NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management

Version 1.0

National Institute of Standards and Technology
U.S. Department of Commerce

Privacy Framework 1.0 at a Glance

- Open, transparent development process
- Voluntary, flexible, publicly available
- Law/technology/sector neutral
- Version 1.0 released January 2020

Value Proposition

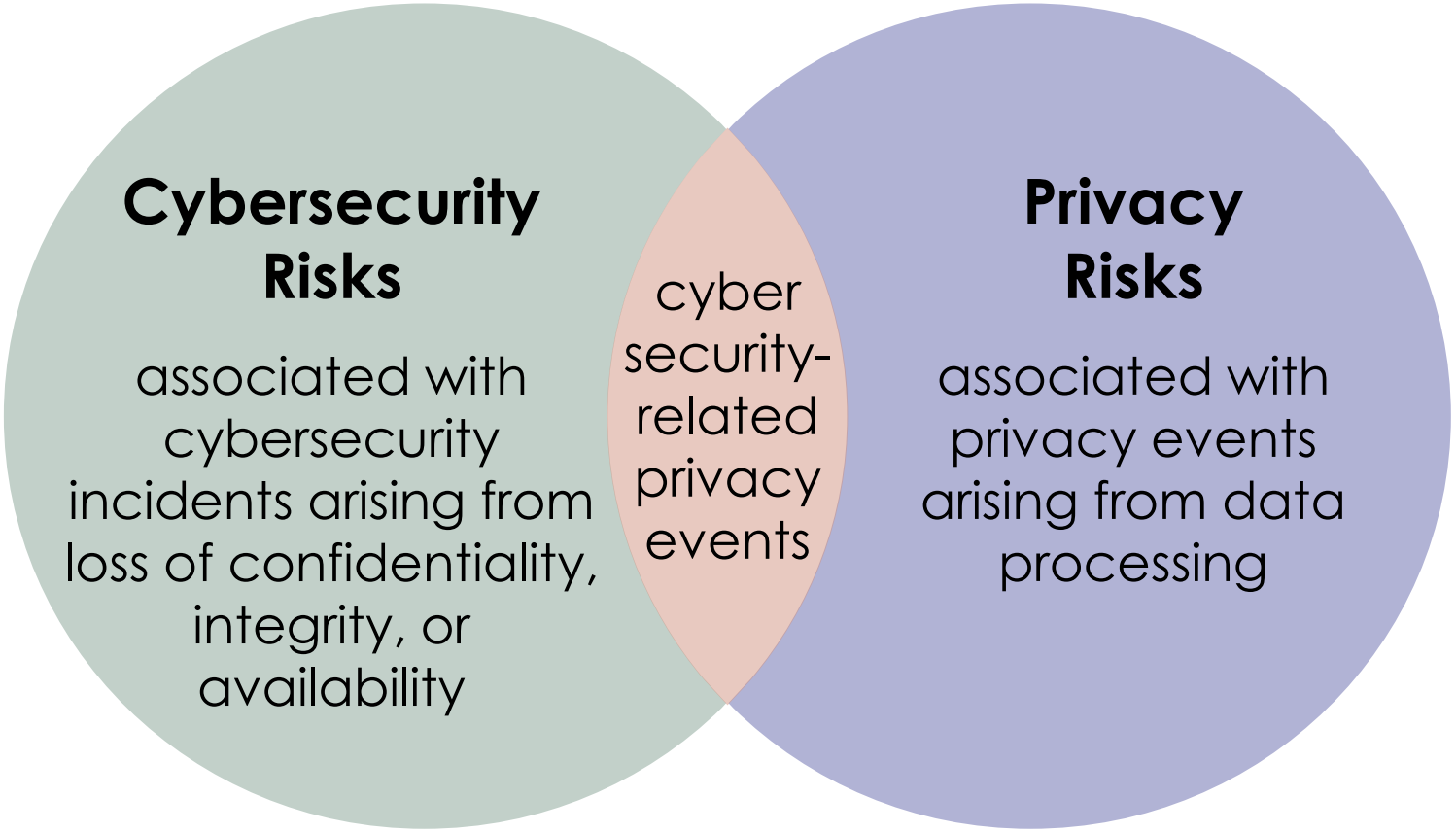
Privacy Framework supports:

Building customer trust

Fulfilling current compliance obligations

Facilitating communication

Relationship Between Cybersecurity and Privacy Risk



Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

NIST Privacy Framework Structure

Privacy Framework Structure

The Core

provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles

are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk

Implementation Tiers

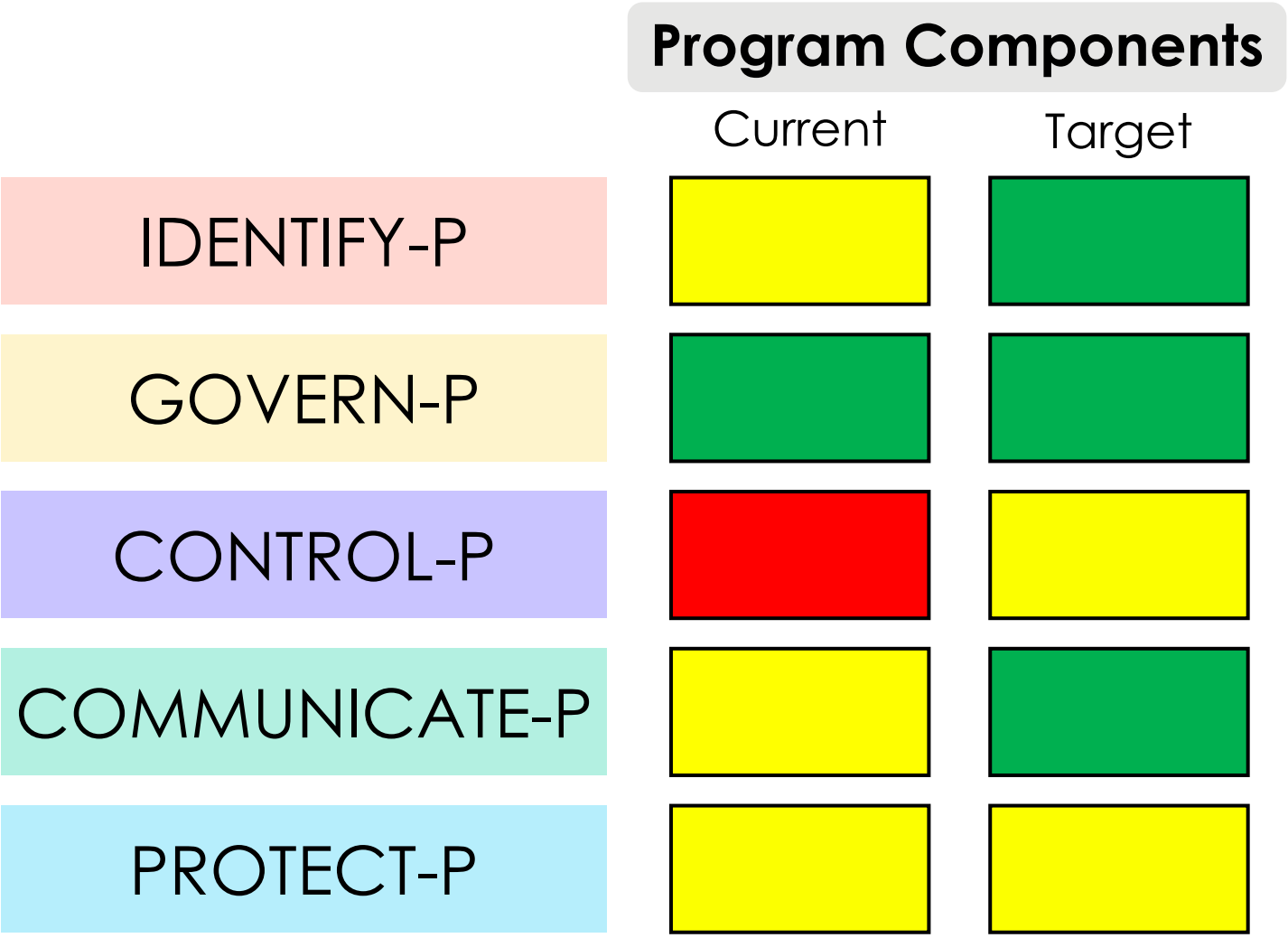
help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

Example Subcategories

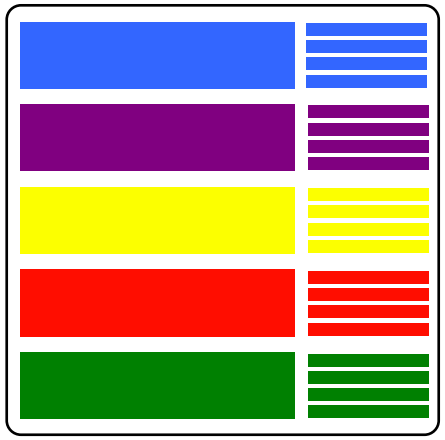
ID-P	ID.IM-P	**ID.IM-P8**	Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
GV-P	GV.PO-P	**GV.PO-P5**	Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
CT-P	CT.DP-P	**CT.DP-P2**	Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
CM-P	CM.AW-P	**CM.AW-P1**	Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
PR-P	PR.AC-P	**PR.AC-P2**	Physical access to data and devices is managed.

NIST Privacy Framework Implementation

Communication and Advocacy with Leadership Example

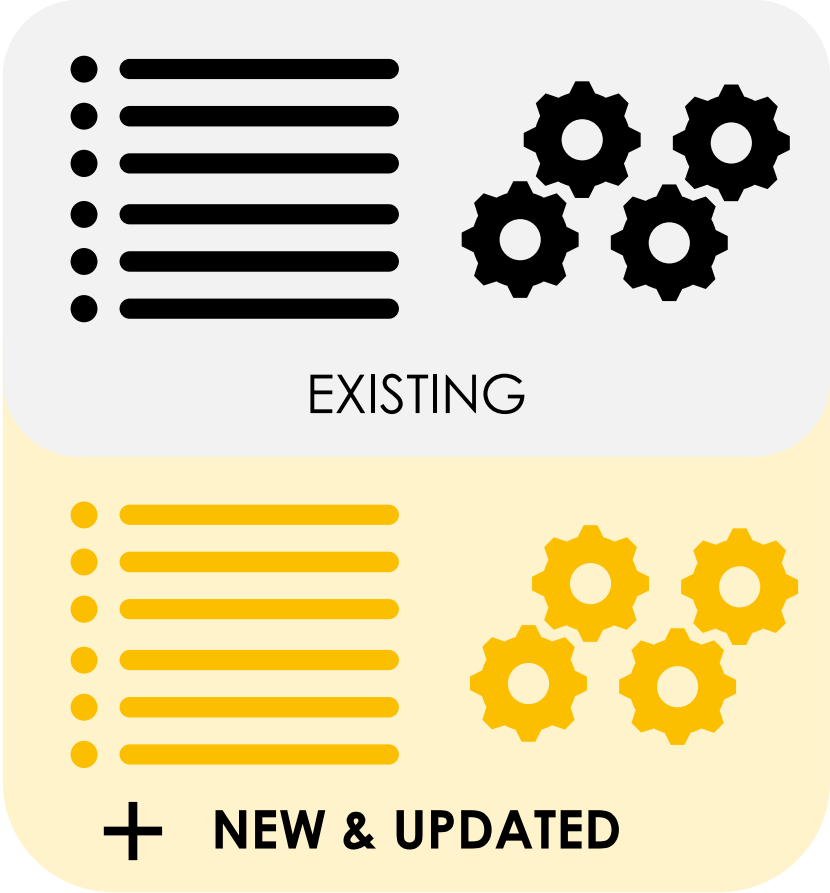


Program Alignment Example

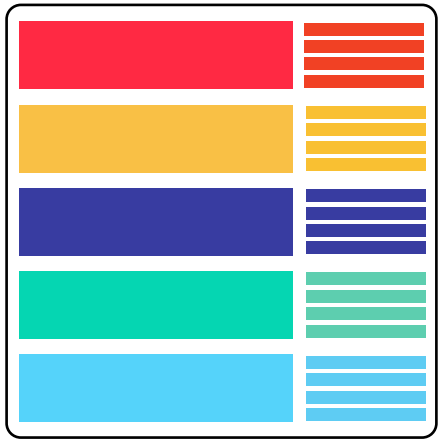


Cybersecurity Framework Profile

Requirements & Controls



Privacy Framework Profile



Resources

Visit Our Learning Center!
https://www.nist.gov/privacy-framework/getting-started-0/learning-center

Small & Medium Business Quick Start Guide

Crosswalks

- GDPR
- LGPD
- DPDPA
- ISO/IEC 27701

and more…

Videos

Translations

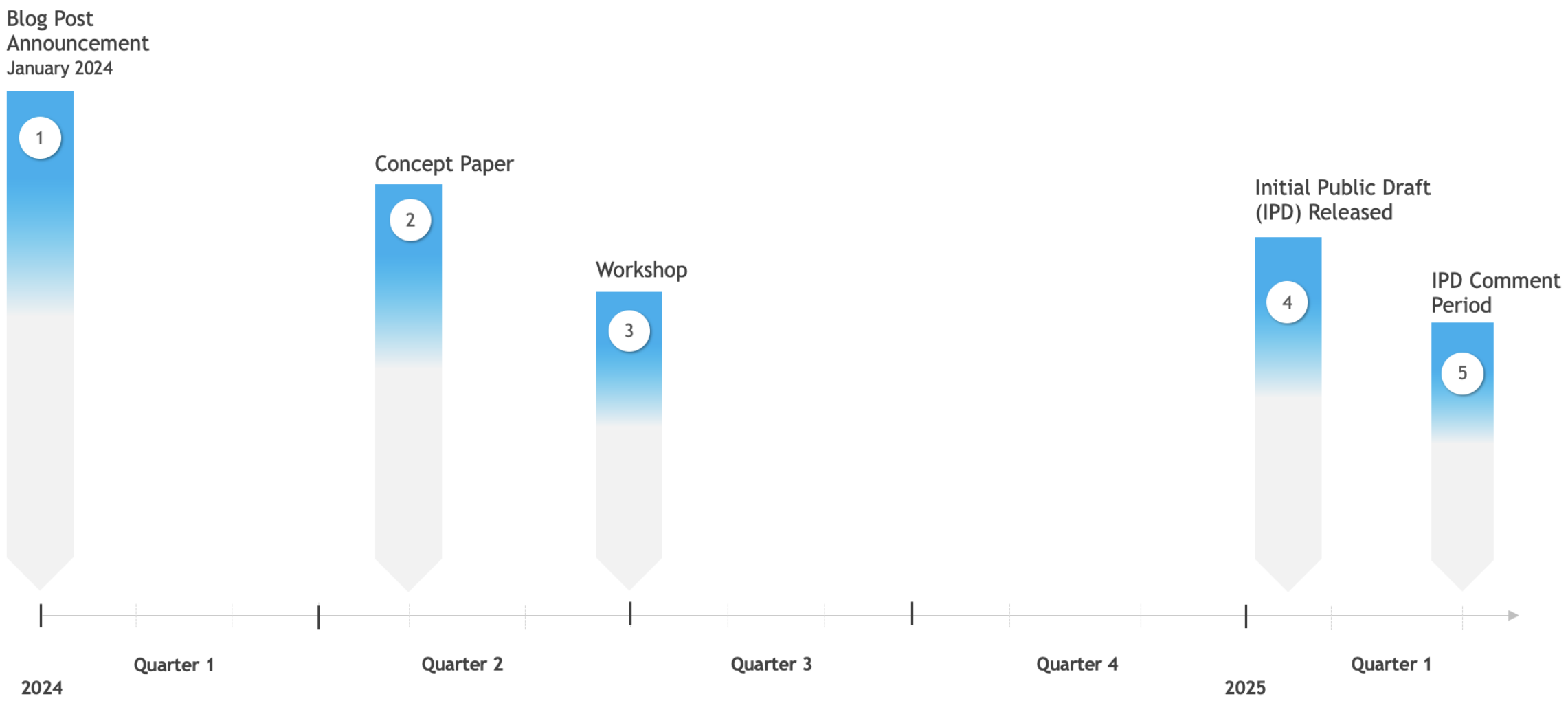
Arabic, Indonesian, Malay, Portuguese, Spanish

Guidelines & Tools

- NIST Privacy and Security Controls Catalog (*SP 800-53 Rev. 5*)
- NIST Privacy Risk Assessment Methodology

Next Steps

Privacy Framework Version 1.1 Development Schedule



Stay Engaged

Website

https://www.nist.gov/privacyframework

Mailing List

Send email to:

privacyframework+subscribe@list.nist.gov

Contact Us

PrivacyFramework@nist.gov

@NISTcyber #PrivacyFramework

Appendix: Core

Identify-P

Function	Category	Subcategory
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
		ID.IM-P4: Data actions of the systems/products/services are inventoried.
		ID.IM-P5: The purposes for the data actions are inventoried.
		ID.IM-P6: Data elements within the data actions are inventoried.
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated.
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.

Identify-P (continued)

Function	Category	Subcategory
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
		ID.RA-P3: Potential problematic data actions and associated problems are identified.
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.
		ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.
		ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.

Govern-P

Function	Category	Subcategory
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.
	Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.
		GV.AT-P2: Senior executives understand their roles and responsibilities.
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.

Govern-P (continued)

	Function	Category	Subcategory
		Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
			GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
			GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
			GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).
			GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
			GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.

Control-P

Function	Category	Subcategory
CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
		CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
		CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
	Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.
		CT.DM-P3: Data elements can be accessed for alteration.
		CT.DM-P4: Data elements can be accessed for deletion.
		CT.DM-P5: Data are destroyed according to policy.
		CT.DM-P6: Data are transmitted using standardized formats.
		CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
		CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.
		CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.

Control-P (continued)

	Function	Category	Subcategory
		Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
			CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
			CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
			CT.DP-P5: Attribute references are substituted for attribute values.

Communicate-P

Function	Category	Subcategory
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
		CM.AW-P3: System/product/service design enables data processing visibility.
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
		CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

Protect-P

Function	Category	Subcategory
PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).
		PR.PO-P2: Configuration change control processes are established and in place.
		PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.PO-P5: Protection processes are improved.
		PR.PO-P6: Effectiveness of protection technologies is shared.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Protect-P (continued)

Function	Category	Subcategory
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
		PR.DS-P4: Adequate capacity to ensure availability is maintained.
		PR.DS-P5: Protections against data leaks are implemented.
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		PR.PT-P3: Communications and control networks are protected.
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

NIST SP 800-66r2: An Overview

Jeffrey Marron| NIST IT Specialist – INFOSEC
Nick Heesters| HHS OCR Senior Advisor for Cybersecurity
October 2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication (SP) 800-66 Rev. 2 – February 2024

PUBLICATIONS

NIST SP 800-66 Rev. 2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide

Author(s)

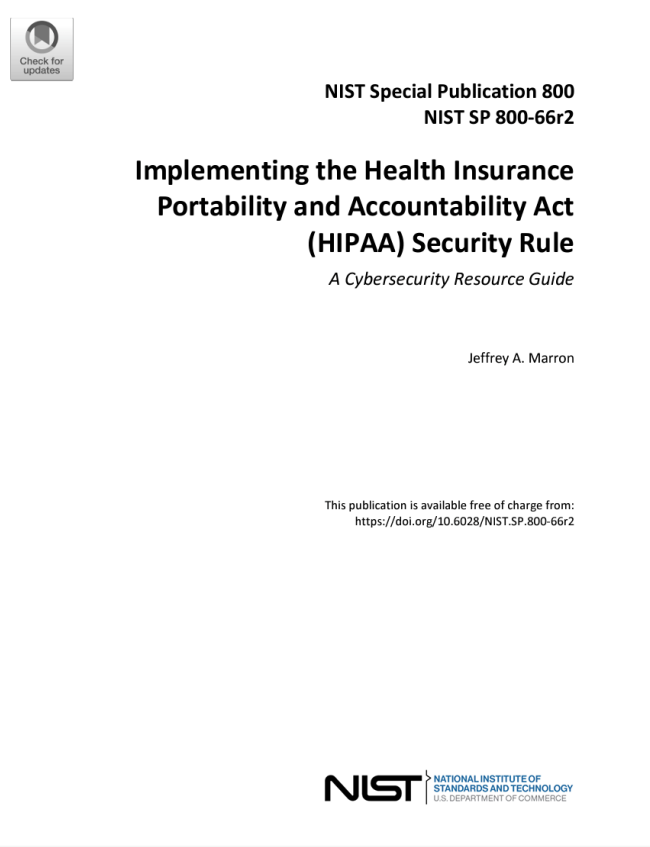
Jeffrey Marron (NIST)

Abstract

The HIPAA Security Rule focuses on safeguarding electronic protected health information (ePHI) held or maintained by regulated entities. The ePHI that a regulated entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. This 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.

Keywords

administrative safeguards; Health Insurance Portability and Accountability Act; implementation specification; physical safeguards; risk assessment; risk management; Security Rule; standards; technical safeguards



Check for updates

NIST Special Publication 800
NIST SP 800-66r2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

More details: https://csrc.nist.gov/pubs/sp/800/66/r2/final

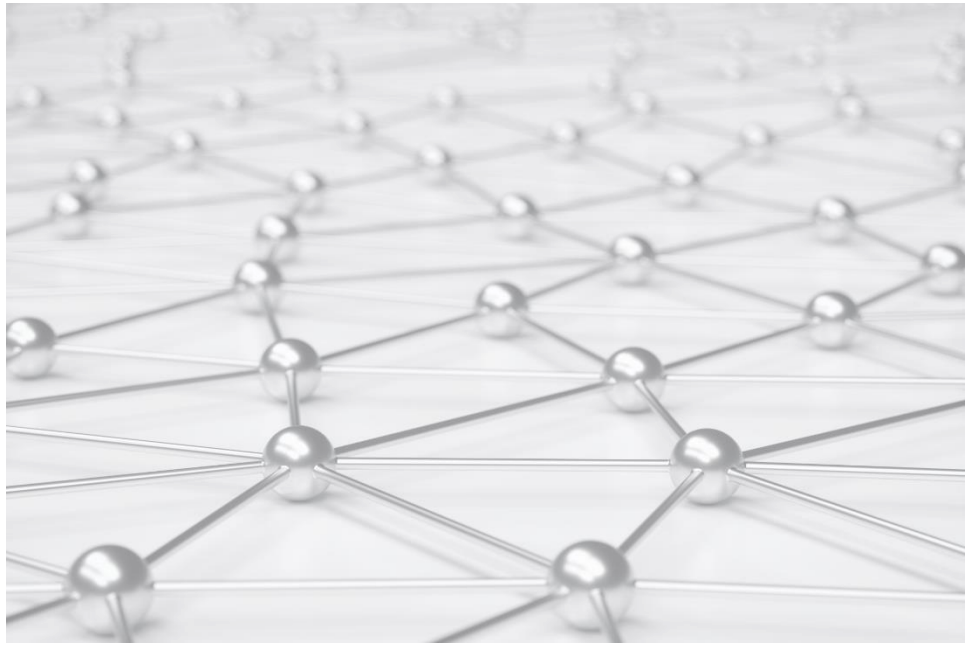
HIPAA Security Rule Overview

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

- Safeguards the confidentiality, integrity, and availability of electronic protected health information (ePHI)

Security Rule Standards

- Administrative Safeguards – actions and policies that manage and maintain security measures to protect ePHI
- Physical Safeguards – physical measures that protect a covered entity's electronic information systems, buildings, and equipment
- Technical Safeguards – technology, policy, and procedures that protect ePHI and control access to it
- Organizational Requirements – standards for business associate contracts and entities and other arrangements for group health plans
- Policies, Procedures, & Documentation Requirements – implementation of appropriate policies & procedures to comply with requirements of the Security Rule & maintaining records of these policies



Examples highlighted on the NIST Cybersecurity and Privacy Reference Tool: Cybersecurity and Privacy Reference Tool | CSRC (nist.gov)

HIPAA Security Rule Overview (cont)

Standard	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure (A)
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)

- An implementation specification is a more detailed description of the method or approach that regulated entities can use to meet a particular standard
- SP 800-66r2 “aims to help educate readers about the security standards included in the HIPAA Security Rule and assist regulated entities in their implementation of the Security Rule.”

Assessing Risk to ePHI

NIST

Section 3 of SP 800-66r2 discusses a risk assessment process

Recent OCR findings and fines on healthcare covered entities are related to lack of a Security Risk Assessment

1. **Prepare** for the assessment – understand use of ePHI
2. Identify reasonably anticipated **threats** to ePHI
3. Identify **vulnerabilities** that could be exploited
4. Determine **likelihood** of threat exploiting a vulnerability
5. Determine **impact** of threat exploiting a vulnerability
6. Determine **level** of risk
7. **Document** risk assessment results

Determining Likelihood and Level of Risk

Likelihood of Threat Event Initiation or Occurrence	Likelihood that Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Threat Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Managing Risk to ePHI

NIST

Section 4 of SP 800-66r2 discusses a risk management process

1. Assess risks
   - Determine organizational **risk tolerance** level(s)
   - Which threat/vulnerability pairs exceed risk tolerance?
   - Do standards and implementation specifications reduce risk below risk tolerance levels?
2. Implement **additional security controls** to bring risk to ePHI within risk tolerance
   - Are other organizational controls already in place?
   - Revisit risk tolerance levels or avoid risk to ePHI
3. Document risk management activities

Self-Assessment for Regulated Entities

NIST

Section 5 of SP 800-66r2 discusses considerations for regulated entities when implementing the Security Rule's standards

- **Key Activities**: Actions that are often associated with the security functions suggested by each HIPAA Security Rule standard
- **Description**: Includes the types of activities that a regulated entity may pursue in implementing a standard.
- **Sample Questions**: Includes questions that a regulated entity may ask itself to determine whether the standard has been adequately implemented

Self-Assessment for Regulated Entities (cont)

NIST

5.1.5. Security Awareness and Training (§ 164.308(a)(5))[61]

HIPAA Standard: *Implement a security awareness and training program for all members of its workforce (including management).*

Table 12. Key activities, descriptions, and sample questions for the Security Awareness and Training standard

Key Activities	Description	Sample Questions
1. **Conduct a Training Needs Assessment**	• Determine the training needs of the organization. • Interview and involve key personnel in assessing security training needs. • Use feedback and analysis of past events to help determine training needs. • Review organizational behavior issues, past incidents, and/or breaches to determine what training is missing or needs reinforcement, improvement, or periodic reminders.	• What awareness, training, and education programs are needed? Which are required? • Is the organization monitoring current threats to determine possible areas of training needs? • Are there current, relevant threats (e.g., phishing, ransomware) about which personnel need training? • Do workforce members need training on any particular organization devices (e.g., IoT devices) or technology that pose a risk to ePHI? • What is the current status regarding how these needs are being addressed (e.g., how well are current efforts working)? • Where are the gaps between the needs and what is being done (e.g., what more needs to be done)? • What are the training priorities in terms of content and audience?
2. **Develop and Approve a Training Strategy and a Plan**	• Address the specific HIPAA policies that require security awareness and training in the security awareness and training program.	• Is there a procedure in place to ensure that everyone in the organization receives security awareness training, including teleworkers and remote personnel?

Self-Assessment for Regulated Entities (cont)

NIST

5.3.4. Person or Entity Authentication (§ 164.312(d))[139]

HIPAA Standard: *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*

Table 24. Key activities, descriptions, and sample questions for the Person or Entity Authentication standard

Key Activities	Description	Sample Questions
1. **Determine Authentication Applicability to Current Systems/Applications**	• Identify the methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed (45 CFR § 164.304). • Identify points of electronic access that require or should require authentication. Ensure that the regulated entity's risk analysis properly assesses risks for such access points (e.g., risks of unauthorized access from within the enterprise could be different than those of remote unauthorized access). • Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that they have been authorized for specific access privileges to information and information systems.	• What authentication methods are available? • What are the advantages and disadvantages of each method? • Can risks of unauthorized access be sufficiently reduced for each point of electronic access with available authentication methods? • What will it cost to implement the available methods in the environment? • Are there trained staff who can maintain the system or should outsourced support be considered? • Are passwords being used? If so, are they unique to the individual? • Is MFA being used? If so, how and where is it implemented?
2. **Evaluate Available Authentication Options**	• Weigh the relative advantages and disadvantages of commonly used authentication approaches. • There are three commonly used authentication approaches available: 1. Something a person knows, such as a password 2. Something a person has or is in possession of, such as a token (e.g., smart card, hardware token) 3. Some type of biometric identification that a person provides, such as a fingerprint	• What are the strengths and weaknesses of each available option? • Which can be best supported with assigned resources (e.g., budget/staffing)? • What level of authentication is appropriate for each access to ePHI based on the assessment of risk? • Has the organization identified all instances of access to ePHI (including by services, vendors, or application programming interfaces [APIs]) and considered

NIST Cybersecurity and Privacy Reference Tool (CPRT) Mapping

Security Rule Identifiers	Security Rules	Standards Identifiers	Standards	Key Activities	Descriptions	Sample Questions
164.308	Administrative Safeguards: Defined in the Security Rule as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."	164.308(a)(1)	Security Management Process: HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.	Identify all ePHI and Relevant Information Systems	Identify where ePHI is generated within the organization, where it enters the organization, where it moves within the organization, where it is stored, and where it leaves the organization. Identify all systems that house ePHI. Be sure to identify mobile devices, medical equipment, and medical IoT devices that store, process, or transmit ePHI. Include all hardware and software that are used to collect, store, process, or transmit ePHI. Analyze business functions and verify the ownership and control of information system elements as necessary. Consider the impact of a merger or acquisition on risks to ePHI. During a merger or acquisition, new data pathways may be introduced that lead to ePHI being stored, processed, or transmitted in previously unanticipated places.	Has all ePHI generated, stored, processed, and transmitted within the organization been identified? Are all hardware and software for which the organization is responsible periodically inventoried? Is the hardware and software inventory updated on a regular basis? Have hardware and software that maintains or transmits ePHI been identified? Does this inventory include removable media and remote access devices? Is the current configuration of organizational systems documented, including connections to other systems? Has a BIA been performed?

Planning Note (02/14/2024):

See NIST's Cybersecurity and Privacy Reference Tool (CPRT) for the following content:

- Key activities, descriptions, and sample questions from the tables in Section 5
- Mappings of the HIPAA Security Rule's standards and implementation specifications to NIST Cybersecurity Framework Subcategories and SP 800-53r5 security controls
- Listings of NIST publications relevant to each HIPAA Security Rule standard

More details: Cybersecurity and Privacy Reference Tool | CSRC (nist.gov)

(CPRT) HIPAA Security Rule Mappings

Key Activities	Description	Sample Questions
1. Isolate Healthcare Clearinghouse Functions [25]	• If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization. • Determine whether a component of the regulated entity constitutes a healthcare clearinghouse under the HIPAA Security Rule. • If no clearinghouse functions exist, document this finding. If a clearinghouse exists within the organization, implement procedures for access that are consistent with the HIPAA Privacy Rule.	• If healthcare clearinghouse functions are performed, are policies and procedures implemented to protect ePHI from the other functions of the larger organization? • Does the healthcare clearinghouse share hardware or software with a larger organization of which it is a part? • Does the healthcare clearinghouse share staff or physical space with staff from a larger organization? • Has a separate network or subsystem been established for the healthcare clearinghouse, if reasonable and appropriate? • Has staff of the healthcare clearinghouse been trained to safeguard ePHI from disclosure to the larger organization, if required for compliance with the HIPAA Privacy Rule?
Implementation Specification (Required)	• *If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.* **Hide all 164.308(a)(4)(ii)(A) References** + 164.308(a)(4)(ii)(A) to CSF v1.1 + 164.308(a)(4)(ii)(A) to SP 800-53 Rev 5.1.1	

More details: Cybersecurity and Privacy Reference Tool | CSRC (nist.gov)

National Online Informative References (OLIR) Program

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS OLIR

National Online Informative References Program OLIR

The OLIR Catalog provides an interface for Developers and Users to view Informative References and analyze Reference Data

Status	Informative Reference (version)	Reference Document	Posted Date	Focal Document
Final	HIPAA-Sec-Rule-CSFv1.1 (1.0.0) (More Details)	Health Insurance Portability and Accountability Act (HIPAA)	2024-03-20	Framework for Improving Critical Infrastructure Cybersecurity
Final	HIPAA-Sec-Rule-800-53-5.1.1 (1.0.0) (More Details)	Health Insurance Portability and Accountability Act (HIPAA)	2024-03-20	Security and Privacy Controls for Information Systems and Organizations

Topical Resources for Regulated Entities

Appendix F of SP 800-66r2: points to an annotated, topical listing of additional **resources** hosted on the document's webpage:

NIST SP 800-66 Rev. 2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide

Date Published: February 2024

Supersedes: SP 800-66 Rev. 1 (10/23/2008)

Planning Note (02/14/2024):

See NIST's Cybersecurity and Privacy Reference Tool (CPRT) for the following content:

- Key activities, descriptions, and sample questions from the tables in Section 5
- Mappings of the HIPAA Security Rule's standards and implementation specifications to NIST Cybersecurity Framework

DOCUMENTATION

Publication:

https://doi.org/10.6028/NIST.SP.800-66r2

Download URL

Supplemental Material:

Appendix F: HIPAA Security Rule Resources (pdf)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STAY IN TOUCH

CONTACT US

NIST.gov

@NIST

HHS Cybersecurity Resources

HHS OCR Guidance:

- Ransomware & HIPAA Video: https://www.youtube.com/watch?v=nBKUlAy1OFA
- Ransomware Fact Sheet: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- Cybersecurity Materials: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- How HIPAA Can Help Defend Against Common Cyberattacks: https://www.youtube.com/watch?v=VnbBxxyZLc8
- HIPAA Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

HHS Healthcare Public Health (HPH) Sector Cybersecurity Performance Goals (CPG):

- https://hhscyber.hhs.gov/performance-goals.html

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients:

- https://405d.hhs.gov/information

HHS Security Risk Assessment Tool:

- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Connect with OCR

Office for Civil Rights
U.S. Department of Health and Human Services

www.hhs.gov/hipaa

Join our Privacy and Security listservs at
https://www.hhs.gov/hipaa/for-professionals/list-serve/

@HHSOCR

HHS Cybersecurity Activities Panel

Moderator

- **Timothy Noonan**, Deputy Director, Health Information Privacy, Data, and Cybersecurity, HHS Office for Civil Rights

Panelists

- **Brian Mazanec**, Deputy Director, Office of Preparedness, HHS Administration for Strategic Preparedness and Response
- **Steve Posnack**, Principal Deputy Assistant Secretary Technology Policy, HHS ASTP/ONC
- **Jessica Wilkerson**, Senior Cyber Policy Advisor Division of Medical Device Cybersecurity, FDA

Related Resources

OCR

- HIPAA Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/index.html
- HIPAA Security Rule Guidance:
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- HIPAA Security Rule Videos:
  - https://www.youtube.com/@USGovHHSOCR
  - https://www.youtube.com/watch?v=VnbBxxyZLc8

ASPR

- HPH Cybersecurity Gateway: https://hhscyber.hhs.gov
- HHS 405(d) – Health Care Industry Cybersecurity Practices: https://405d.hhs.gov

ASTP/ONC

- Health IT: https://www.healthit.gov
- Security Risk Assessment Tool
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

FDA

- Medical Device Cybersecurity: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

HIPAA Security Rule Policy Update

Marissa Gordon-Nguyen
Senior Advisor for Policy
Health Information Privacy, Data, and Cybersecurity Division
HHS Office for Civil Rights

October 23, 2024

1996 – HIPAA Enacted

- Efficiency and effectiveness of the health care system
  - Security for electronic health information transactions
    - Considerations for security standards
      - What's needed?
      - What's possible?
      - How hard is it?
    - Administrative, physical, and technical safeguards

1998 Proposed Rule → 2003 Final Rule

- Health Care Financing Administration (HCFA)
- Administrative procedures, Physical safeguards, Technical security services, and Technical security mechanisms
- Requirements and Implementation features
- 2,350 public comments

- Centers for Medicare and Medicaid Services (CMS)
- Administrative, Physical, and Technical safeguards and Organizational requirements
- Standards and Implementation specifications
- Based on comments, standards framed in generic terms

2009 HITECH Act

- Promotion of health information technology for improving health care quality, safety, and efficiency
- Business associate liability for compliance with Security Rule requirements
- Annual guidance on effective and appropriate security safeguards
- Increased penalties for violations of the HIPAA Rules

2009 Delegation of Authority to OCR

- Secretary delegated Security Rule authority to OCR, citing:
  - Increased adoption of electronic records and electronic exchange

    ↓

    Increasing intersection of security and privacy
  - HITECH Act mandate to strengthen enforcement

2010 Proposed Rule → 2013 Final Rule

- HITECH Act penalties
- HITECH Act liability for business associates
- Definition of “electronic media”

Consistent Approach to HIPAA Security

- Confidentiality, integrity, and availability of ePHI
- Reasonable and appropriate safeguards
- Risk analysis and risk management
- Flexible, scalable, and technology neutral requirements

2024 Proposed Rule

- Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

- Under Review at White House Office of Management and Budget:

RegInfo.gov→Regulatory Review→EO 12866 Regulatory Review→HHS

Resources

- Security Rule:

http://www.hhs.gov/hipaa/for-professionals/security/index.html

- Sign up for OCR listserv updates at:

https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html

Contact Us

Office for Civil Rights

U.S. Department of Health and Human Services

ocrmail@hhs.gov
www.hhs.gov/ocr

Voice: (800) 368-1019
TDD: (800) 537-7697
Fax: (202) 519-3818

200 Independence Avenue, S.W.
H.H.H Building, Room 509-F
Washington, D.C. 20201