Back to top

Mobile device security: Physicians, healthcare providers, and other healthcare professionals use smartphones, laptops, and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help protect and secure health information when using mobile devices.

- **How Can You Protect and Secure Health Information When Using a Mobile Device?** (ONC) – Provides suggestions for how to secure mobile devices.
- **Managing Mobile Devices in Your Health Care Organization** (ONC) – Details five steps that an organization can take to help manage mobile devices
- **A Guide to Understanding Your Organization's Mobile Device Policies and Procedures Fact Sheet** (ONC) – Helps healthcare providers and professionals understand their organization's mobile device policies and procedures.
- **Using a Mobile Device: How to Protect and Secure Health Information Brochure** (ONC) – Provides healthcare providers and professionals with tips for understanding how to protect and secure patient health information when using a mobile device in a public space, home, office, or healthcare facility.
- **User's Guide to Telework and Bring Your Own Device (BYOD) Security** (NIST SP 800-114**)** – Provides recommendations for securing BYOD devices used for teleworking and remote access, as well as those directly attached to the enterprise's own networks. Section 6 provides guidance in securing mobile devices for telework.
- **Mobile Device Security: Cloud and Hybrid Builds** (NIST) – Proposes a reference design on how to architect enterprise-class protection for mobile devices accessing corporate resources.
- **Mobile Application Security Project** (Open Worldwide Application Security Project (OWASP)) – Provides a security verification standard and testing guide for mobile apps that covers the processes, techniques, and tools used during a mobile app security test.
- **Vetting the Security of Mobile Applications** (NIST SP 800-163) – Outlines and details a mobile application vetting process. This process can be used to ensure that mobile

applications conform to an organization's security requirements and are reasonably free from vulnerabilities.

- **Electronic Health Records on Mobile Devices** (NIST) – Provides a modular, open, end-to-end reference design that can be tailored and implemented by healthcare organizations of varying sizes and information technology (IT) sophistication. The guide shows how healthcare providers can use open-source and commercially available tools and technologies to more securely share patient information with caregivers who are using mobile devices.
- **Guidelines for Managing the Security of Mobile Devices in the Enterprise** (NIST SP 800-124) – Explains the security concerns inherent in mobile device use and provides recommendations for selecting, implementing, and using technologies to centrally manage and secure mobile devices against a variety of threats.

Back to top

Cloud services: Like many technologies, cloud services can assist regulated entities in complying with the Security Rule by providing process and services that regulated entities may not be able to develop or administer on their own. However, cloud services can also introduce risks to ePHI. These resources may help regulated entities understand, select, and manage cloud services.

- **Free Tools for Cloud Environments** (CISA) – Aids businesses transitioning into a cloud environment in identifying the proper tools and techniques needed for data security and protecting critical assets.
- **Guidance on HIPAA and Cloud Computing** (HHS) – Assists regulated entities, including cloud service providers, in understanding their HIPAA obligations.
- **Cloud Security Basics** (National Security Agency (NSA)) – Provides foundational information about cloud services – both their benefits and the risks introduced – so that organizations can make informed decisions before procuring a cloud service provider.
- **Security Guidance for Critical Areas of Focus in Cloud Computing** (CSA) – Provides crowd-sourced cloud security practices to assist in implementing and adopting a cloud-native approach.
- **Cloud Computing Synopsis and Recommendations** (NIST SP 800-146) – Provides the NIST-established definition for cloud computing, describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides recommendations on how organizations should consider the relative opportunities and risks of cloud computing.
- **Guidelines on Security and Privacy in Public Cloud Computing** (NIST SP 800-144) – Provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations that organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

- **General Access Control Guidance for Cloud Systems** (NIST SP 800-210) – Presents cloud access control characteristics and a set of general access control guidance for cloud service models.

Back to top

Ransomware & Phishing: New threats are constantly emerging. The resources below can help regulated entities protect ePHI from ransomware and phishing, two common threats. The recommendations in these resources may also help regulated entities protect ePHI from a variety of other threats.

- **FACT SHEET: Ransomware and HIPAA** (HHS OCR) – Describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role that HIPAA plays in assisting regulated entities to prevent and recover from ransomware attacks.
- **Stop Ransomware** (CISA) – Designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.
- **HICP Ransomware Attack Fact Sheet** (HHS 405(d)) – Provides information and guidance on mitigating ransomware attacks.
- **HICP Ransomware Threat Slides** (HHS 405(d)) – Provides information and guidance on mitigating ransomware attacks.
- **Ransomware Guidance** (NIST) – Illustrates how ransomware attacks can happen and how to stay prepared, get helpful information, and find support.
- **Tips and Tactics: Ransomware** (NIST) – Gives steps to protect an organization from the threat of ransomware and to help recover from a ransomware attack.
- **Tips and Tactics: Preparing Your Organization for Ransomware Attacks** (NIST) – Includes basic practices for protecting against and recovering from ransomware attacks.
- **Prepare, React, and Recover from Ransomware** (HHS 405(d)) – Provides industry-tested best practices (Prepare, React, Recover) to ensure that an organization is prepared for ransomware attacks and can continue to keep patients safe in the event of an attack.
- **Ransomware Prevention and Response for Chief Information Security Officers** (Federal Bureau of Investigation (FBI)) – Assembles existing Federal Government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.
- **HICP Email Phishing Fact Sheet** (HHS 405(d)) – Provides information and guidance on recognizing and mitigating phishing attacks.
- **HICP Email Phishing Threat Slides** (HHS 405(d)) – Provides information and guidance on recognizing and mitigating phishing attacks.
- **Phishing** (HHS OCR) – Provides foundational information about phishing and tips to avoid becoming a victim.

- **Phishing Guidance** (NIST) – Provides information about common types of phishing messages and why any business owner or employee needs to be vigilant against their danger. This resource also helps in learning how to stay prepared, get helpful information, and find support.

Back to top

Education, Training, and Awareness: Cybersecurity risk management and compliance with the Security Rule are ongoing activities that require the support of workforce members. The resources below can help regulated entities develop and maintain programs that invest in the education, training, and awareness of workforce members.

- **Cybersecurity Newsletters Archive** (HHS) – Helps HIPAA-covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues and highlighting best practices to safeguard PHI.
- **Resource Library (**HHS 405(d)) – The HHS 405(d) program creates free resources that can be used by organizations of all sizes. In the Resource Library, click on the links for "Cybersecurity Awareness" or use the search feature to find information and materials to share with your workforce members.
- **Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information Presentation** (ONC) – Assists healthcare organizations in creating a culture of awareness among their healthcare providers, professionals, and staff. The available presentation provide training on how to protect and secure patient health information when using a mobile device.
- **Security Risk Assessment Videos** (ONC) – Includes informative videos about conducting risk assessments and using the SRA Tool.
- **Cybersecurity for Small Business: Protect Your Small Business** (FTC) – Presents the basics for protecting a business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with NIST, the U.S. Small Business Administration, and the Department of Homeland Security.
- **Security Awareness and Training Resources** (HHS) – Includes a comprehensive list of the HHS OCIO information security and role-based training resources that address topics such as phishing, executive and managerial training, and IT administration.
- **InfraGard** – Details a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. InfraGard connects owners and operators in critical infrastructure with the FBI to provide education, share information, network, and hold workshops on emerging technologies and threats.
- **Security Rule Educational Paper Series** (HHS) – Presents a group of educational papers that are designed to give regulated entities insight into the Security Rule and assistance with implementation of the security standards.

- **Security 101 for Covered Entities** – Provides an overview of the Security Rule and its intersection with the HIPAA Privacy Rule.
- **Administrative Safeguards** – Provides information and considerations for regulated entities for the standards and implementation specifications of the Administrative safeguards in the Security Rule.
- **Physical Safeguards** – Provides information and considerations for regulated entities for the standards and implementation specifications of the Physical safeguards in the Security Rule.
- **Technical Safeguards** – Provides information and considerations for regulated entities for the standards and implementation specifications of the Technical safeguards in the Security Rule.
- **Organizational, Policies and Procedures and Documentation Requirements** – Presents the standards for Organizational Requirements and Policies and Procedures and Documentation Requirements, as well as their implementation specifications.

Back to top

Medical device security: Connected medical devices are an important component of modern patient care. However, precautions must be taken to securely integrate these devices into organizational networks and to protect ePHI. The resources below can assist regulated entities in these efforts.

- **FDA Medical Device Cybersecurity** (Food and Drug Administration (FDA)) – Presents updates, risks, reports, and medical device guidance for product manufacturers and health delivery organizations.
- **Medical Device and Health IT Joint Security Plan** (HPH SCC) – Provides a total product life cycle reference guide to developing, deploying, and supporting cyber secure technology solutions in the healthcare environment.
- **HICP Fact Sheet – Attacks Against Connected Medical Devices** (HHS 405(d)) – Provides information and guidance on mitigating medical device attacks.
- **HICP Threat Slides – Attacks Against Connected Medical Devices** (HHS 405(d)) – Provides information and guidance on mitigating medical device attacks.
- **The FDA's Role in Medical Device Cybersecurity** (FDA) – Discusses myths and facts about medical device cybersecurity in a table geared toward manufacturers and providers.
- **Postmarket Management of Cybersecurity in Medical Devices** (FDA) – Helps manufacturers and healthcare providers manage cybersecurity in medical devices, particularly those that are networked.
- **Securing Wireless Infusion Pumps** (NIST) – Demonstrates how healthcare delivery organizations (HDOs) can use standards-based, commercially available cybersecurity

technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

- **Securing Picture Archiving and Communication System (PACS)** (NIST) – Provides an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem.
- **Securing Telehealth Remote Patient Monitoring Ecosystem** (NIST) - Demonstrates how an organization may implement a solution to enhance privacy and secure their remote patient monitoring ecosystem.

Back to top

Internet of Things (IoT) Used in Healthcare: There are many types of IoT devices other than medical devices being used in healthcare environments. These IoT devices can provide useful services to assist in patient care but must also be secured. The resources below can assist regulated entities in securing IoT devices used in healthcare facilities.

- **Foundational Cybersecurity Activities for IoT Device Manufacturers** (NIST IR 8259) – Describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers.
- **IoT Device Cybersecurity Capability Core Baseline** (NIST IR 8259A) – Provides organizations with a starting point to use in identifying the device cybersecurity capabilities for new IoT devices that they will manufacture, integrate, or acquire.
- **IoT Non-Technical Supporting Capability Core Baseline** (NIST IR 8259B) – Provides organizations with a starting point to use in identifying the non-technical supporting capabilities needed in relation to IoT devices that they will manufacture, integrate, or acquire.
- **Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks** (NIST IR 8228) – Aims to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' life cycles.
- **Securing Telehealth Remote Patient Monitoring Ecosystem** (NIST) - Demonstrates how an organization may implement a solution to enhance privacy and secure their remote patient monitoring ecosystem.
- **Profile of the IoT Core Baseline for Consumer IoT Products** (NIST IR 8425) – Documents the consumer profile of NIST's IoT core baseline and identifies cybersecurity capabilities commonly needed for the consumer IoT sector.
- **IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements** (NIST SP 800-213) – Provides guidance that organizations can use to securely integrate IoT devices into their environments, including a process to identify capabilities needed in IoT devices.

- **IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog** (NIST SP 800-213A) – Provides a catalog of technical and non-technical IoT device capabilities that organizations can use in conjunction with SP 800-213.

Back to top

Application Security: Modern devices and services often use applications to store, process, and transmit data. In many cases, these applications can provide useful services. However, they may also introduce risk to ePHI. The following resources may help regulated entities assess and manage risk to ePHI from applications[2].

- **Health App Use Scenarios & HIPAA** (HHS) – Provides scenarios that help app developers determine whether they are business associates and required to comply with HIPAA.
- **App Developers: Start with Security** (FTC) – Provides tips to help developers approach app and software security.
- **Marketing Your Mobile App: Get It Right from the Start** (FTC) – Provides guidelines to help comply with truth-in-advertising standards and basic privacy principles.
- **Vetting the Security of Mobile Applications** (NIST SP 800-163) – Outlines and details a mobile application vetting process. This process can be used to ensure that mobile applications conform to an organization's security requirements and are reasonably free from vulnerabilities.
- **Implementation of DevSecOps for a Microservices-based Application with Service Mesh** (NIST SP 800-204C) – Provides guidance for the implementation of DevSecOps primitives for cloud-native applications.
- **Mobile Application Security Project** (OWASP) – Provides a security verification standard and testing guide for mobile apps that covers the processes, techniques, and tools used during a mobile app security test.

Back to top

Protection of Organizational Resources and Data: Protecting the confidentiality, integrity, and availability of ePHI is paramount to the Security Rule. ePHI is often accessed via organizational resources (e.g., assets, services, workflows, network accounts). Regulated entities may find value in the following materials to protect organizational data and the resources that store and access ePHI.

[2] Note that not all health app developers are business associates and required to comply with HIPAA. Check out the HHS "Health App Use Scenarios & HIPAA" resource to help determine if a health app developer is a HIPAA business associate.

- **Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals** (HHS OCR) – Provides guidance on safeguarding PHI.
- **Zero Trust Architecture** (NIST SP 800-207) – Presents an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust focuses on protecting resources (e.g., ePHI).
- **Zero Trust Maturity Model** (CISA) – Provides guidance to assist organizations in the development of zero trust strategies and implementation plans and to present ways in which various CISA services can support zero trust solutions.
- **Digital Identity Guidelines** (NIST SP 800-63-3) – Provides technical requirements for federal agencies implementing digital identity services and defines technical requirements in the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.
- **Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations** (NIST SP 800-52) – Provides guidance on the selection and configuration of TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms.
- **Trustworthy Email** (NIST SP 800-177) – Gives recommendations and guidelines for enhancing trust in email.
- **Managing the Security of Information Exchanges** (NIST SP 800-47) – Provides guidance on identifying information exchanges, considerations for protecting exchanged information, and the agreements needed to help manage protection of the exchanged information.
- **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations** (NIST SP 800-171) - Provides recommended security requirements for protecting the confidentiality of controlled unclassified information.

Back to top

Incident Handling/Response: At some point, every organization is going to experience a cybersecurity incident. The resources in this section assist regulated entities in planning for incidents and properly handling those that threaten ePHI.

- **Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)** (HPH SCC) – Advises health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency.
- **Healthcare System Cybersecurity Readiness & Response Considerations** (HHS ASPR) – Helps healthcare facilities and the systems they may be a part of understand the roles and responsibilities of stakeholders before, during, and after a cyber incident

- **ASPR TRACIE[3] Technical Resources Page** (HHS ASPR) – Comprised of two libraries with materials (e.g., fact sheets, technical briefs, articles, toolkits, webinars, and plans) helpful to stakeholders in improving healthcare system preparedness and resilience.
- **OCR Cyber Attack Checklist** (HHS OCR) – Explains the steps for a HIPAA-covered entity or its business associate to take in response to a cyber-related security incident.
- **Cyber Attack Quick Response Infographic** (HHS) – Illustrates the steps for a HIPAA-covered entity or business associate to take in response to a cyber-related security incident.
- **Best Practices for Victim Response and Reporting of Cyber Incidents** (Department of Justice (DOJ)) – Provides planning and response guidance based on lessons learned by federal prosecutors while handling cyber investigations and prosecutions. The authors drafted the document with smaller organizations in mind, but larger organizations should also find it useful.
- **Healthcare Organization and Hospital Discussion Guide for Cybersecurity** (Centers for Disease Control and Prevention (CDC)) – Supports and enhances healthcare organizations and hospitals in addressing cybersecurity. Specifically, this document is intended for personnel whose job responsibilities include cybersecurity preparedness and response planning.
- **Guide for Cybersecurity Event Recovery** (NIST SP 800-184) – Provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. It also provides an example scenario that demonstrates guidance and informative metrics that may be helpful for improving the resilience of information systems.
- **Computer Security Incident Handling Guide** (NIST SP 800-61) – Provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.
- **Cyber Storm: Securing Cyber Space** (CISA) – Provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. The exercise series brings together the public and private sectors to simulate the discovery of and response to a significant cyber incident impacting the Nation's critical infrastructure.

Back to top

Equipment and Data Loss: ePHI can be put at risk due to loss of organizational equipment or data. These resources provide regulated entities with the information needed to prevent the loss of equipment or data and to mitigate the effects of loss.

- **HICP Fact Sheet – Loss or Theft of Equipment or Data** (HHS 405(d)) – Provides information and guidance on mitigating the loss or theft of equipment or data.

[3] Technical Resources, Assistance Center, and Information Exchange

- **HICP Threat Slides – Loss or Theft of Equipment or Data** (HHS 405(d)) – Provides information and guidance on mitigating the loss or theft of equipment or data.
- **HICP Fact Sheet – Insider, Accidental, or Intentional Data Loss** (HHS 405(d)) – Provides information and guidance on mitigating data loss.
- **HICP Threat Slides – Insider, Accidental, or Intentional Data Loss** (HHS 405(d)) – Provides information and guidance on mitigating data loss.
- **Guidelines for Media Sanitization** (NIST SP 800-88) – Assists organizations and system owners in making practical sanitization decisions based on the confidentiality categorization of their information.

Back to top

Contingency Planning: Information systems are vital elements in most business processes. For regulated entities, these systems help to store, process, and transmit ePHI. It is critical for the services provided by these systems to operate effectively without excessive interruption. Contingency planning supports this requirement by enabling the recovery of systems following disruptions. Regulated entities may find these resources helpful in creating and maintaining contingency plans.

- **Plan A… B… Contingency Plan!** (HHS OCR) – Provides foundational information about contingency plans and what is required by HIPAA.
- **Contingency Planning Guide for Federal Information Systems** (NIST SP 800-34) – Provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities. While written for the Federal Government, the content in this publication could also assist other regulated entities.
- **ASPR TRACIE Technical Resources Page** (HHS ASPR) – Comprised of two libraries with materials (e.g., fact sheets, technical briefs, articles, toolkits, webinars, and plans) helpful to stakeholders in improving healthcare system preparedness and resilience.
- **Healthcare COOP and Recovery Planning** (HHS ASPR) – Includes a collection of resources, ideas, templates, references, and hyperlinks to additional information relating to Healthcare Continuity of Operations (COOP) and Healthcare Disaster Recovery.
- **Business Impact Analysis (BIA) Template** (NIST) – Assists regulated entities in performing a business impact analysis (BIA) on an information system. The template is meant only as a basic guide and may not apply equally to all systems. Modify this template or the general BIA approach as required to best accommodate a specific system.
- **Contingency Planning: Low Impact System Template** (NIST) – Provides a sample template to address NIST SP 800-53 security controls from the Contingency Planning family for a low-impact information system. The template provided is a guide and may

be customized as necessary to best fit the system or organizational requirements for contingency planning.

- **Contingency Planning: Moderate Impact System Template** (NIST) – Provides a sample template to address NIST SP 800-53 security controls from the Contingency Planning family for a moderate-impact information system. The template provided is a guide and may be customized as necessary to best fit the system or organizational requirements for contingency planning.
- **Contingency Planning: High Impact System Template** (NIST) – Provides a sample template to address NIST SP 800-53 security controls from the Contingency Planning family for a high-impact information system. The template provided is a guide and may be customized as necessary to best fit the system or organizational requirements for contingency planning.

Back to top

Supply Chain: Organizations obtain many products and services from third parties that can help in the protection of ePHI. However, regulated entities need to ensure the security of these products and services.

- **Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2)** (HPH SCC) – Provides a toolkit for small to mid-sized healthcare institutions to better ensure the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program.
- **Key Practices in Cyber Supply Chain Risk Management: Observations from Industry** (NIST IR 8276) – Provides the ever-increasing community of digital businesses a set of key practices that any organization can use to manage the cybersecurity risks associated with their supply chains.
- **Supply Chain Risk Management Practices for Federal Information Systems and Organizations** (NIST SP 800-161) – Provides guidance to federal agencies on identifying, assessing, and mitigating information and communications technology (ICT) supply chain risks at all levels of their organizations. Non-federal organizations may also find the guidance useful.

Back to top

Information Sharing: Regulated entities may find benefits in both the sharing and receiving of information related to cybersecurity and the protection of ePHI. These resources can assist regulated entities in setting up and maintaining organizational information sharing programs.

- **Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)** (HPH SCC) – Explains best practices for how healthcare organizations can set up and manage cyber threat information-sharing programs for their enterprise.
- **Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)** (HPH SCC) – Identifies many of the cybersecurity information-sharing organizations and their key services, as health organizations are beginning to understand the importance of cybersecurity information sharing and implementing information-sharing systems.
- **Guide to Cyber Threat Information Sharing** (NIST SP 800-150) – Helps organizations establish information-sharing goals, identify cyber threat information sources, scope information-sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices.

Back to top

Access Control/Secure Remote Access: To protect ePHI, regulated entities need to ensure proper access control – both internal to the organization and remote access – to ePHI. The resources in this section can help regulated entities secure access to ePHI.

- **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** (NIST SP 800-46) – Provides information on security considerations for several types of remote access solutions and makes recommendations for securing a variety of telework, remote access, and BYOD technologies as well as creating related security policies.
- **User's Guide to Telework and Bring Your Own Device (BYOD) Security** (NIST SP 800-114**)** – Provides recommendations for securing BYOD devices used for teleworking and remote access, as well as those directly attached to the enterprise's own networks.
- **Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions** (NIST) – Summarizes key concepts and recommendations related to telework and remote access solutions.
- **Utilizing Two-Factor Authentication** (HHS) – Describes two-factor authentication, a process in which a user must provide two different types of information to gain access to an account or system.
- **Hardening Remote Access VPN** (HHS) – Provides guidance on hardening virtual private network (VPN) services via an information sheet jointly issued by the National Security Agency (NSA) and CISA.
- **Guide to SSL VPNs** (NIST SP 800-113) – Assists organizations in understanding Secure Sockets Layer (SSL) VPN technologies and makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions.

- **Guide to IPsec VPNs** (NIST SP 800-77) – Provides practical guidance to organizations on implementing security services based on Internet Protocol Security (IPsec) so that they can mitigate the risks associated with transmitting sensitive information across networks.

Back to top

Telework: Many organizational personnel work remotely and/or telework. To protect ePHI, regulated entities need to ensure that workers are securely connecting to organizational resources. The resources in this section may help regulated entities in securing organizational telework.

- **12 Tips for Safe Teleworking from HICP** (HHS 405(d)) – Details 12 tips that can be implemented from an organization and from home to help fight cyber attacks while teleworking.
- **Telework Essentials Toolkit** (CISA) – Assists business leaders, IT staff, and end users in developing a secure telework environment through simple, actionable recommendations. The Toolkit provides three personalized modules for executive leaders, IT professionals, and teleworkers.
- **Management Checklist for Teleworking Surge During COVID-19 Response** (HPH SCC) – Serves as a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and IT security, and supply chain resilience.
- **User's Guide to Telework and Bring Your Own Device (BYOD) Security** (NIST SP 800-114) – Provides recommendations for securing BYOD devices used for teleworking and remote access, as well as those directly attached to the enterprise's own networks.
- **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** (NIST SP 800-46) – Provides information on security considerations for several types of remote access solutions and makes recommendations for securing a variety of telework, remote access, and BYOD technologies as well as creating related security policies.
- **Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions** (NIST) – Summarizes key concepts and recommendations related to telework and remote access solutions.

Back to top

Cybersecurity Workforce: A properly skilled and knowledgeable workforce is essential to meeting organizational missions and protecting ePHI. Regulated entities can reference this resource in developing their workforce.

- **Workforce Framework for Cybersecurity (NICE Framework)** (NIST SP 800-181) – Provides a set of building blocks for describing the tasks, knowledge, and skills that are needed by individuals and teams to perform cybersecurity work. Through these building blocks, the National Initiative for Cybersecurity Education (NICE) Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners explore cybersecurity work and engage in appropriate learning activities to develop their knowledge and skills.

Back to top