LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing
NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management

OVERALL CLASSIFICATION IS

TLP:WHITE

February 27, 2020

Agenda

- Purpose
- Introduction
- Privacy Framework
- Cybersecurity and Risk Management
- Privacy Risk Assessment
- Privacy Framework Basics: Core
- Privacy Framework Basics: Profiles
- Privacy Framework Basics: Implementation Tiers
- Privacy Framework Application
- Strengthening Accountability
- Questions

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

Forensic Stats

Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Purpose

- The security and privacy risks associated with sensitive information are increased by several growing trends in healthcare, including clinician mobility and wireless networking, health information exchange, Managed Service Providers (MSP), “bring your own devices,” and the use of Personal Health Records (PHRs).
- The sophistication of malware and security threats is increasing. Compounding these challenges are the limited budgets that healthcare organizations typically have available to mitigate risk, coupled with the rising consequences of failure to safeguard sensitive information.

Security Boulevard

NIST Privacy Framework

Purpose (continued)

- NIST recently **released** its privacy framework designed to provide organizations with privacy protection strategies to improve their current methods for using and protecting sensitive data, while clarifying privacy risk management concepts.
- The guide is also designed to help organizations identify the privacy outcomes they want to accomplish and prioritize steps to achieve those privacy goals.
- To apply the limited funds available in a way that maximizes the reduction of business risk, healthcare organizations should use a top-down approach based on risk assessment, and should mitigate risk through a combination of administrative, physical, and technical security controls.

Introduction

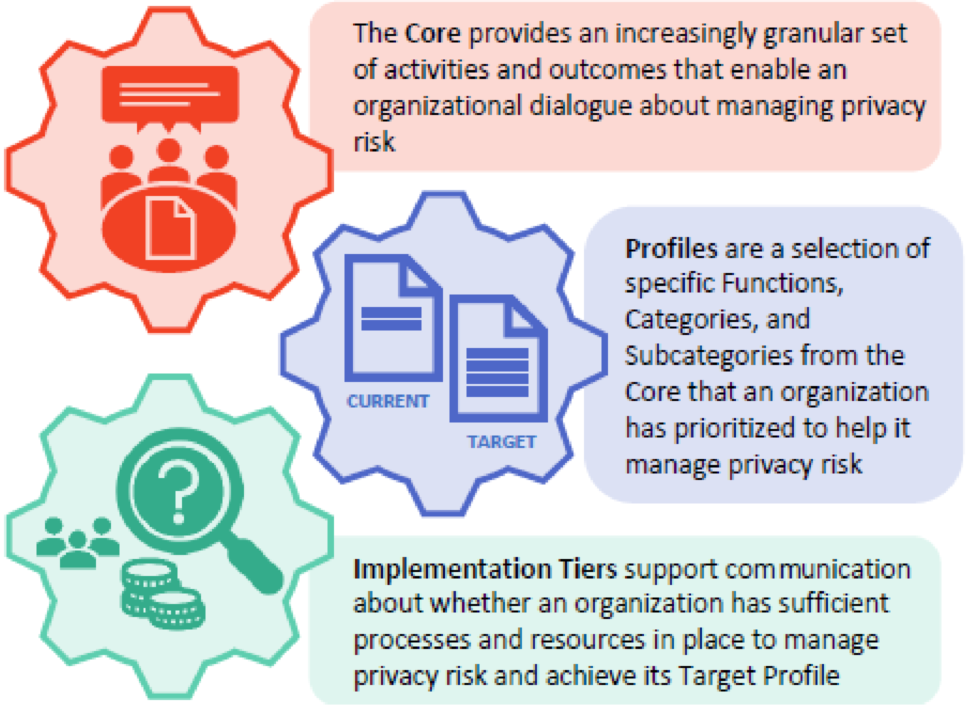
- Failure to manage *privacy risks* can negatively impact patients directly which would in turn have follow-on effects on health care organizations' brands, bottom lines, and future growth potential.
- Privacy is challenging because not only is it an all-encompassing concept that helps to safeguard important values such as human autonomy and dignity, but also the means for achieving it can vary.
- This voluntary NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction.
- Using an easily adaptable approach Privacy Framework's purpose is to help organizations manage privacy risks by:
  - Taking privacy into account as they design and deploy systems, products, and services that affect individuals;
  - Communicating about their privacy practices; and
  - Encouraging collaboration throughout the among executives, legal, and information technology (IT).

Health IT Security

NIST Privacy Framework

Privacy Framework

- The Privacy Framework is composed of three parts: Core, Profiles, and Implementation Tiers.
- Each component reinforces how organizations manage privacy risk through the connection between what is driving the business/mission, specific privacy risk management roles and responsibilities with in the organization, and privacy protection activities.
- Digital privacy risk management is a comparatively new concept, and privacy and security are related but distinct concepts.
  - An organization with a strong security posture may not be addressing all its privacy needs



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 an organization has prioritized to help it manage privacy risk

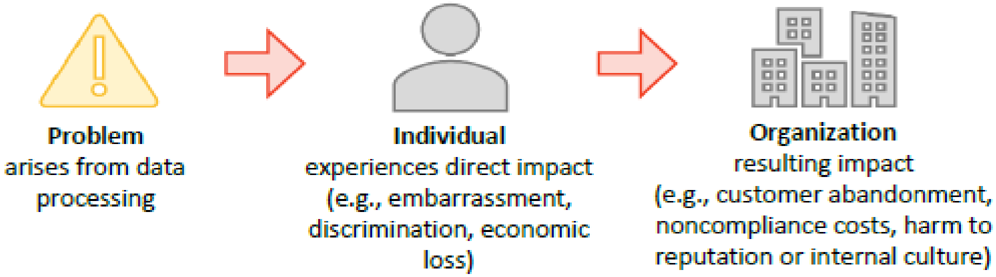
Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

NIST Privacy Framework

NIST Privacy Framework

Cybersecurity and Privacy Risk Management

- In today’s world of vital electronic information and malicious threats, healthcare organizations are finding that a reactive, bottom-up, technology-centric approach to determining security and privacy requirements is not adequate to protect the organization and its patients.
- The Privacy Framework approach to privacy risk is to consider *privacy events* as unique potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal.
- Problems also can arise where there is a loss of *confidentiality*, *integrity*, or *availability* at some point in the data processing, such as data theft by external attackers or the unauthorized access or use of data by employees.
- Once an organization can identify the likelihood of any given problem arising from the data processing, which the Privacy Framework refers to as a *problematic data action*, it can assess the impact should the problematic data action occur. This impact assessment is where privacy risk and organizational *risk* intersect. Individuals, whether singly or in groups (including at a societal level) experience the direct impact of problems.
    - Organizations commonly manage these types of impacts at the enterprise risk management level; by connecting problems that individuals experience to these well-understood organizational impacts, organizations can bring privacy risk into parity with other risks they are managing in their broader portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs.



Problem arises from data processing

Individual experiences direct impact (e.g., embarrassment, discrimination, economic loss)

Organization resulting impact (e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

NIST Privacy Framework

Privacy Risk Assessment

- The evaluation and identification of Privacy risks is know as *Privacy risk assessment.*

- Generally, privacy risk assessments assist organizations in weighing the benefits of the data processing against the risks and to determine the appropriate response—sometimes referred to as proportionality.

- There are several ways an organization may choose to respond to privacy risks such as:
  - **Mitigating the risk**
  - **Transferring or sharing the risk**
  - **Avoiding the risk**
  - **Accepting the risk**

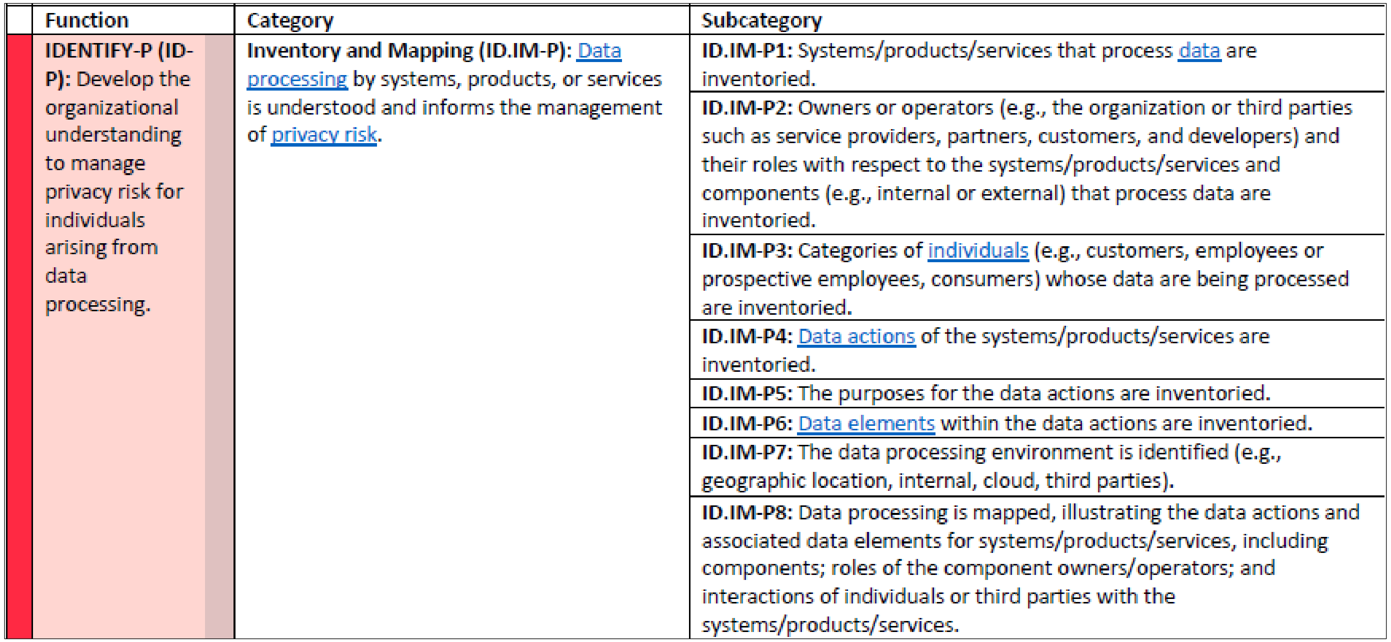
"Before I write my name on the board, I'll need to know how you're planning to use that data."

DATAFLOQ

NIST Privacy Framework

Privacy Framework: Core

- The Core provides a set of privacy protection activities.
- ***Functions*** are meant to assist the organization in their privacy risk management through management and comprehension of data processing, *risk management* decision making, and process improvement by learning from previous activities.
- **Categories** are the subdivisions of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category.



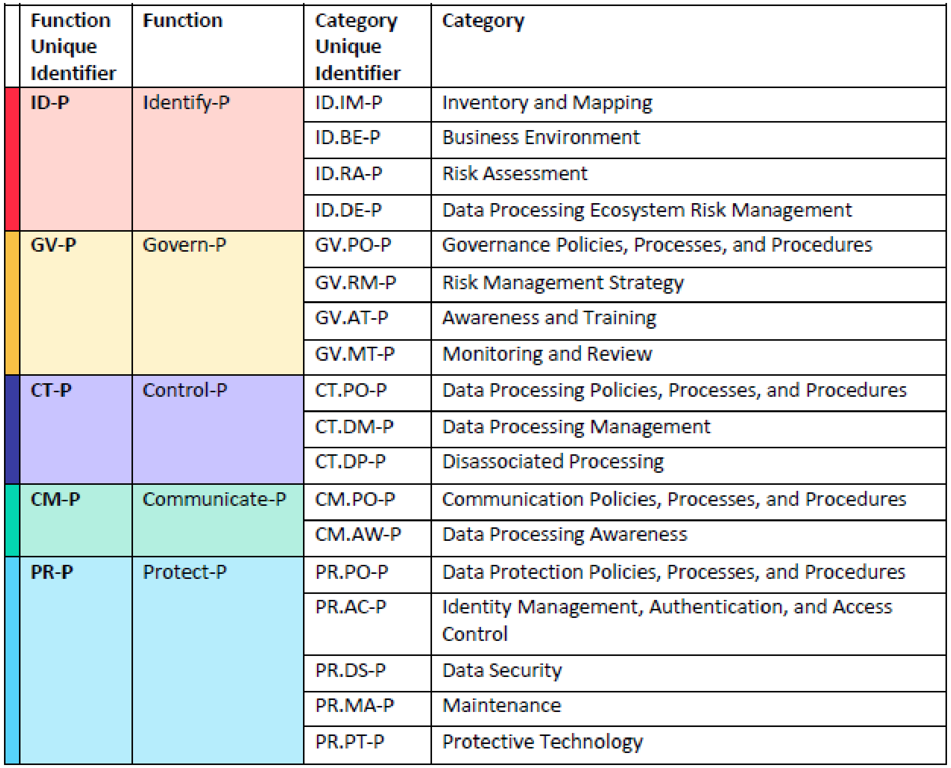
	Function	Category	Subcategory
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**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.

NIST Privacy Framework

NIST Privacy Framework

Privacy Framework: Core continued…

- The five Functions, Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P, defined below, can be used to manage privacy risks arising from data processing.
  - Identify-P – Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
  - Govern-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.
  - Control-P – Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
  - Communicate-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.
  - Protect-P – Develop and implement appropriate data processing safeguards.



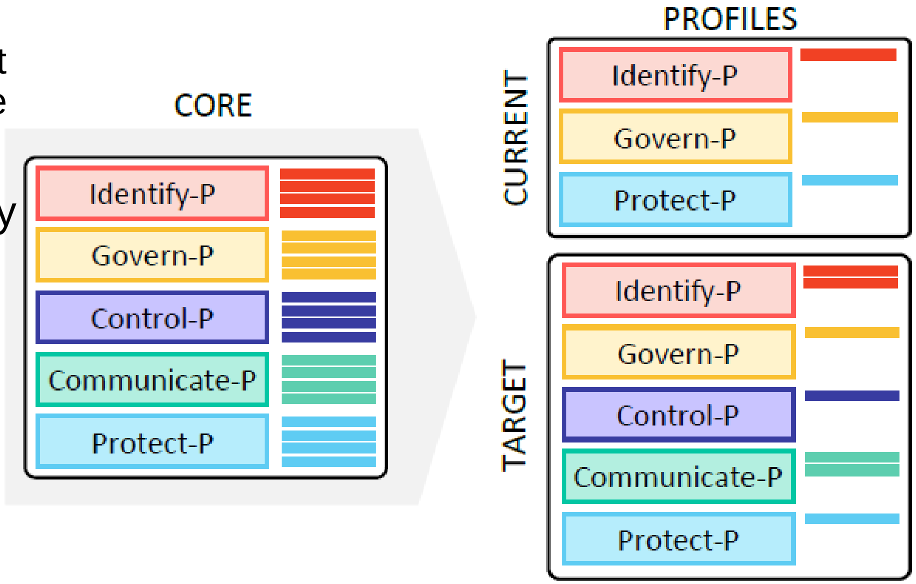
Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

NIST Privacy Framework

NIST Privacy Framework   Cybersecurity Framework

Privacy Framework: Profiles

- Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.
  - A Current Profile indicates an organizations current achievement privacy outcomes that an organization is currently achieving, while a Target Profile indicates the outcomes needed to achieve the desired privacy risk management goals.
- When developing a Profile, an organization may select or tailor the Functions, Categories, and Subcategories to its specific needs, including developing its own additional Functions, Categories, and Subcategories to account for unique organizational risks.
  - An organization determines these needs by considering its mission or business objectives, privacy values, and risk tolerance;



NIST Privacy Framework

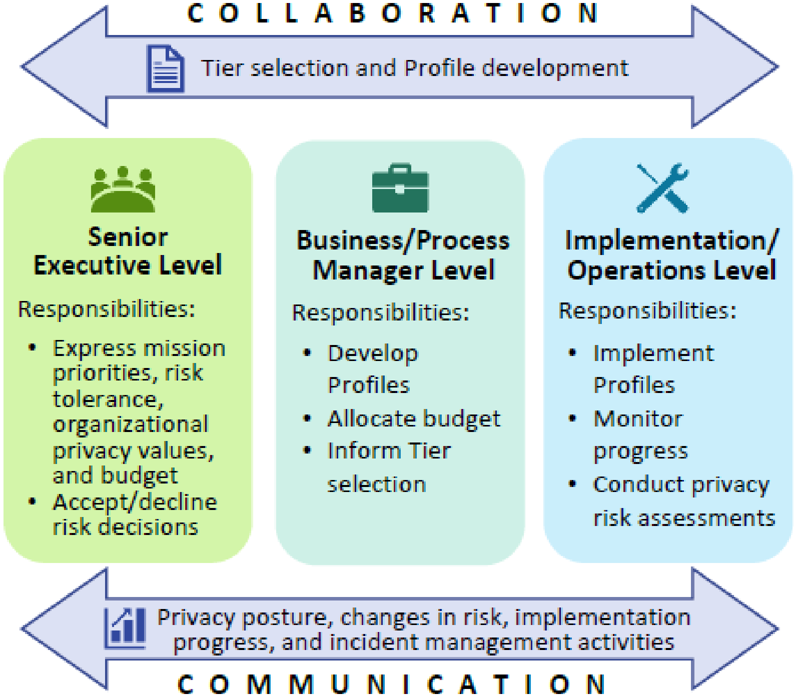
NIST Privacy Framework

Privacy Framework: Implementation Tiers

- Tiers support organizational decision-making about how to manage privacy risk by taking into account the nature of the privacy risks engendered by an organization's systems, products, or services and the sufficiency of the processes and resources an organization has in place to manage such risks.
- When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices, the degree of integration of privacy risk into its enterprise risk management portfolio, its data processing ecosystem relationships, and its workforce composition and training program.
- An organization can use the Tiers to communicate internally about resource allocations necessary to progress to a higher Tier or as general benchmarks to gauge progress in its capability to manage privacy risks.
- An organization can also use Tiers to understand the scale of resources and processes of other organizations in the data processing ecosystem and how they align with the organization's privacy risk management priorities.

Privacy Framework Application

- When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to optimize beneficial uses of data and the development of innovative systems, products, and services while minimizing adverse consequences for individuals.
- The Privacy Framework can help organizations answer the fundamental question, “How are we considering the impacts to individuals as we develop our systems, products, and services?”
    - An organization may already have robust privacy risk management processes, but may use the Core’s five Functions as a streamlined way to analyze and articulate any gaps.
    - Alternatively, an organization seeking to establish a privacy program can use the Core’s Categories and Subcategories as a reference.



COLLABORATION

Tier selection and Profile development

Senior Executive Level

Responsibilities:

- Express mission priorities, risk tolerance, organizational privacy values, and budget
- Accept/decline risk decisions

Business/Process Manager Level

Responsibilities:

- Develop Profiles
- Allocate budget
- Inform Tier selection

Implementation/ Operations Level

Responsibilities:

- Implement Profiles
- Monitor progress
- Conduct privacy risk assessments

Privacy posture, changes in risk, implementation progress, and incident management activities

COMMUNICATION

NIST Privacy Framework

NIST Privacy Framework

Strengthening Accountability

- Accountability is generally considered a key privacy principle, although conceptually it is not unique to privacy.
- Accountability occurs throughout an organization, and it can be expressed at varying degrees of abstraction, for example as a cultural value, as governance policies and procedures, or as traceability relationships between *privacy requirements* and *controls*.
- Privacy risk management can be a means of supporting accountability at all organizational levels as it connects senior executives, who can communicate an organization's privacy values and risk tolerance, to those at the business/process manager level, who can collaborate on the development and implementation of governance policies and procedures that support organizational privacy values.
- These policies and procedures can then be communicated to those at the implementation/operations level, who collaborate on defining the privacy requirements that support the expression of the policies and procedures in an organization's systems, products, and services.

NIST Privacy Framework

References

- NIST Publishes Privacy Framework

https://securityboulevard.com/2020/01/nist-publishes-privacy-framework/

- NIST: A Leader In Forensic Science and Valued CSAFE Partner

https://forensicstats.org/blog/2018/01/19/nist-leader-forensic-science-valued-csafe-partner/

- NIST PRIVACY FRAMEWORK: A Tool For Improving Privacy Through Enterprise Risk Management

https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

- Framework for Improving Critical Infrastructure Cybersecurity

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- Interoperability Slowed by Concerns Around Privacy and Security

https://healthitsecurity.com/news/interoperability-slowed-by-concerns-around-privacy-and-security

Questions

Upcoming Briefs

- Wearable Device Security

- Product Evaluations
- Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

- Requests for Information
- Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.