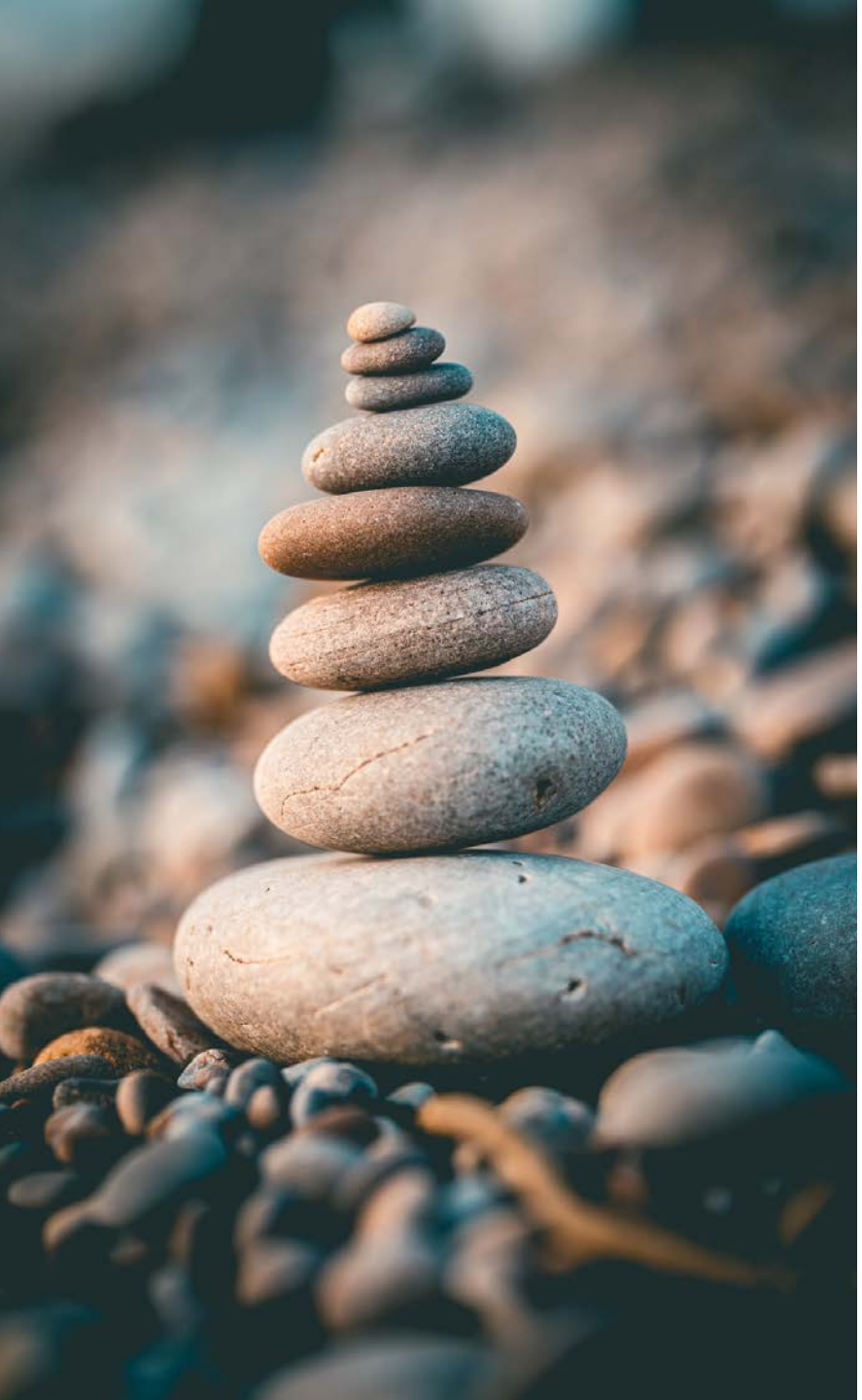
Building Trust through the NIST Privacy Framework

Chris Carlson

Principle Consultant, Level Perspective Inc



Agenda

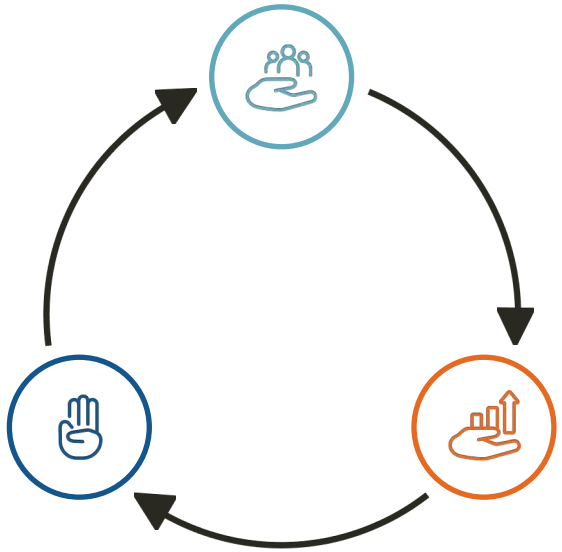
1. Trust in Healthcare
2. Trust in Health Information Management
3. NIST Privacy Framework

Trust in Healthcare

The Trust Landscape

1| Consistency & Reliability in Delivering Care

Accurate, complete, available, and up-to-date patient records across care settings



2| Transparency & Openness in Managing Health Data

Data Access: Easy medical record access, and clear data usage practices.

Informed Consent: Clear understanding of purpose and benefits of sharing.

Breach Notification: Prompt and transparent notification.

3| Integrity & Honesty in Patient Interactions

Ethical Use: using data only for intended/consented purpose.

Data Privacy & Security: Robust mechanisms to protect patient data

Trust in Healthcare

The Trust Challenge

Digital health solutions **multiply the volumes of patient data** being collected, processed, and shared.

With data breaches and privacy concerns making headlines, **patients are becoming increasingly wary** of how their sensitive health information is handled.

Trust in Health Information Management

NIST Privacy Framework

A National Institute of Standards and Technology framework to identify and manage privacy risks.

1| CORE

A set of privacy activities and outcomes that support detailed dialogue about privacy risks and desired outcomes.

2| PROFILES

A structured approach to identify an organization's current and desired state of privacy activities and outcomes.

3| IMPLEMENTATION TIERS

Descriptive categories regarding an organization's privacy risk management processes and resources for managing current and target state profiles.

Fosters a culture where privacy is integral to operations, ensuring that as digital health evolves, patient trust remains at the forefront.

1| The Core

Establishing a Common Language

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
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

PRIVACY FRAMEWORK FUNCTION AND CATEGORY UNIQUE IDENTIFIERS

Collection of activities and outcomes that establish a consistent understanding of privacy terms and objectives.

Helps establish an unambiguous (or at least less ambiguous) destination of desired outcomes.

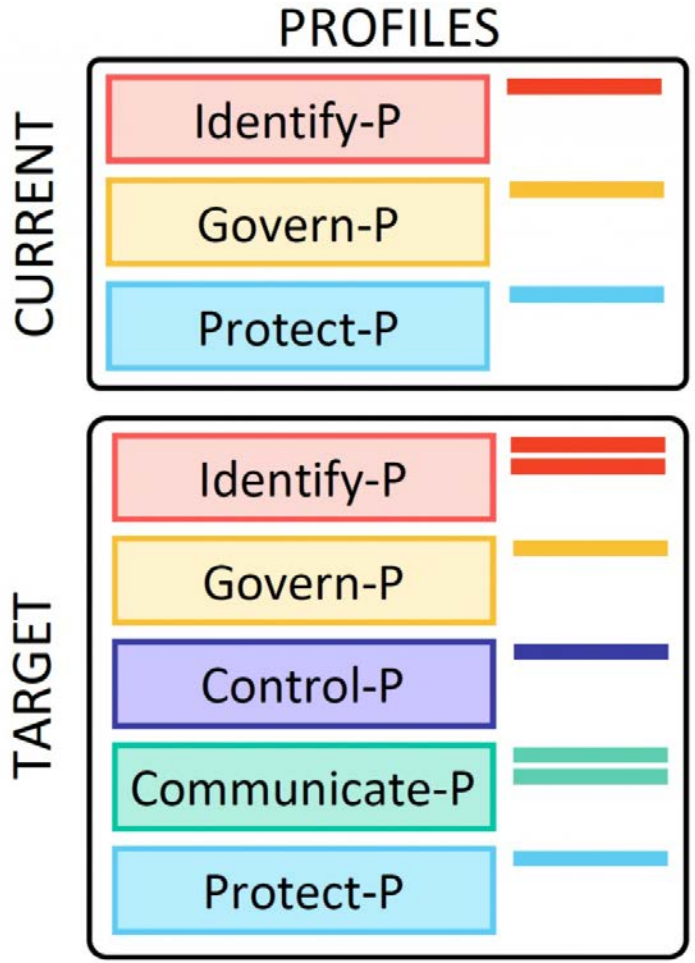
Function	Category	Subcategory
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, 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.

PRIVACY FRAMEWORK CORE

"The single biggest problem in communication is the illusion that it has taken place." George Bernard Shaw

2| Profiles

From Current Reality to Future Vision



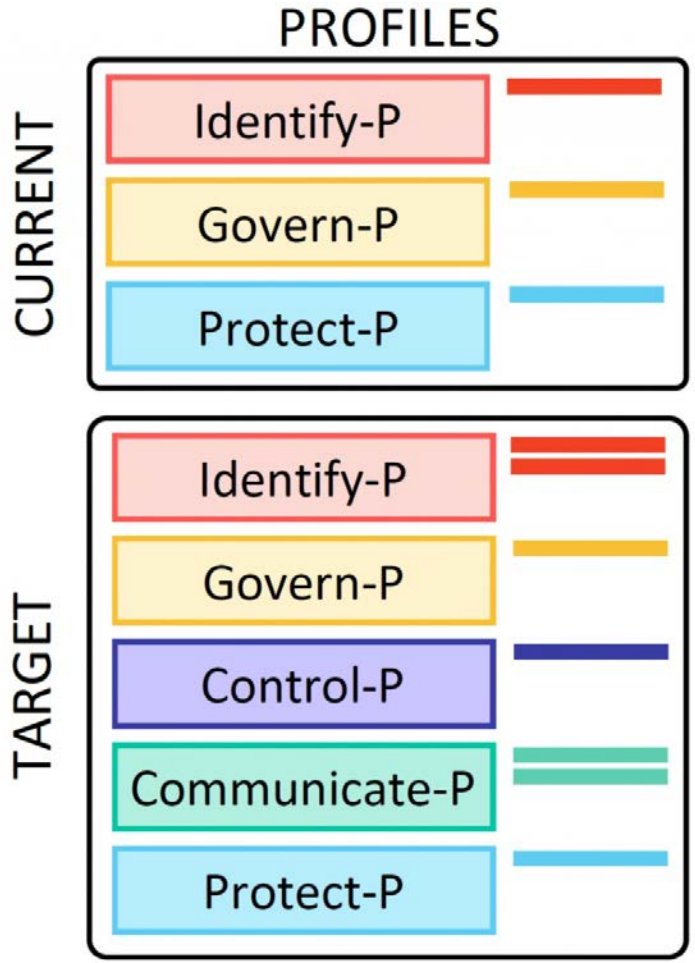
What are They?

Snapshot of Now: capture a clear picture of current privacy practices and outcomes.

Blueprint for Tomorrow: help define a vision for the desired future state of privacy practices and outcomes.

2| Profiles

From Current Reality to Future Vision



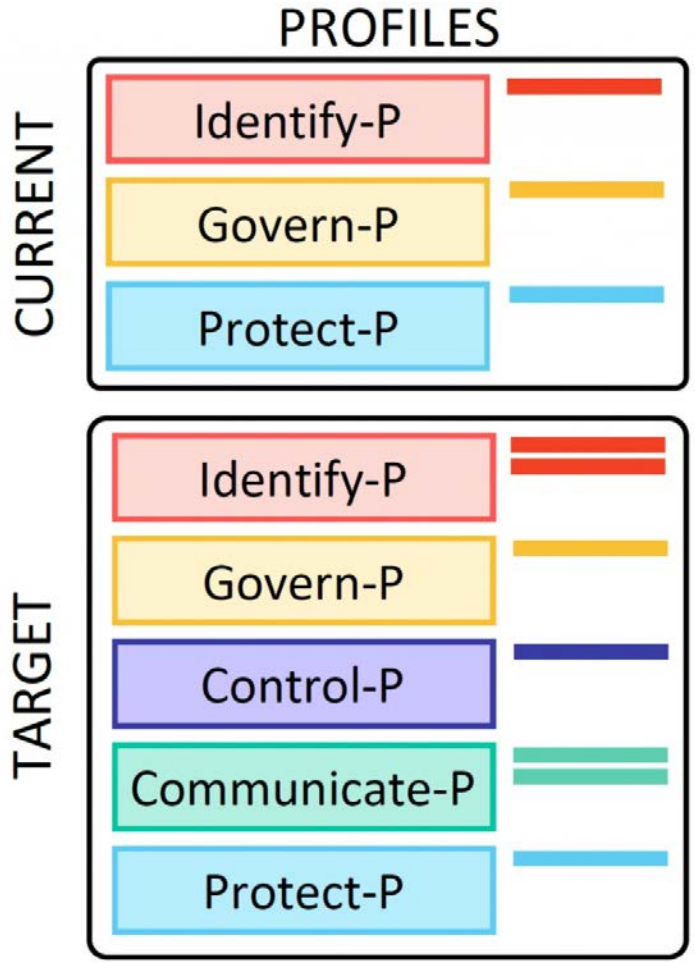
Current vs Target State

Self Assessment: by understanding the current state, privacy gaps, vulnerabilities and strengths can be identified

Strategic Vision: the target state acts as a north star, describing privacy measures tailored to the organization's unique needs

2| Profiles

From Current Reality to Future Vision



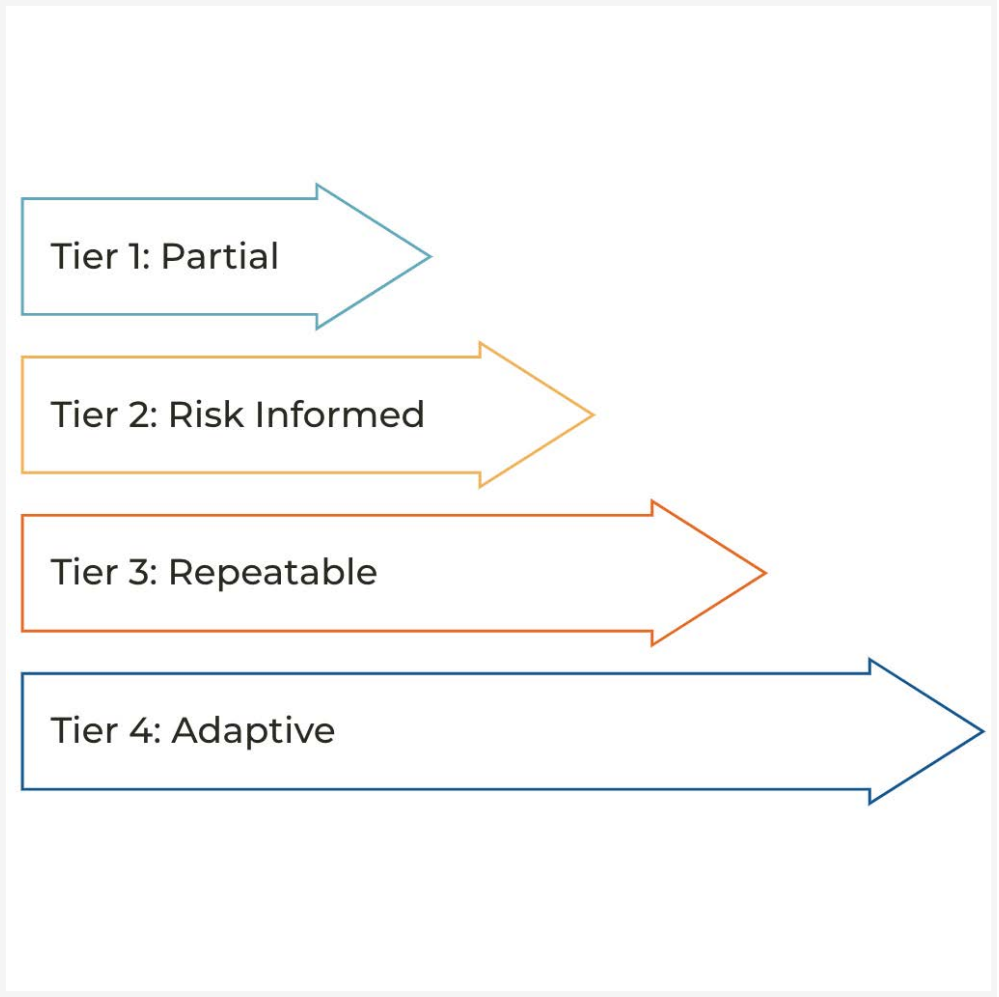
Stakeholder Alignment

Unified Direction: Promotes common understanding across all stakeholder groups

Collaborative Effort: Emphasizes collective and collaborative responsibilities and efforts in transition to target state.

3| Implementation Tiers

Descriptive Guidance for Progress



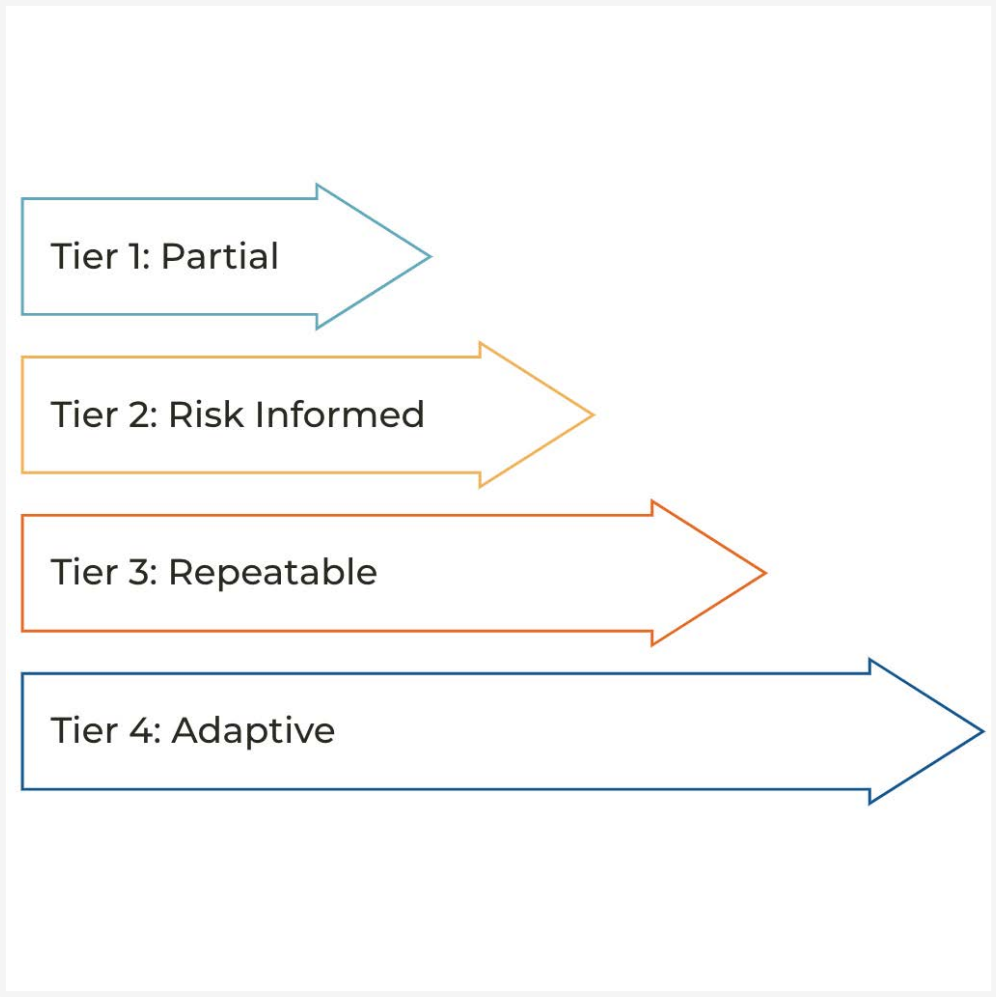
What are They?

Benchmarks of Maturity: Describe privacy practice sophistication, from basic (Tier 1) to advanced (Tier 4).

Not a One-Size-Fits-All: Tiers are not a linear progression but are tailored to the organization's specific risk profile and privacy needs.

3| Implementation Tiers

Descriptive Guidance for Progress



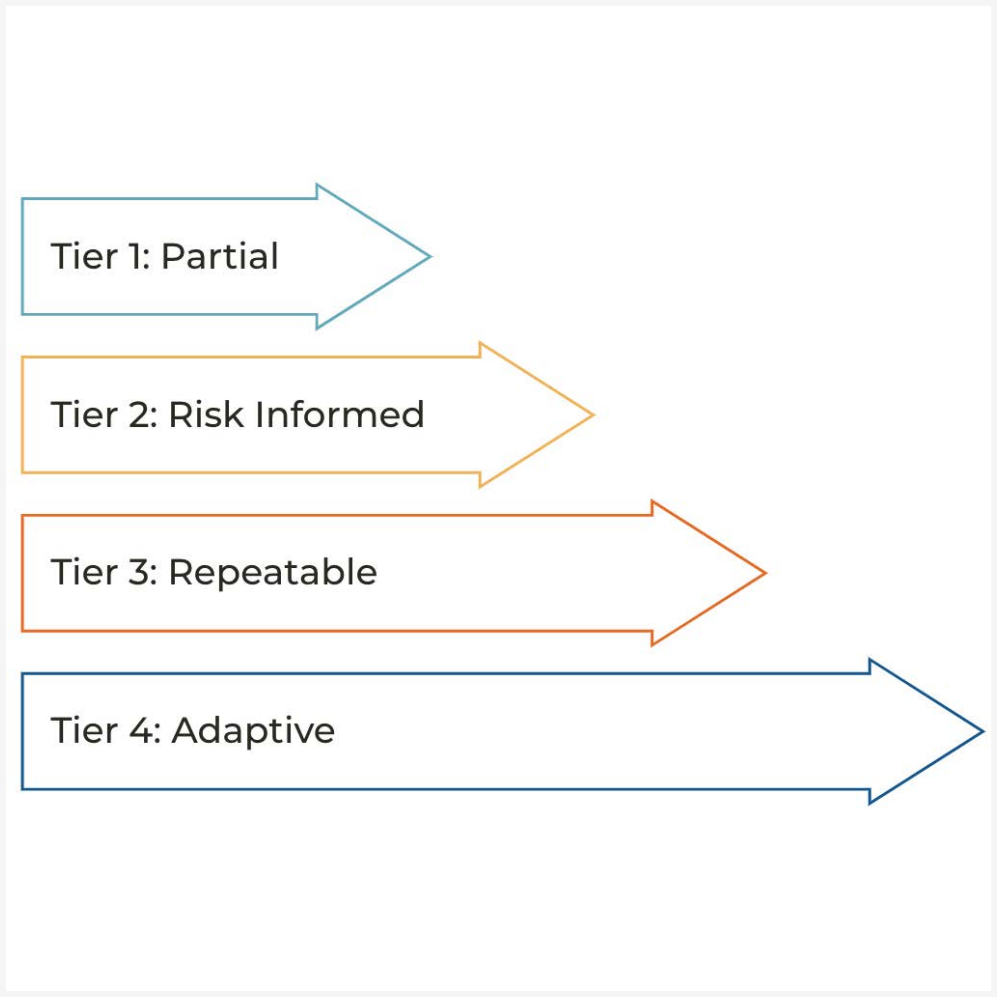
Measuring Current Practices

Self-Reflection: Help objectively assess current privacy posture and practices.

Identify Gaps: By understanding their current tier, organizations can pinpoint desired areas for enhancement or attention.

3| Implementation Tiers

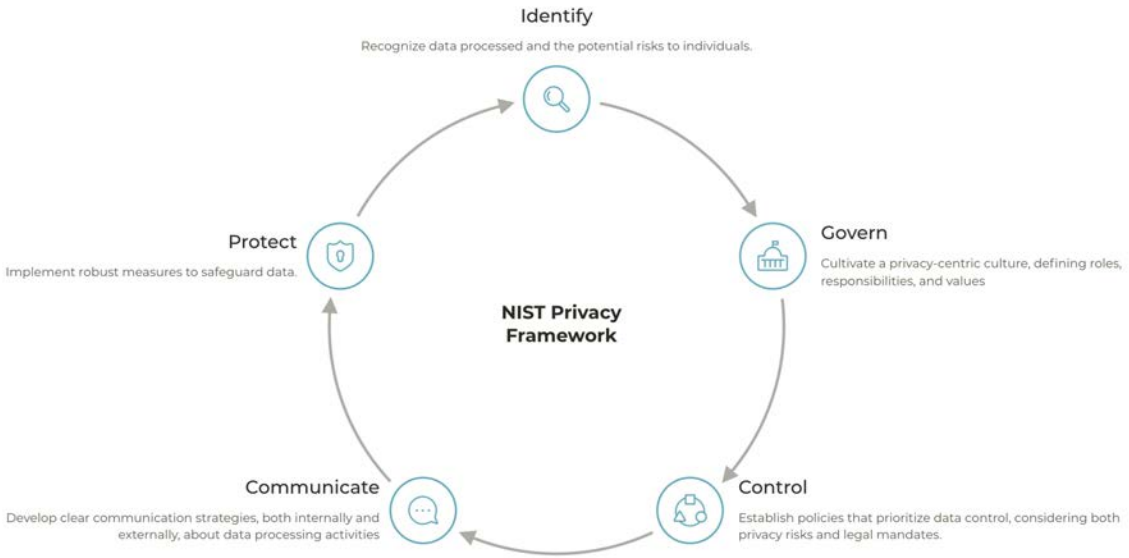
Descriptive Guidance for Progress



Roadmap to Desired State

Guided Progression: Provide a structured pathway to evolve privacy practices towards the desired target state.
Flexible & Adaptable: Can adapt and shift between tiers as privacy needs, risks, and objectives change over time.

Trust Through the NIST Privacy Framework



Challenges Addressed

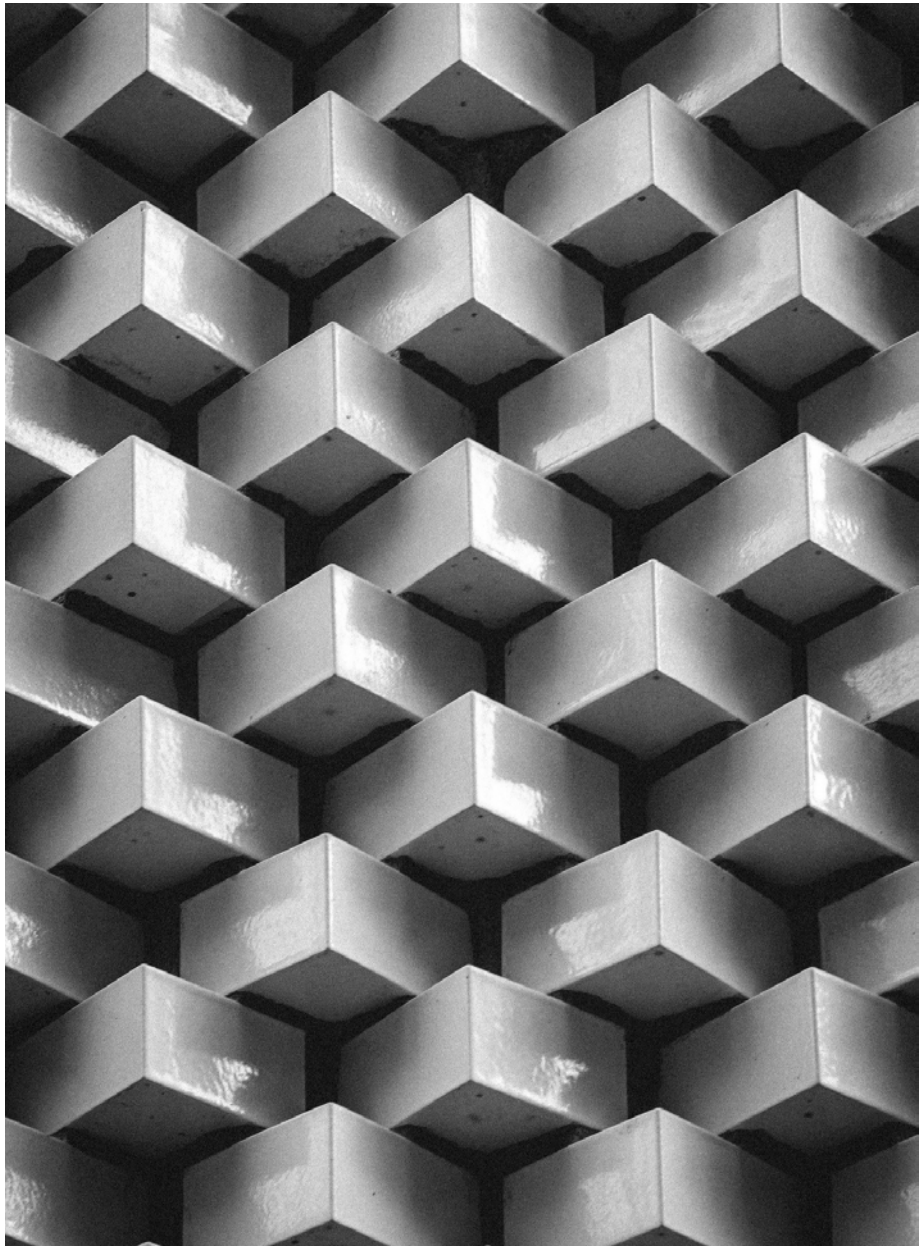
Rising Privacy Risks: Accelerated digital health solution adoption increases identifiable individual data processing and privacy risks.

The Multifaceted Nature of Privacy: Privacy, encompassing values like human autonomy and dignity, is broad and continuously evolving, making it challenging to consistently address and communicate.

Advantages of Adopting

Enhanced Communication: It establishes common language, objectives and tools that support clear, understandable and transparent conversations about data privacy.

Compliance and Beyond: Offers a systematic way to manage privacy outcomes across myriad data standards, systems, processes and legislative requirements, while also enabling organizational independence to prioritize and address areas of highest concern.



“Trust is built with consistency.”

Lincoln Chafee