

From: Lori P Potter <Lori.Potter@kp.org>  
Sent: Tuesday, October 22, 2019 1:18 PM  
To: privacyframework <privacyframework@nist.gov>  
Cc: Jamie Ferguson <Jamie.Ferguson@kp.org>; Walter G. Suarez <Walter.G.Suarez@kp.org>; Anne D Mcnealis <Anne.D.McNealis@kp.org>  
Subject: Kaiser Permanente comments on the Privacy Framework Preliminary Draft

Kaiser Permanente appreciates the opportunity to offer feedback on the NIST Privacy Framework preliminary draft. Our comment letter is attached.

Regards,

Lori Potter

Lori Potter

Senior Counsel

Government Relations

One Kaiser Plaza

Oakland, CA 94612

510-271-6621; tie-line 8-423-6621

510-3015644 (cell)

lori.potter@kp.org



Kaiser Foundation Health Plan  
Program Offices

October 24, 2019

National Institute of Standards and Technology (NIST)  
Attention: Katie MacFarland  
100 Bureau Drive, Stop 2000  
Gaithersburg, MD 20899

Submitted electronically to: [privacyframework@nist.gov](mailto:privacyframework@nist.gov)

RE: *NIST Privacy Framework: Preliminary Draft*

Dear Ms. MacFarland:

Kaiser Permanente appreciates the opportunity to offer the following comments on the NIST Privacy Framework preliminary draft (Framework) published in the Federal Register on September 9, 2019.<sup>1</sup>

The Kaiser Permanente Medical Care Program is the largest private integrated healthcare delivery system in the U.S., with 12.3 million members in eight states and the District of Columbia.<sup>2</sup> As part of its mission, Kaiser Permanente has implemented a secure Electronic Health Record (EHR) system, KP HealthConnect® to support the delivery of healthcare services to our members and to enhance communications among providers.

NIST solicits feedback on the draft Framework, before issuing an updated version of the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. This draft is aligned, both structurally and conceptually, with the previously published *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), April 16, 2018).

### **General Comments**

As an integrated care delivery system with provider and health plan organizations, Kaiser Permanente is committed to protecting our members' health information, and welcomes this additional opportunity to provide input to an important area of NIST responsibility. We

---

<sup>1</sup> 84 FR 47255

<sup>2</sup> 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.

previously provided comments and recommendations in response to the November 2018 request for information (RFI) on *Developing a Privacy Framework*, and the April 2019 NIST Privacy Framework *Discussion Draft*.

Overall, the preliminary draft Framework provides a good set of guiding principles and structural elements to help organizations build a solid privacy foundation, and to align privacy risks with broader enterprise risks within an organization.

### **Purpose, Objectives and Scope for the Privacy Framework**

NIST should clearly state the purpose and rationale for the Framework. The Executive Summary and the Introductory sections should explain why it is critical to drive better privacy engineering and help organizations protect individuals' privacy. Similarly, the Framework should describe the scope of the document.

**We recommend the next version of the Framework include a section devoted to purpose, objectives and scope** that discusses how and why a privacy framework can help organizations manage privacy risks, why it will be useful to a wide range of organizations of all sizes, and why it should remain agnostic to any particular technology, sector, law, or jurisdiction.

### **Privacy Framework Structure and Privacy Risk Management**

We applaud NIST's efforts to organize the overall Framework into a model comprising three major components (*Core* – activities and outcomes; *Profiles* – functions, categories and subcategories; and *Implementation Tiers* – processes and resources) and for choosing to focus the draft Framework around Privacy Risk Management. The simplicity of the model allows the draft Framework to define processes and outcomes that support an enterprise's mission and business objectives, cover many existing practices, assist in strengthening individual privacy protections, enable organization use, and facilitate compliance with applicable laws and regulations.

The model also allows organizations to better integrate privacy risks with other business and operational risks within the organization. However, we recommend NIST expand two sections in the next version of the document. Specifically, NIST should include a definition of privacy risk management in the overview and add a discussion of why it is important and how it relates to other risk areas of an organization. Section 1.2 contains a very brief overview of privacy risk management. Given how significant and central this is to the framework, it is important for NIST to expand on this section.

NIST should also consider modifying Section 1.2.1 to focus on Information Security risks and its relationship to Privacy risks, and not limit the discussion to cybersecurity risks (a component of information security). By focusing only on cybersecurity risks, the framework leaves out several other information security components (administrative, physical, technical) that directly relate to, and impact privacy risks. The graph used in this section (venn diagram) that correlates cybersecurity risks with privacy risks should be replaced with a diagram that correlates information security risks with privacy risks.

To be relevant in the context of organizations' respective sectors of the economy, the Framework would benefit from documenting examples of the use of the framework in selected industry sectors – and provide these examples as supplemental materials – to illustrate how components of the Framework (Core, Profiles, Implementation Tiers), and the foundational focus on privacy risk management, apply, in a practical way, to specific sectors. NIST should include the health and health care sector in this supplemental analysis because of its significant legislative, regulatory, and operational privacy achievements over the past twenty (20) years. Creating a cross-reference to national policies, such as HIPAA privacy and security rules, will be a critical component of such an analysis. As a general approach, the draft Framework includes, and does not diverge from, existing privacy policies and practices in the health/health care sector.

Due to its flexible nature, the draft Framework can be integrated into existing requirements and practices. NIST has achieved the intended outcomes related to privacy risk integration, privacy risk management guidance, relationship definition between privacy and cybersecurity risk (however we recommend expanding this relationship to information security), various stakeholder roles' understanding of privacy risks and mitigations, scalable guidance, and a cost-effective implementation.

It is too early to assess whether the proposed Framework would improve the ability of organizations to adapt to and address privacy risks arising from emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), or Internet of Things devices (IOT). These concepts and technologies are still evolving and not yet widely adopted and implemented. Moreover, a broader legal and regulatory framework for the adoption and use of such innovations does not yet exist.

### **Core, Profiles and Implementation Tiers of the Privacy Framework**

The *Core*, which comprises Functions, Categories, and Sub-Categories, provides a set of activities and outcomes that enable an organizational dialogue about managing privacy risk.

We agree with the five identified Functions, (Identity, Govern, Control and Communicate to manage privacy risks associated with data processing; and Protect, to manage the privacy risks associated with privacy breaches). However, we strongly recommend including three additional functions related to managing privacy breaches – and that would align with Protect. They are: 1) Detect; 2) Respond; and 3) Recover. These are key functions that organizations need to consider when addressing privacy breaches. While they have been incorporated into the Cybersecurity Framework, they are also an integral part of the Privacy Framework.

We are concerned that the *Core* sub-categories in the draft Framework would have the effect of system controls with potentially excessive prescriptive authority built into the design. Organizations should be able to determine the relative risks and assign values to each of the elements independently, consistent with the overall structure.

The draft Framework defines *Profiles* as the representation of privacy outcomes that an organization aims to achieve. In health care, this outcomes-based approach for designing Core

elements is not compatible with the process-based regulatory and compliance regimes enforced by federal, state, and local laws and regulations. The resulting incompatibility will lead to disparate results in scoring and reporting on specific elements and for aggregating items.

### **Sectoral Concerns**

As we previously commented in the Discussion Draft from April 2019, sectoral considerations are critical to the development of the Framework, even as they will complicate its broad application and implementation. Privacy in the health care sector requires balancing multiple interests; moreover, it is governed by multiple, often overlapping state and federal laws and regulations, including but not limited to the HIPAA Privacy Rule. To assist in applying the Framework in our sector, we offer the following principles that seek to address individual privacy, as well as the delivery of safe and effective health care:

- **Enable Privacy Protection and Quality Care Delivery:** The Framework should enable health care entities to protect patient privacy while also delivering safe and high-quality care. The Framework should promote laws and policies that enable health care organizations to achieve both goals simultaneously. The federal HIPAA Privacy and Security Rules, as well as state laws and regulations, already require providers and certain other entities to protect the privacy and security of individually identifiable health information. At the same time, delivering safe and high-quality health care necessarily uses personal information.
- **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 do not mandate specific standards, methodologies, technologies, or other prescriptive requirements that can only be updated or 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. Implementations of the Framework should incorporate and reference the health sector notice requirements as well as the remedies available to stakeholders under applicable laws and regulations.

### **Specific Comments in Response to the Draft Privacy Framework and Appendices**

As requested in the NIST Notice, we have organized our specific comments and recommendations in response to the draft Framework sections utilizing the comment template made available by NIST (attached).

## **Conclusion**

Kaiser Permanente looks forward to working with NIST on the draft Framework. We appreciate your consideration of our comments. Please feel free to contact me ( [jamie.ferguson@kp.org](mailto:jamie.ferguson@kp.org); 510.271.5639) or Lori Potter ([lori.potter@kp.org](mailto:lori.potter@kp.org); 510-271-6621) if you need additional information.

Sincerely,

A handwritten signature in black ink that reads "JA Ferguson". The signature is written in a cursive, slightly slanted style.

Jamie Ferguson  
Vice President, Health IT Strategy and Policy  
Kaiser Foundation Health Plan, Inc.

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	4	119	NA	As noted in our general comment letter, overall, the preliminary draft Framework provides a good set of guiding principles and structural elements to help organizations build a solid privacy foundation, and to align privacy risks with broader enterprise risks within an organization. However, the next version of the Framework should include a section devoted to purpose, objectives and scope.	<p>NIST should clearly state the purpose and rationale for the Framework. The Executive Summary and the Introductory sections should explain why it is critical to drive better privacy engineering and help organizations protect individuals' privacy. Similarly, the Framework should describe the scope of the document.</p> <p>We recommend the next version of the Framework include a section devoted to purpose, objectives and scope that discusses how and why a privacy framework can help organizations manage privacy risks, why it will be useful to a wide range of organizations of all sizes, and why it should remain agnostic to any particular technology, sector, law, or jurisdiction.</p>	General/Editorial

2	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	5	153	1.1	We applaud NIST's efforts to organize the overall Framework into a model comprising three major components (Core – activities and outcomes; Profiles – functions, categories and subcategories; and Implementation Tiers – processes and resources) and for choosing to focus the draft Framework around Privacy Risk Management. The simplicity of the model allows the draft Framework to define processes and outcomes that support an enterprise's mission and business objectives, cover many existing practices, assist in strengthening individual privacy protections, enable organization use, and facilitate compliance with applicable laws and regulations.	NA	General
3	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	6	196	1.2	While the model also allows organizations to better integrate privacy risks with other business and operational risks within the organization, as noted in our general comment letter, we recommend NIST expand two sections (1.2 and 1.2.1) in the next version of the document.	NIST should include a definition of privacy risk management in the overview and add a discussion of why it is important and how it relates to other risk areas of an organization. Section 1.2 contains a very brief overview of privacy risk management. Given how significant and central this is to the framework, it is important for NIST to expand on this section.	Editorial



4	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	6	202	1.2.1	While the model also allows organizations to better integrate privacy risks with other business and operational risks within the organization, as noted in our general comment letter, we recommend NIST expand two sections (1.2 and 1.2.1) in the next version of the document.	NIST should also consider modifying Section 1.2.1 to focus on Information Security risks and its relationship to Privacy risks, and not limit the discussion to cybersecurity risks (a component of information security). By focusing only on cybersecurity risks, the framework leaves out several other information security components (administrative, physical, technical) that directly relate to, and impact privacy risks. The graph used in this section (venn diagram) that correlates cybersecurity risks with privacy risks should be replaced with a diagram that correlates information security risks with privacy risks.	Editorial
---	-------------------	-----------------------------------------	---	-----	-------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

5	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	248	1.2.1	Immediately after subsection 1.2.1 and before the current next subsection (1.2.2 Relationship between Privacy Risk Management and Risk Assessment), we recommend NIST add a new section: "1.2.2 Relationship Between Privacy Risk and Other Business Risks," and discuss in it HOW other risks in the organization interact with privacy risks, the importance of an integrated, comprehensive risk management strategy that includes privacy risks along with other risks, and provide examples of the interactions between various risks within an organization.	Add new subsection 1.2.2 Relationship Between Privacy Risk and Other Business Risks. In this subsection, discuss HOW other risks in the organization interact with privacy risks, the importance of an integrated, comprehensive risk management strategy that includes privacy risks along with other risks, and provide examples of the interactions between various risks within an organization.	Editorial
6	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	239	1.2.1	Call out for "problematic data action"	Expand on "problematic data action" in a text box on page 7.	Editorial
7	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	248	1.2.2	The explanation on the relationship between these two concepts, Privacy Risk Management and Risk Assessment, needs more substance and examples.	Provide more substance and examples on the relationship between these two concepts (Privacy Risk Management and Risk Assessment) in this subsection 1.2.2.	General

8	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	249	1.2.2	"Privacy risk management is a cross-organizational set of processes that helps organizations to understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks. Privacy risk assessment is a sub-process for identifying, evaluating, prioritizing, and responding to specific privacy risks."	Include a subset of this statement in a text box to emphasize: "Privacy risk assessments can help an organization understand in a given context the values to protect, the methods to employ, and the way to balance implementation of different types of measures."	Editorial
9	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	278	1.2.2	"Privacy risk assessments help organizations distinguish between privacy risk and compliance risk" - these are not always mutually exclusive.	NA	General

10	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	284	1.2.2	<p>As stated in our general comment letter, to be relevant in the context of organizations' respective sectors of the economy, the Framework would benefit from documenting examples of the use of the framework in selected industry sectors – and provide these examples as supplemental materials – to illustrate how components of the Framework (Core, Profiles, Implementation Tiers), and the foundational focus on privacy risk management, apply, in a practical way, to specific sectors. NIST should include the health and health care sector in this supplemental analysis because of its significant legislative, regulatory, and operational privacy achievements over the past twenty (20) years. Creating a cross-reference to national policies, such as HIPAA privacy and security rules, will be a critical component of such an analysis. As a general approach, the draft Framework includes, and does not diverge from, existing privacy policies and practices in the health/health care sector.</p>	<p>The Framework would benefit from documenting examples of the use of the framework in selected industry sectors - and provide these examples as supplemental materials - to illustrate how components of the Framework (Core, Profiles, Implementation Tiers), and the foundational focus on privacy risk management, apply, in a practical way, to specific sectors. NIST should include the health and health care sector in this supplemental analysis and create a cross-reference to national policies such as HIPAA privacy and security rules.</p>	General/Editorial
----	-------------------	-----------------------------------------	---	-----	-------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------

11	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	284	1.2.2	As stated in our general comment letter, due to its flexible nature, the draft Framework can be integrated into existing requirements and practices. NIST has achieved the intended outcomes related to privacy risk integration, privacy risk management guidance, relationship definition between privacy and cybersecurity risk (however we recommend expanding this relationship to information security), various stakeholder roles' understanding of privacy risks and mitigations, scalable guidance, and a cost-effective implementation.	We recommend expanding this relationship to information security.	General/Editorial
12	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	7	284	1.2.2	As noted in our general comment letter, it is too early to assess whether the proposed Framework would improve the ability of organizations to adapt to and address privacy risks arising from emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), or Internet of Things devices (IOT). These concepts and technologies are still evolving and not yet widely adopted and implemented. Moreover, a broader legal and regulatory framework for the adoption and use of such innovations does not yet exist.	NA	General

13	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	9	312	2.1	Modification of Figure 4	Consider modifying Figure 4 to show the grouping of Identity-P, Govern-P, Control-P and Communicate-P as managing privacy risks associated with processing, and Protect-P as managing the privacy risks associated with privacy breaches.	Technical
14	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	9	313	2.1	Emphasis	Emphasize the distinction and interaction between Control-P and Protect-P (i.e., Control-P is more of the administrative safeguards and Protect-P is more of the technical safeguards.)	Technical

15	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	9	314	2.1	As noted in our general comment letter, we agree with the five identified Functions, (Identity, Govern, Control and Communicate to manage privacy risks associated with data processing; and Protect, to manage the privacy risks associated with privacy breaches). However, we strongly recommend including three additional functions related to managing privacy breaches – and that would align with Protect. They are: 1) Detect; 2) Respond; and 3) Recover. These are key functions that organizations need to consider when addressing privacy breaches. While they have been incorporated into the Cybersecurity Framework, they are also an integral part of the Privacy Framework.	We strongly recommend including three additional functions related to managing privacy breaches – and that would align with Protect. They are: 1) Detect; 2) Respond; and 3) Recover. These are key functions that organizations need to consider when addressing privacy breaches. While they have been incorporated into the Cybersecurity Framework, they are also an integral part of the Privacy Framework.	Editorial/Technical
16	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	9	335	2.1	Core Functions - add additional three as referenced above.	As recommended above, NIST should consider adding three additional Functions here: 1) Detect-P; 2) Respond-P; and 3) Recover-P as these three additional functions deal with what happens with respect to privacy risk management AFTER there is a privacy incident.	Editorial/Technical

17	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	9	335	2.1	As stated in our general comment letter, we are concerned that the Core sub-categories in the draft Framework would have the effect of system controls with potentially excessive prescriptive authority built into the design. Organizations should be able to determine the relative risks and assign values to each of the elements independently, consistent with the overall structure.	NA	General
18	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	9	335	2.1	As stated in our general comment letter, the draft Framework defines Profiles as the representation of privacy outcomes that an organization aims to achieve. In health care, this outcomes-based approach for designing Core elements is not compatible with the process-based regulatory and compliance regimes enforced by federal, state, and local laws and regulations. The resulting incompatibility will lead to disparate results in scoring and reporting on specific elements and for aggregating items.	NA	General
19	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	10	356	2.1	Control-P emphasis	Emphasize the distinction and interaction between Control-P and Protect-P (i.e., Control-P is more of the administrative safeguards and Protect-P is more of the technical safeguards.)	Technical



20	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	10	368	2.1	Protect-P emphasis	Emphasize the distinction and interaction between Control-P and Protect-P (i.e., Control-P is more of the administrative safeguards and Protect-P is more of the technical safeguards.)	Technical
21	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	10	373	2.2	Earlier in the document NIST states that an organization should develop a current profile and a target profile to identify needed improvements. The first step would be to inquire, to what would a profile be applied? Smaller entities without subsidiaries or regional operational differences or regional systems or state laws could, conceivably, choose to apply its selected profile against the entire organization's privacy activities, but throw in any other element and it becomes a bit more challenging.	Provide examples of a small, medium and large entity and application of the profile.	Editorial
22	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	10	373	2.2	If systems/solutions are conducting the "data processing" is the profile to be applied by individual systems? This appears to be a conceivable approach as the Framework calls out the SDLC process and integration of the profile into it.	NA	General/Editorial

23	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	10	373	2.2	Profiles will be important components to help address actions that need to be taken, from a privacy risk management standpoint, after a privacy incident has occurred.	Consistent with the recommendations above regarding the need to add three new Functions (Detect-P, Respond-P, Recover-P), similarly here there should be Profiles added to address these three new Functions.	Editorial/Technical
24	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	10	373	2.2	The draft Framework defines Profiles as the representation of privacy outcomes that an organization aims to achieve. In health care, this outcomes-based approach for designing Core elements is not compatible with the process-based regulatory and compliance regimes enforced by federal, state, and local laws and regulations. The resulting incompatibility will lead to disparate results in scoring and reporting on specific elements and for aggregating items.	NA	General
25	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	11	397	2.3	While the four Tiers seem reasonable, they are simply listed in the document with little information about them.	It will be valuable to have a brief description of each of the four proposed Tiers - similar to the descriptions of the proposed Functions in the earlier sections.	General/Editorial

26	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	12	414	3.0	<p>As stated in our general comment letter, to be relevant in the context of organizations' respective sectors of the economy, the Framework would benefit from documenting examples of the use of the framework in selected industry sectors – and provide these examples as supplemental materials – to illustrate how components of the Framework (Core, Profiles, Implementation Tiers), and the foundational focus on privacy risk management, apply, in a practical way, to specific sectors. NIST should include the health and health care sector in this supplemental analysis because of its significant legislative, regulatory, and operational privacy achievements over the past twenty (20) years. Creating a cross-reference to national policies, such as HIPAA privacy and security rules, will be a critical component of such an analysis. As a general approach, the draft Framework includes, and does not diverge from, existing privacy policies and practices in the health/health care sector.</p>	<p>The Framework would benefit from documenting examples of the use of the framework in selected industry sectors - and provide these examples as supplemental materials - to illustrate how components of the Framework (Core, Profiles, Implementation Tiers), and the foundational focus on privacy risk management, apply, in a practical way, to specific sectors. NIST should include the health and health care sector in this supplemental analysis and create a cross-reference to national policies such as HIPAA privacy and security rules.</p>	General/Editorial
----	-------------------	-----------------------------------------	----	-----	-----	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------

27	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	12	437	3.1	Mapping to industry-specific national privacy "frameworks," such as HIPAA (for health care) will be particularly helpful in this section, as a way of contextualizing the applicability of the framework to specific industry sectors.	Include mapping to existing industry-specific national "frameworks," legal and regulatory requirements, standards, etc. Consider adding a text box to emphasize the adoption (or development, as applicable) of consensus-based standards, guidelines, and practices.	General/Editorial
28	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	13	470	3.2	One element missing from Figure 6 and the entire discussion on Strengthening Accountability is the depiction of the external drivers/forces affecting the internal elements in the iterative cycle being described. Highlighting these external forces, including national and jurisdictional laws and regulations, as well as new consumer expectations, will be beneficial in this section.	Add a discussion highlighting external forces, including national and jurisdictional laws and regulations, as well as consumer expectations.	General/Editorial
29	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	14	475	3.3	The "ready, set, go" model seems a bit simplistic for a national privacy framework. Most organizations have more complex processes that are difficult to fit into a "ready, set, go" conceptualization. While the simplicity of the model has some appeal, components are missing for what happens before the "ready" and after the "go" (e.g., evaluation, feedback, remediation.)	Consider adding components to address what happens before the "ready" and after the "go" (evaluation/feedback/remediation).	General/Editorial

30	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	15	525	3.4	We appreciate NIST including this section dealing with the relationship between the Privacy Framework and the SDLC.	NA	General
31	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	17	596	3.6	This section should not be limited to "buying" decisions, but to all externally contracted services. Profiles could be standardized across business agreements of many kinds.	The 3.6 section header and both paragraphs - language needs to be changed to "buying and any other externally contracted service" in all instances.	Editorial
32	Kaiser Permanente	Jamie Ferguson Jamie.Ferguson@KP.org	18	611	Appendix A	Appendix A covers topics around implementation, scalability, alignment, and roles. It does not cover the topic of "flexibility" and how the model can be flexible so as to allow organizations to contextualize it within their respective sectors. For example, "Table 1 - Privacy Framework Function and Category Unique Identifiers," which provides a very detailed and complete set of Functions, Categories and Sub-Categories, should allow organizations to at least add industry-specific categories and sub-categories, if not additional functions.	Include the topic of "flexibility" and how the model can be flexed for organizations to contextualize, including allowing organizations to add industry-specific categories, sub-categories, and additional functions. Additionally, as stated in other section comments, NIST can greatly add value if it would develop and document examples of how to apply the Framework to industry-specific sectors (such as health care). Those use cases can be provided as Supplemental information in additional appendices to the Framework document.	General/Editorial