KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

January 14, 2019

National Institute of Standards and Technology
Attn: Katie MacFarland
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Submitted to privacyframework@nist.gov

RE: *Developing a Privacy Framework*

Kaiser Permanente appreciates the opportunity to provide feedback on the *Developing a Privacy Framework.*

The Kaiser Permanente Medical Care Program is the largest private integrated healthcare delivery system in the U.S., with 12.2 million members in eight states and the District of Columbia.[1] Kaiser Permanente is committed to providing high-quality, affordable health care and improving the health of our members and the communities we serve.

General Comments

NIST solicits feedback about how organizations define the various challenges to implementing and maintaining strong privacy protections for the individuals they serve. We believe that health care poses unique considerations for developing a Framework that will ensure the right balance between the need for informed patient care with strong privacy protections.

As an integrated care delivery system with provider and health plan organizations, Kaiser Permanente is committed to protecting our members' health information. We recommend that NIST adopt a Privacy Framework (Framework) that embodies the following principles that address privacy as well as safe and effective health care:

Balance Privacy Protection with Quality Care Delivery*:* The Framework should seek to balance protecting patient privacy with delivering safe and high-quality care. The Framework should

[1] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., the nation's largest not-for-profit health plan, and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and over 650 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan to meet the health needs of Kaiser Permanente's members.

promote the development of laws and policies that enable health care organizations to achieve both goals simultaneously.

Harmonize Laws and Regulations: A robust Framework should endorse harmonizing federal, state, and local laws and regulations that protect the privacy and confidentiality of individually identifiable health information necessary to provide health services or related products and services.

Promote Innovation and Flexibility: A flexible Framework will promote regulations that avoid mandating specific standards, methodologies, technologies, and other prescriptive requirements that can only be changed via new laws or regulations. Flexibility supports innovation, best use of resources, cost effectiveness, and allows organizations to implement systems that best meet their needs.

Clear and Open Communications with Stakeholders*:* Confidentiality and trust are core values in the caregiving relationship. The Framework should recognize the need to clearly communicate how information is collected, used, shared and maintained, consistent with applicable laws and regulations.

We offer the following responses to NIST's questions.

Organizational Considerations

The greatest challenges in improving organizations' privacy protections for individuals

There is very little consistency in privacy requirements across sectors (health, banking, consumer services) and across jurisdictions within a sector (federal and state laws within the health sector, for example). This complexity makes it difficult for organizations to offer a basic set of consistent protections.

We strongly support a more universal, level playing field that provides entities and their consumers with consistent expectations and a minimum set of guarantees for information privacy.

The greatest challenges in developing a cross-sector standards- based framework for privacy

A broad-based Framework must navigate various challenges: conflicting, overlapping, and missing definitions; different personal identification/person matching; compliance with an array of federal/state laws and regulations; provenance when data source is critical information; varying consumer controls; entity security infrastructure differences. In addition, the same requirements do not apply to different types of entities across the information lifecycle/continuum within a single sector (e.g., under HIPAA, organizations defined as HIPAA covered entities follow a much stricter set of rules for use and disclosure of protected health information (PHI), while entities not defined in HIPAA have far greater discretion and less enforcement of policies regarding how they use and disclose the identical information).

There are no consistent privacy policies and practices across sectors. One challenge is how sensitive data are defined and handled by various industry sectors (e.g., banking data vs. health data; more sensitive health data vs. less sensitive health data). Sensitive data may or may not be defined in different laws. For example, substance use disorder data held by certain programs (defined under Federal regulations, 42 CFR Part 2, known as Part 2 data) is more strictly regulated and requires additional authorization for use and disclosure in a HIPAA context. The same data might not be subject to the same additional requirements if it exists outside a Part 2 program, so these inconsistencies further complicate the privacy landscape and may not provide the right benefit to consumers.

Finally, consumers may have different expectations, depending on various factors, like age and experience with technology. A robust Framework should be flexible enough to adjust to user risk tolerance and level of need.

How organizations define and assess risk generally, and privacy risk specifically

Generally, organizations use multiple risk assessment models in an enterprise risk management framework. The HIPAA Security Rule is a good example of a risk assessment model for data and systems security. Its broad approach encompasses ongoing monitoring and periodic performance of a comprehensive, structured, documented risk assessment across all information assets.

Within our organization, we have established a comprehensive internal infrastructure, with policies and procedures that encompass not only privacy risks and HIPAA compliance, but also information security oversight, data management, vendor risk assessment, regulatory implementation, cybersecurity, data governance and exception management.

The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management

Privacy risks are integral to our enterprise risk management framework, which incorporates both privacy and information security risk management. As we noted above, we maintain an organizational infrastructure to ensure broad-based privacy and security practices across our program.

Current policies and procedures for managing privacy risk; How senior management communicates and oversees policies and procedures for managing privacy risk; Formal processes within organizations to address privacy risks that suddenly increase in severity

As we describe above, we have established a risk management framework across all parts of our medical care program to protect the privacy and security of our members' information.

Kaiser Permanente's approach to detecting and managing heightened threats is built on a foundation of compliance with state and Federal laws and regulations; it also includes multifactorial threat surveillance and multi-layered defense. We have established privacy and security policies, procedures, and practices that reflect our strong commitment to manage risk effectively to protect our members' data, encompassing various systems that support nearly all aspects of care delivery, health plan operations, research, and population health. Internal training includes ongoing education and communication aimed at ensuring that our workforce understand the importance of protecting our members' privacy and the consequences of data breach.

The minimum set of attributes desired for the Privacy Framework, as described in the Privacy Framework Development and Attributes section of this RFI, and whether any attributes should be added, removed or clarified

Generally, we agree with the proposed minimum set of attributes for the Framework.[2] We recognize that these principles will have to be sufficiently adaptable, flexible, and scalable to allow organizations to achieve the right balance between protecting privacy and ensuring information is available when needed. As we note in our General Comments above, that balance is critical for safe and effective health care delivery, where inaccurate, incomplete, or inconsistent data can carry a significant risk to patient safety. Therefore, data protections should be strong but not so strong that they impede or prevent delivering care safely and effectively.

There may be barriers that impede or seriously restrict the use of data for legitimate research purposes; these burdens to advancing medical knowledge may provide little or no additional benefit to individuals.

What an outcome-based approach to privacy would look like

While an outcome-based approach is a reasonable concept, it will be important to get the policy right before any metrics are proposed or developed. Ensuring a risk-based approach to privacy is "baked in" from the beginning to help improve outcomes and reduce risk represents an ideal that may not be practical. For instance, the ability to monitor pre-defined outcomes and then adjust them after enough data are collected would require substantial changes to existing systems, plus financial investments.

NIST should carefully consider whether developing such an approach is achievable for various types of organizations. As a preliminary step, NIST could explore the feasibility of defining and measuring the functional, technical, and business capabilities needed to achieve a desired privacy outcome.

What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above

[2] The Framework should be: Consensus driven, developed and updated through open, transparent processes; Common and accessible language; Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses; Risk-based, outcome-based, voluntary, and non-prescriptive; Readily usable as part of any enterprise's broader risk management strategy or process; Compatible with or able to be paired with other privacy approaches; A living document.

As a covered entity under HIPAA, we comply with its Security Rule; as stated above, HIPAA requires a security risk-based analysis. We also find the following resources to be useful: NIST risk management framework; NIST information security resources; NIST cybersecurity framework; and the OCR HIPAA Security Risk Assessment (SRA) Tool.

An advantage of the HIPAA Security Rule is the flexibility that allows organizations to develop security systems that meet their needs, that supports existing infrastructures, and that considers the context for data privacy. That approach is preferable and more achievable than a framework that rests primarily on privacy by design.

How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;

Regulatory requirements and regulatory reporting requirements should provide consistency for the industry as well as for individuals. Currently, however, there exists a patchwork of inconsistent, duplicative, overlapping, and sometimes conflicting federal and state requirements that strain the resources of organizations obligated to comply.

Healthcare already is a heavily regulated industry with numerous, complex, sometimes contradictory state and federal reporting requirements that must be met. For the healthcare sector, these existing reporting requirements are prescriptive, with terms related to time span, volume and other elements. Regulations should not mandate specific standards, methodologies, technologies, etc. Overly prescriptive requirements that can only be changed via new laws and regulations will slow innovation and hamper flexibility. Functional requirements can be more adaptable.

When it comes to health care, in addition to adding costs, some regulations also can disrupt care delivery, clinical workflows, and potentially impact access to care if they require providers to implement and follow new processes and procedures. This can interfere with care delivery if not implemented without considering that context. For example, additional restrictions on certain substance use disorder data (through 42 CFR Part 2) can create barriers to treatment, care coordination, and case management without any gains for patients. Part 2 regulations can be further modernized to enable providers to fully benefit from advances in health information exchange.

Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices

As we stated in our last response above, we oppose requiring specific standards, methodologies, or technologies in statute, or regulation, or guidance having a regulatory effect. When “hardwired,” these requirements can stifle innovation, increase costs, strain resources, and reduce organizations’ ability to implement security systems that best meet their needs.

The role(s) national/international standards and organizations that develop national/international standards play or should play in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles

We strongly support the adoption and use of voluntary consensus standards accredited in an accepted framework such as that of the American National Standards Institute (ANSI), or meeting the same essential requirements. Standards Development Organizations (SDOs) play an important role in identifying the need for technical standards to address policy expectations, and in developing, testing, and publishing such standards for industry adoption. SDOs also play a key role in maintaining (including deprecating) existing standards, and in measuring/evaluating the degree to which standards are fulfilling the needs of the industry.

Structuring the Privacy Framework

Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information life cycle (i.e., the different stages—from collection to disposal—through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?

As we describe above, Kaiser Permanente has established a program-wide approach to implementing and ensuring robust privacy policies and practices. We manage privacy risk according to the very complex, numerous federal and state regulatory requirements that are mandated within the health care environment and govern how we access, use, and disclose data.

Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.

Many elements of the Framework can be applied to the development of a model Privacy Framework, including:

- Applying the overall structure of the Framework (Identify, Protect, Detect, Response, Recovery), but with different concepts more appropriate to the Privacy space, such as Rights, Choices, Controls, Context, Communication (communicating rights, choices, controls between organizations);
- Parsing the organization into functions, categories, and sub-categories;
- Providing standards, guidelines, and best practices;
- Establishing a Framework core, implementation tiers, and Framework profiles.

To encourage use and for ease of implementation, NIST should consider mapping the elements of the Framework to existing regulatory requirements. For the healthcare sector, this would involve a discussion of how Framework element relates to or supports elements of the HIPAA Privacy, Security, or Breach Notification Rules.

Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around:

- *The information life cycle*

    - Yes, we support that proposal.
- *Principles such as FIPPs*
    - A principles-based framework could be beneficial, but principles should be subject to broad multi-stakeholder processes before being used in this context. For example, current FTC FIPPs are at odds with the DHS FIPPs and OECD FIPPs, all of which are at odds with emerging US state legislation based on EU GDPR principles.
- *The NIST privacy engineering objectives of predictability, manageability, and disassociability or other objectives*
    - No. We believe this should be a second layer of privacy framework documentation, after defining the framework core, tiers and profiles.
- *Use cases or design patterns*
    - Both would be appropriate.
- *A construct similar to the Cybersecurity Framework functions, categories, and subcategories*
    - Yes, we support that proposal (See our comments, above).

Specific Privacy Practices
KP suggests referring to NIST SP 800-53 for organizations to select a standard baseline that is appropriate for an organization. Also, NIST seeks comment on the degree of adoption of the following practices regarding products and services:

De-identification
Adopting this practice would pose challenges, as there are different definitions of de-identification, and different practices for handling de-identified data. We recommend NIST provide additional clarification and guidance for various use cases, such as HIPAA de-identification.

Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared
In health care, covered entities subject to HIPAA must provide an explanation, via a Notice of Privacy Practices (NPP), about the permitted uses and disclosures of PHI for various purposes such as treatment, payment, and operations (TPO), research, etc. We recommend against requiring entities to provide granular level of information (metadata) about the what, when, why, how a particular data element was collected, stored, used or disclosed, which could be extremely burdensome, particularly for paper-based systems.

Enabling user preferences
This capability already exists to some extent in health care; however, this would be a challenge particularly in paper-based systems.

Setting default privacy configurations
This practice is currently adopted by the health care industry, consistent with regulatory requirements.

Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective

This practice has not been adopted or is being done only in a very limited way. We think this technology could be a valuable capability, depending of how easy it would be to implement in complex systems like health care.

Whether the practices listed above are widely used by organizations

Please see our comments above.

Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework

We suggest including:

- Identification, Authentication, Authorization, Access Controls, Audit
- Data provenance, Data segmentation

How the practices listed above or other proposed practices relate to existing international standards and best practices

NIST SP800-53 security controls embody a set of existing best practices that could be incorporated by reference. Additionally, national and international standards already exist for many of the areas of the Framework. For example, voluntary consensus standards for privacy and security used in health care are published by HL7; ISO; OASIS; and other SDOs.

Which of these practices you see as being the most critical for protecting individuals' privacy

We strongly believe that there are overarching commitments entities must make to ensure individual privacy protections. There must be a level of trust by individuals in the organization's ability to protect their information. We also strongly support the concept of a level playing field across all sectors that give both entities and consumers a minimum, consistent set of expectations about privacy of information.

Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization

- NIST Privacy Engineering Objectives
- Data segmentation
- Electronic, executable, standardized privacy controls

NIST must consider that these technologies all generate results (i.e., audit results, activity reports) that could require subsequent, and possibly labor-intensive manual action that in turn will present a whole separate set of challenges for organizations to find funding for these human resources.

Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence

Many of these practices are relevant for newer, emerging technologies.

How standards or guidelines are utilized by organizations in implementing these practices

Existing standards and guidelines are too inconsistent. For example, multiple privacy policy standards are required under HIPAA. However, these requirements only apply to entities subject to HIPAA. So, when it comes to personal health information, entities are not regulated the same way even when they receive, collect, maintain, use, and disclose the same individually identifiable information. Thus, the Framework must contain an approach that addresses these disparities.

*****

We appreciate your willingness to consider our comments.

Sincerely,

Jamie Ferguson	Lori Potter
Vice President	Senior Counsel
Health IT Strategy and Policy	Government Relations