Navigating HIPAA, 405(d), and CPGs

Jon Moore | MS, JD, HCISPP

Chief Risk Officer and Head of Consulting Services and Client Success

Clearwater

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda

- Audits and Recognized Security Practices
- NIST CSF 2.0
- 405(d) HICP
- NIST SP 800-66 Rev 2
- HHS Cybersecurity Performance Goals (CPGs)
- Putting It Together

Today's Presenter

Jon Moore, MS, JD, HCISPP

Chief Risk Officer and Head of Consulting Services and Client Success

- 25+ years Executive Leadership, Technology Consulting and Law
- 14+ years Data Privacy & Security
- 10+ years Healthcare
- Former PwC Federal Healthcare Leadership Team
- Former IT Operational Leader PwC Federal Practice
- BA Economics Haverford College, MS E-Commerce Carnegie Mellon University, JD Dickinson Law Penn Stat University
- Architect of Federal IT GRC Solution
- Expertise and Focus: Healthcare, Risk Management, Compliance
- Speaker and Published Author on Security, Privacy, IT Strategy and Impact of Emerging Technologies

https://www.linkedin.com/in/jonamoore

OCR Announces Renewal of HIPAA Audits

The U.S. Department of Health and Human Services (HHS) announced a HIPAA audit survey in the Federal Register on February 12, 2024. Later, the OCR director confirmed that random audits of covered entities and business associates would begin later this year.

"OCR intends to initiate audits of HIPAA-regulated entities later this year. These audits can assist regulated entities in improving their HIPAA compliance and their protection of health information."

Melanie Fontes Rainer
Director for Office for Civil Rights (OCR)

Periodic Audits Required by HITECH Act

Periodic audits have always been a requirement of Section 13411 of the HITECH Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009) (full-text), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.).

Section 13411 Audits.

The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C (Security Standards for the Protection of Electronic Protected Health Information) and E (Privacy of Individual Health Information) of part 164 (Security and Privacy) of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements.

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164?toc=1

Benefits of Adopting Recognized Security Practices

On January 5, 2022, H.R 7898 was signed into law which amended Section 13412 of the HITECH Act to require HHS to take the Recognized Security Practices of HIPAA-regulated entities into account in certain HIPAA Security Rule enforcement and audit activities, when the organization demonstrates the recognized security practices have been in place continuously for the 12 months prior to a security incident.

Circumstance

When making determinations **relating to fines . . ., decreasing the length and extent of an audit . . ., or remedies otherwise agreed to by the Secretary**, the Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place.

Benefits

(1) **mitigate fines** under section 1176 of the Social Security Act (as amended by section 13410);

(2) result in the **early, favorable termination of an audit** under section 13411; and

(3) **mitigate the remedies that would otherwise be agreed to** in any agreement with respect to resolving potential violations of the HIPAA Security rule

Practices

The term 'recognized security practices' means the standards, guidelines, best practices, methodologies, procedures, and processes developed under **section 2(c)(15) of the National Institute of Standards and Technology Act**, the approaches promulgated under **section 405(d) of the Cybersecurity Act of 2015**, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts.[1]

History

The NIST Cybersecurity Framework originated in response to Executive Order 13636, in 2013, which called for the development of a voluntary framework to improve cybersecurity in critical infrastructure sectors. NIST led the development process in collaboration with industry, government, and academia, releasing the first version of the framework in 2014, with subsequent updates and revisions to enhance its effectiveness in addressing evolving cybersecurity challenges. **The most recent version, 2.0, was released February 26, 2024.**

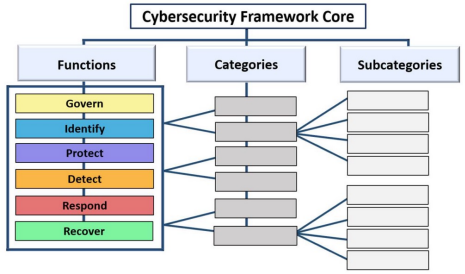
Purpose

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to **manage and reduce their cybersecurity risks**. It is useful regardless of the maturity level and technical sophistication of an organization's cybersecurity programs. Nevertheless, **the CSF does not embrace a one-size-fits all approach. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions**. By necessity, the way organizations implement the CSF will vary.

[1] *The NIST Cybersecurity Framework 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*

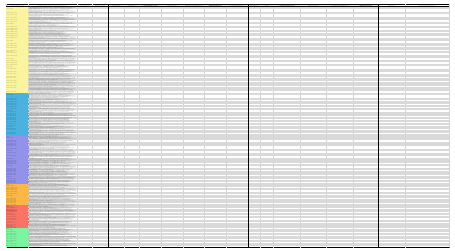
Structure of NIST Cybersecurity Framework 2.0 (CSF)

The NIST Cybersecurity Framework includes three components: Core, Organizational Profiles, and Tiers.



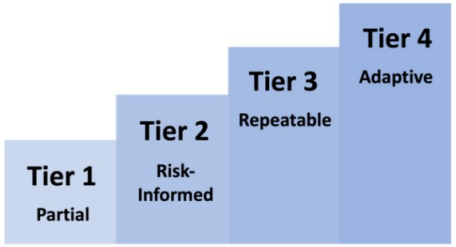
Core

CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.



Organizational Profiles

A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.



Tiers

Applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

Clearwater

Adoption of NIST Cybersecurity Framework

Adopting the CSF includes defining a target organizational profile, understanding your organization's current profile, creating an action plan to move the organization to the target organizational profile and then implementing the plan.

Step	Summary	Description[1]
1	Scope Organization Profile	Document the high-level facts and assumptions on which the Profile will be based. An organization can have as many Organizational Profiles as desired, each with a different scope. For example, a Profile could address an entire organization or be scoped to an organization system or to countering ransomware threats and handling ransomware incidents involving those systems.
2	Gather Information	Examples of information may include organizational policies, risk management priorities and resources, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirements and standards followed by the organization, practices and tools (e.g., procedures and safeguards), and work roles.
3	Create Organizational Profile	Determine what types of information the Profile should include for the selected CSF outcomes and document the needed information. Consider the risk implications of the Current Profile to inform Target Profile planning and prioritization. Also, consider using a Community Profile or other industry guidance to inform the Target Profile.
4	Analyze Gaps and Create Action Plan	Conduct a gap analysis to identify and analyze the differences between the Current and Target Profiles, and develop a prioritized action plan (e.g., risk register, risk detail report, Plan of Action and Milestones [POA&M]) to address those gaps.
5	Implement Action Plan and Update Profile	Follow the action plan to address the gaps and move the organization toward the Target Profile. An action plan may have an overall deadline or be ongoing.

[1] *The NIST Cybersecurity Framework (CSF) 2.0 p. 7*

HSCC JCWG NIST CSF Implementation Guide

To assist healthcare organizations in adopting the NIST CSF, the Health and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Workgroup (JCWG) Risk Analysis Task Group created a Framework Implementation Guide.

History

EO 13636 called on Sector Specific Agencies (SSAs) to "coordinate with the Sector Coordinating Councils (SCCs) to review the Cybersecurity Framework.

The Risk Management (RM) Sub-Working Group (SG) was formally chartered under CIPAC under the Joint HPH Cybersecurity Working Group (WG) in late 2015.

Initially released in February 2016 as Version (Ver.) 1, Ver. 1.1 with additional minor updates and corrections was published in May 2016. The Joint HPH Cybersecurity WG was later re-chartered under CIPAC as the HPH Sector Coordinating Council (HSCC) Joint Cyber WG (JCWG) and the original RM SG was renamed as Task Group 1A (TG-1A) under the JCWG in 2018. Ver. 2 was subsequently published in 2023.

Purpose

The HSCC JCWG developed this document in consultation with the SCC and GCC to help Health Care and Public Health sector organizations understand and leverage the NIST Cybersecurity Framework's Informative References in their implementation of sound cybersecurity and cyber risk management programs, address the five Core Function areas of the NIST Cybersecurity Framework to ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with their overall information security and privacy risk management activities.

Creating a Target Profile

A key step in adopting the CSF is creating a reasonable and appropriate organizational target profile. This is often a struggle for organizations as they are unfamiliar with the references available to support the effort and have not conducted a proper risk analysis.

Organization Information

- Policies
- Risk management priorities
- Resources
- Enterprise risk profiles
- Business impact analysis (BIA)
- Requirements and standards followed by the organization,
- Practices and tools (e.g., procedures and safeguards)
- Security Team

External Guidance

- 405(d) HICP
- NIST Special Publications (ex. 800-66, 800-53)
- Informative References
- Community Profiles (ex. NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST IR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile)

Target Profile

A Target Profile specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends.

405(d) Health Industry Cybersecurity Practices (HICP)

The 405(d) Health Industry Cybersecurity Practices provide voluntary cybersecurity recommendations to enhance the security posture of healthcare organizations, aiming to effectively protect patient data and mitigate the top 5 cyber threats.

History

HHS established the the 405(d) Task Group in 2017. The 405(d) Task Group, part the the HSCC JCWG, includes thought leaders from across the HPH sector. **This group collaborated to provide the sector with practical, understandable, implementable, industry-led, voluntary, and consensus-based cybersecurity guidelines to cost-effectively reduce cybersecurity risks for healthcare organizations.**

The first publication was released in 2018. This was followed up with the 2023 Edition.

Purpose

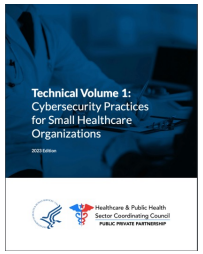
The 405(d) Program is focused on **providing organizations across the nation with useful and impactful HPH focused resources, products, and tools that help educate, raise awareness, and provide vetted cybersecurity best practices** and strengthen the sector's cybersecurity posture against cyber threats.

Structure of 405(d) HICP

The 405(d) Health Industry Cybersecurity Practices are structured into three volumes, covering cybersecurity best practices for small, medium, and large healthcare organizations, including specific practices tailored for the use of networked medical devices.

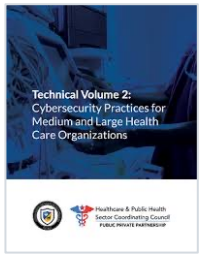
Main Document

Discusses the current cybersecurity threats facing the HPH sector. It sets forth a call to action for the HPH sector, especially executive decision makers, with the goal of raising general awareness.



Technical Volume 1

Outlines the ten cybersecurity practices (herein called practices) and sub practices for small healthcare organizations. While it is intended for use by IT and/or cybersecurity professionals, it also serves to guide organizations on what to ask their IT and/or cybersecurity teams or vendors.



Technical Volume 2

Outlines the ten cybersecurity practices and sub-practices for medium-sized and large healthcare organizations. It is intended for IT and/or cybersecurity professionals.

405(d) HICP Threats and Practices

405(d) HICP is intended to recommend practices specifically to address the top 5 cyber threats facing the Healthcare Industry. Top practice categories are the same for all organization sizes and types while the sub practices differ based on the anticipated level of risk, resources, and nature of business of the organization.

Threats Addressed

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

Cybersecurity Practices

CSP 1. Email Protection Systems
CSP 2. Endpoint Protection Systems
CSP 3. Access Management
CSP 4. Data Protection and Loss Prevention
CSP 5. Asset Management
CSP 6. Network Management
CSP 7. Vulnerability Management
CSP 8. Security Operation Centers and Incident Response
CSP 9. Network Connected Medical Devices
CSP 10. Cybersecurity Oversight and Governance

Sizes and Types of Organizations

To adopt the 405(d) Health Industry Cybersecurity Practices, healthcare organizations can start by identifying the set of practices recommended for their organization given the definitions within the Main Volume.

Best Fit		Small	Medium	Large
Common attributes	**Health information exchange partners**	One or two partners	Several exchange partners	Significant number of partners, or partners with less rigorous standards or requirements
				Global data exchange
	IT capability	No dedicated IT professionals on staff, or IT is outsourced	Dedicated IT resources are on staff, co-managed with outsourcing, or fully outsourced IT	Dedicated IT resources with dedicated budget
			IT is responsible for security	CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Non-existent or limited funding	Funding allocated for specific initiatives (projects)	Dedicated budget with strategic roadmap specific to cybersecurity
			Potentially limited future funding allocations	
			Cybersecurity budgets are blended with IT	
Provider attributes	**Size (provider)**	1-10 physicians	11-50 physicians	Over 50 physicians
	Size (acute / post-acute)	1-25 providers	26-500 providers	Over 500 providers
	Size (hospital)	1-50 beds	51-299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated Delivery Networks (IDNs)
				Participate in Accountable Care Organizations (ACOs) or Clinically Integrated Networks (CINs)
Other org types			Practice management organization	Health plan
			Managed service organization	Large device manufacturer
			Smaller device manufacturers	Large pharmaceutical organization
			Smaller pharmaceutical companies	
			Smaller payor organizations	

Considerations:

Characteristics of your organization and the nature of the products and/or services you provide may decrease or increase the complexity of your cybersecurity needs. You may consider practices outside of your "best fit" size category as you continuously build and improve your cybersecurity strategy.

Also, **if a small organization is tightly linked with other small organizations or a large organization, sharing information between them, it may be appropriate to increase the level and strength of controls** in accordance with the risk.

Clearwater

2023 Hospital Cyber Resiliency Initiative

Recently a study was done by HHS in coordination with the HSCC to measure the adoption of 405(d) HICP within the Hospital Community. This study provides incite into where organizations continue to struggle, and additional focus is needed.

Category	Practices
Components with Significant Progress	• Email Protection Systems
Components with Urgent Need for Improvement	• Endpoint Protection Systems • Identity and Access Management • Network Management • Vulnerability Management • Security Operations Center and Incident Response
Components with need for Additional Research/Follow Up	• IT Asset Management • Cybersecurity Oversight and Governance • Network Connected Medical Devices
Components Where Further Attention is Recommended	• Data Protection and Loss Prevention

NIST SP 800-66 Rev 2 – Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

This NIST special publication provides practical guidance and resources that can be used by regulated entities of all sizes to safeguard ePHI and better understand the security concepts discussed in the HIPAA Security Rule.

Ensure — Ensure that each organization is selecting security practices and controls that adequately safeguard ePHI of which they are the steward.

Inform — Inform the development of compliance strategies that are in concert with the size and structure of the entity.

Provide — Provide guidance on best practices for developing and implementing a risk management program.

Create — Create appropriate documentation that demonstrates effective compliance with the HIPAA Security Rule.

Additional Resource:

In addition to the 800-66 Rev 2 main document, NIST Provides an Online Cybersecurity and Privacy Reference Tool for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide, 2.0.0. This tool provides current crosswalk of the HIPAA requirements to the NIST CSF, NIST Special Publications and other control frameworks.

NIST SP 800-66r2 Content

The publication provides specific guidance on risk assessment and risk management as well as considerations when implementing the HIPAA Security Rule

Risk Analysis	1. **Prepare for Assessment**: Understand where ePHI is created, received, maintained, processed, and transmitted. Identify where ePHI is generated, where and how it enters, where it moves, where it is stored, and leaves the organization. 2. **Identify Reasonably Anticipated Threats**: The regulated entity identifies the potential threat events and threat sources that are applicable to it and its operating environment. 3. **Identify Potential Vulnerabilities and Predisposing Conditions**: The regulated entity develops a list of vulnerabilities that could be exploited by potential threat sources. This list should focus on both technical and non-technical areas. 4. **Determine Likelihood Threat Exploit a Vulnerabi**lity: For each threat event/threat source identified in Step 2, consider: The likelihood that the threat will occur and the likelihood that an occurred threat would exploit a vulnerability and result in an adverse impact 5. **Determine the Impact of a Threat Exploiting a Vulnerability**: Determine the impact that could occur to ePHI if a threat event were to exploit a vulnerability. A regulated entity may choose to express this impact in qualitative terms or other scale they choose. 6. **Determine the Level of Risk**: Assess the level of risk to ePHI while considering the information gathered and determinations made during the previous steps. 7. **Document the Risk Assessment Res**ults: Once the risk assessment has been completed, the results of the risk assessment should be documented.
Risk Management	1. Determine risk to ePHI in accordance with Organization's risk tolerance. 2. Select additional security controls to reduce risk to ePHI. 3. Document Risk Management activities.
Considerations when Implementing	• **Key Activities**: Actions that are often associated with the security functions suggested by each HIPAA Security Rule standard. • **Description**: An expanded explanation about the key activities and the types of activities that a regulated entity may pursue when implementing a standard . • **Sample Questions**: Questions that a regulated entity may ask itself to determine whether the standard has been adequately implemented.

Department of Health and Human Services Cybersecurity Performance Goals (CPGs)

The CPGs are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizations in particular, can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety.

Essential Goals

- Mitigate Known Vulnerabilities
- Email Security
- Multifactor Authentication
- Basic Cybersecurity Training
- Strong Encryption
- Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers
- Basic Incident Planning and Preparedness
- Unique Credentials
- Separate User and Privileged Accounts
- Vendor/Supplier Cybersecurity Requirements

Enhanced Goals

- Asset Inventory
- Third Party Vulnerability Disclosure
- Third Party Incident Reporting
- Cybersecurity Testing
- Cybersecurity Mitigation
- Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures
- Network Segmentation
- Centralized Log Collection
- Centralized Incident Planning and Preparedness
- Configuration Management

Mappings:

CPGs are mapped to HICP practices, sub practices, and NIST 800-53 controls. References to Additional Resources are also provided.