Clearwater

Whitepaper

Building Frameworks to Manage Healthcare Data Within the Changing U.S. Privacy Landscape

Table of Contents

Introduction

As the world is more connected to digital life, state and federal agencies are issuing a growing number of standards and mandates focused on data privacy and protection.

Across the U.S., many states—for example, California, Nevada, and Maine—have already enacted state-directed privacy laws. Elsewhere, many other state governments are considering similar measures.

And while moves to protect data—especially protected health information (PHI) and personally identifiable information (PII)—are headed in the right direction, these state-level mandates can create confusion and compliance issues.

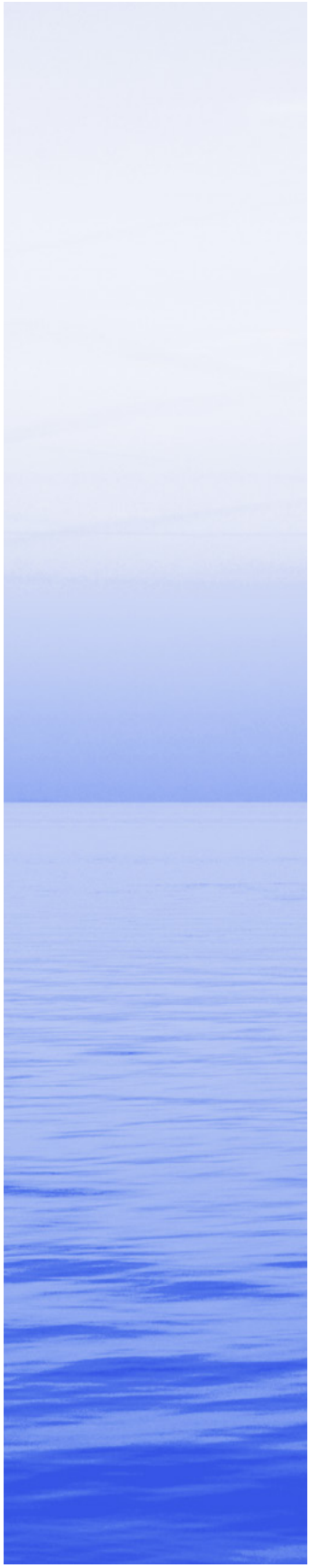
That's why there is a growing push among some for more unified, possibly even federalized, data privacy standards, similar, for example, to federal standards that protect health-related information through the Healthcare Accountability and Portability Act (HIPAA).

But as a healthcare organization that handles PHI or PII, how do you develop a data privacy and protection program that meets all of the emerging and changing standards and regulations, especially if you have limited resources or highly trained staff?

Setting the foundation of your program in an existing cybersecurity framework is a great place to start.

There are a variety of frameworks—from free recommendations from the National Institute of Standards and Technology (NIST) to more complex standards that entail certifications from the International Organization for Standardization (ISO).

But before we dive into NIST and ISO and explore how you can put them to use for your programs, let's look at some of the ways data and privacy laws are changing.



State privacy laws

We briefly mentioned that a growing number of states have enacted state-level data privacy requirements. An example of one is the California Consumer Privacy Act (CCPA). CCPA went into effect on Jan. 1, 2020, and enforcement is expected to begin by July 1, 2020.

While these are effective measures for data protection, CCPA doesn't apply to every organization doing business in California. It's only applicable if a business has a gross revenue that exceeds $25 million and if the company handles PII of 50,000 or more people each year. It also indicates the company must generate at least half of its revenue from selling consumer information.

Like the European General Data Protection Regulation (GDPR) that applies to businesses outside the EU that do business with EU consumers, CCPA could eventually apply to a larger set of entities.

Here's another example of a new state-level data privacy law: New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD).

SHIELD amends New York's existing data breach notification law. Here are some of the ways it changes some of the existing state standards:

- Broadens definition of private information
- Expands definition of a breach
- Expands territorial scope
- Imposes data security requirements

If you're unsure of specific privacy law mandates for your state, the International Association of Privacy Professionals (IAPP) has a state-by-state privacy law comparison you can review here.

Common privacy characteristics

According to IAPP, there are some common characteristics within existing and proposed state privacy laws. These laws look to tackle provisions for:

1. Right to access personal data collected or shared. This can include information collected about a person, the information shared with third parties, and which third parties have access to that data.
2. Right to request incorrect or outdated information be corrected, but not deleted
3. Right to have personal information deleted under certain restrictions

4. Right to restrict the business's ability to process personal information
5. Right of data portability, for example, to get personal information disclosure in a common file format
6. Right to opt out of selling of personal information to third parties
7. Right to prohibit businesses from making decisions about a person based only on automated processes that don't require input from a human
8. Right to seek civil damages from a violation
9. Strict opt-in for the sale of personal information for people younger than a certain age
10. Organizations must provide people with notices about certain data practices, privacy operations and privacy programs
11. Organizations are required to notify consumers and appropriate authorities when there is a breach
12. A requirement to do formal risk assessments related to privacy and security policies and procedures
13. Prevents organizations from treating a person who exercises a consumer right differently than one who does not
14. Prohibition of the collection of personal information without a specific use
15. Prohibition of processing personal information without a specific use
16. Obligation to exercise care, loyalty and confidentiality in the best interest of consumers

Here are a few things CCPA covers:

- The right of Californians to know what personal information is being collected about them
- The right of Californians to know if their personal information is sold or disclosed and to whom
- The right of Californians to opt out of the sale of personal information
- The right of Californians to access their personal information
- The right of Californians to equal service and price, even if they exercise their privacy rights

Proposed federal mandates

While there are common threads through some state laws like the 16 listed above, some professionals believe a federal standard could be more beneficial—but only if it's not more lax than existing state laws and wouldn't override more stringent mandates.

One such proposed law, Consumer Data Privacy and Security Act of 2020 (CDPSA), is currently in the Senate. If it becomes law, CDPSA would be consistent with current legal data privacy frameworks such as CCPA and GDRP.

CDPSA may be viewed more favorably for small and mid-size businesses than GDPR, for example, because it would exempt some small businesses from certain compliance requirements.

Building your data privacy program

The ever-changing and broadening privacy scope for organizations can make it challenging to create a new program or mature your existing policies and procedures.

So how do you deal with data privacy regulations and develop an effective privacy program at the same time? Start by looking at existing cybersecurity frameworks, your current scope of work, and where your company intends to grow both short and long term.

NIST Privacy Framework

The NIST Privacy Framework is a good place to start. It's free, readily available online, and easy to understand. Unlike ISO standards, NIST is non-regulatory, but it provides a solid framework to help you build your privacy risk management solution.

The NIST Privacy Framework is designed to be an enterprise risk management tool. It integrates privacy practices into your organizational processes and can be tailored to meet your specific organization needs.

NIST can help organizations of all sizes that deliver products or services—from any sector—improve privacy risk management processes by using a framework non-specific to one country or region that also promotes international cooperation and collaboration on privacy issues.

There are a lot of informative NIST references available for free online. You can use these to help create a new privacy program for your organization or strengthen the accountability of your program. One of the great things about this NIST framework is that it supports the typical system development lifecycle and you can use it within your existing data processing ecosystem.

The core of the NIST Privacy Framework are these functions:

- Identify
- Govern
- Control
- Communicate

NIST privacy framework components

While the NIST Privacy Framework may draw your attention as a great resource for addressing your internal privacy practices, it also addresses privacy risks related to external parties, like your supply chain. It consists of three main components: the core, profiles, and implementation tiers.

NIST core

The NIST core creates an increasingly granular set of activities and outcomes that helps your organization communicate and manage privacy risks. Core activities are designed to help your organization achieve a specific privacy outcome to help you manage risk, with three components: functions, categories, and subcategories.

NIST functions: identify

The identify function helps your organization understand and manage privacy risks for individuals that often arise from data processing. This includes inventorying and mapping, for example, your data processing systems, products or services. Which privacy risks are associated with each?

From there, map your data processes including data actions and associated elements for these systems, products, and services, including components, roles of the component owners/operators, and interactions individuals or third parties have with those systems, products, and services.

NIST functions: govern

The govern function helps you develop and implement your organizational governance structure to enable ongoing understanding of your risk management priorities, which are informed by privacy risk. This includes governance policies, processes, and procedures used to manage and monitor your regulatory, legal, environmental, and operational requirements to ensure you understand (and inform your stakeholders) of privacy risks.

NIST functions: control

The control function helps you develop and implement appropriate activities so you can manage your data with sufficient granularity to manage your organizational privacy risks. For example, you'll need to ensure your data is managed consistently with your organizational risk strategy to ensure you're protecting individuals' rights to privacy, increasing manageability of these processes, and enabling privacy principle implementation such as individual participation, data quality, and data minimization.

NIST functions: communicate

The communicate function is important for developing and implementing appropriate activities to ensure your organization has a reliable understanding about how you process data and associated privacy risks. It also ensures that effective mechanisms are in place and maintained to increase predictability consistent with your organization's risk strategy to protect privacy.

Some examples are notices or internal or public reports that communicate data processing purposes, practices, associated privacy risks, and options that support individuals' data processing preferences and requests.

NIST functions: protect

The protect function guides development and implementation of appropriate data processing safeguards to ensure your organization manages data consistently with your risk strategy to protect individual privacy and maintains data confidentiality, integrity, and availability – for example, data protection when data is at rest.

NIST profiles

NIST profiles include a selection of specific functions, categories, and subcategories from the NIST core to help your organization prioritize goals to manage privacy risk. For example:

- Organizational or industry sector goals
- Legal/regulatory requirements and industry best practices
- Organizational risk management priorities
- Privacy needs for individuals

To explore how the NIST core and NIST profiles are different, consider this: the core includes everything you should do. Your current profile outlines the policies and procedures you currently have. Your target profile is where you want to be as you journey to mature your program to include all of the core components.

NIST implementation tiers

NIST also has implementation tiers to guide how you communicate whether you have sufficient processes and resources in place to manage privacy risks and to reach your target profile. The implementation tiers can be used to map out a path to improve privacy.

A couple questions you should ask:

- What are the privacy risks you need to manage as an organization?
- Do you have sufficient resources and processes in place to manage your risks?

Implementation tiers can help you self-assess your privacy program to see if your program is:

- Partial
- Risk-informed
- Repeatable
- Adaptive

When looking at those tiers, where are you in terms of having resources and processes now and where do you want to be?

Implementing privacy frameworks

When it comes to implementing the NIST Privacy Framework for your organization, in addition to the implementation tiers, accountability and buy-in are key. Here are a few recommendations to bring your team on board with why this is an important program that will help protect your organization both short and long term:

- **Senior executives:** With buy-in and support from your senior executives and key stakeholders such as board members, you can more effectively communicate program priorities, establish organizational risk tolerance, outline your organization's privacy values, set budgets, and accept/decline risk decisions made over time.
- **Mid-level and other managers**: These managers will help you develop profiles, allocate budgets, and inform tier selection.

- **Implementation/operations:** Your implementation and operations teams are vital in implementing profiles, monitoring progress, and conducting privacy risk assessments.

Before beginning your privacy framework implementation, some additional helpful tips include:

- Organize your preparation resources
- Determine your privacy capabilities
- Define your privacy requirements
- Conduct privacy risk assessments
- Create privacy requirements with traceability
- Monitor changing privacy risks

ISO 27701 Privacy Information Management Systems (PIMS)

While NIST is free and doesn't require certifications, if you want to take your privacy program to the next level, ISO 27701 includes standards and certification requirements. These guidelines map to GDPR, CDPA, Gramm-Leach-Bliley Act (GLBA), and HIPAA.

ISO 27701 is not a checklist, but a set of controls you can examine to help you decide how you'd like to implement these controls within your organization. PIMS addresses PII and how you use it within your organization.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact