America's Health Insurance Plans
601 Pennsylvania Avenue, NW
South Building, Suite Five Hundred
Washington, DC 20004

AHIP

October 23, 2019

Submitted Via Electronic Mail to: privacyframework@nist.gov

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive
Stop 200
Gaithersburg, MD 20899

RE: NIST Privacy Framework: Preliminary Draft Comments

Dear Ms. MacFarland:

America's Health Insurance Plans (AHIP) appreciates the opportunity to respond to the National Institute of Standards and Technology (NIST) proposed Privacy Framework as published in the *Federal Register* on September 9, 2019.[1] AHIP is the national association whose members provide coverage for health care and related services to millions of Americans every day. Through these offerings, we improve and protect the health and financial security of consumers, families, businesses, communities, and the nation. We are committed to market-based solutions and public-private partnerships that improve affordability, value, access, and well-being for consumers.

AHIP supports the agency's approach of developing the Framework in collaboration with public and private stakeholders. As a preliminary matter, we believe the Framework will help improve privacy practices across all sectors of U.S. entities, particularly those entities that do not have baseline privacy practices. In the health sector, however, we have been highly regulated and have been embedding privacy and security protocols in our business systems, operations, policies, practices, training and other practices to protect consumers' health information. As a result, we believe that the health sector can help serve as an example of successful practices for protecting information privacy and security.

[1] 84 Fed. Reg. 47255. The Preliminary Draft and related resources were available on the NIST website at: https://www.nist.gov/privacy-framework/working-drafts.

The NIST Privacy Framework Must Be Voluntary for HIPAA-Covered and Similarly Situated Entities

Because health entities are governed by federal laws and regulations[2] and a multitude of state legal requirements, we endorse the Privacy Framework as a voluntary tool that can further assist entities with identifying, assessing, managing, and communicating privacy risks to foster the development of innovative approaches to protecting individuals' privacy.

Health entities, in particular, need the flexibility to utilize the NIST Privacy Framework to complement their robust privacy and security programs and processes that have been in place for many years, with the understanding that refinements and improvements can always be made to keep pace with industry practices and to avert developing threats. In this regard, we encourage NIST to recognize that the health care sector, unlike other segments of the U.S. economy, is heavily regulated and the Privacy Framework is not intended for our sector, nor should it be utilized as a new layer of mandated and duplicative requirements.

We note that there are some private entities and public organizations that may access, use, transmit or disclose health information without having to comply with federal or state privacy laws. We continue to encourage NIST and other agencies to help identify gaps for protecting consumers' health data, and to work with the Administration and Congress to help promote better privacy protections of consumers' health information by these non-HIPAA entities.

The NIST Privacy Framework Will Work in Tandem with the Cybersecurity Framework

Managing privacy risks through a prioritized, flexible, outcome-based, and cost-effective approach that is compatible with existing legal and regulatory compliance requirements is a solid approach for the Privacy Framework. The NIST Framework for Improving Critical Infrastructure Cybersecurity (referred to as the "Cybersecurity Framework) has been successfully utilized in this manner. Health care entities look to the Cybersecurity Framework as a tool for building solid protections that are multi-layered legal and non-legal practices and solutions based on an entity's own administrative, physical and technical resources, operating environment, and perceived risks that are balanced against the costs and benefits of implementing protections. That model has

[2] Federal laws include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Electronic and Clinical Health Act, Gramm-Leach-Bliley Act (GLBA), the Genetic Information Nondiscrimination Act, and the Confidentiality of Substance Use Disorder Patient Records (commonly referred to as the "Part 2" requirements).

enabled entities to make assessments and decisions, and has been widely-adopted because of flexibility to be customized to achieve success.

Cybersecurity risks are part of the universe of privacy and security risks that entities face. Both NIST Models will work in tandem as complimentary guidance for protecting against some common threats, as noted in the released draft.

Specific Comments in Response to the Draft Privacy Framework and Appendices

As requested in the NIST Notice, we have organized our specific comments in response to the Privacy framework utilizing the comment template that was made available for public use. Our specific comments relating to specific provisions and recommendations are attached in the NIST template.

We thank you for the opportunity to provide comments on these important issues. We stand ready to continue our dialog and to help shape this important work. If you have any questions about our comments, please contact Marilyn Zigmund Luke at mzluke@ahip.org.

Sincerely,

Marilyn Zigmund Luke
Vice President

Commen+G1A+A1:I1	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	N/A	N/A	N/A	There are some private entities and public organizations that may access, use, transmit or disclose health information without having to comply with laws such as HIPAA and the HITECH Act. Some entities and consumers may not appreciate when health information is - and is not - covered by federal and state laws.	We continue to advocate for NIST and other agencies to help identify gaps for protecting consumers' health data, and to address these gaps, where possible, in the NIST privacy framework, as well as in public forums and educational events.	General
2	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	N/A	N/A	N/A	The Privacy Framework should incorporate information on how current and cutting-edge technologies (e.g., mobile devices, social media, the Internet of Things (IoT), and artificial intelligence) can help promote consistency and technical capabilities for protecting individuals' privacy within the healthcare and non-healthcare sectors, as well as with public agencies.	NIST should consider adding a specific discussion section to the draft. In the alternative, future work can address these concepts and how they apply to the Privacy Framework.	General
3	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	20-22, etc.			We understand that NIST intends to apply the definition of "data processing" very broadly. This term can have a different meaning to different entities and may be based on the transaction or event as it is occurring.	NIST should add more descriptive text to clarify this term.	Editorial
4	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	6	175	1.1	More clarity is needed for the definitions of "data processing" and "data management."	NIST should consider a separate definition for "data management" and "data processing." For example, the term data management can be interpreted broadly as the data can be available in many places and formats. Data "at rest" and data that are moving can have different privacy and security protections. A definition of "data processing" is provided in the Appendix, as adopted from NIST IR 8062 [5]. Perhaps a corresponding definition can be listed for "data managment."	General
5	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	N/A	N/A	N/A	NIST should consider including cross-references to existing documents and standards that will associate NIST Privacy Framework with other framework programs such as ISO, COBIT, HITRUST, and other accepted industry standards.	In future public forums and discussions, NIST should solicit and receive feedback on how these standards could be incorporated into future revisions of the Privacy Framework.	Technical and Editorial
6	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	N/A	N/A	N/A	The NIST Cybersecurity framework was built on NIST guidance documents that had been developed, vetted, and made final over many years. The Privacy Framework is recognized by NIST as new and unlike the process that was used for the Cybersecurity Framework.	NIST should further explain how the Privacy framework will be solidified in practice and what future products, if any, NIST has in concept or developement.	General
7	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	22-24	N/A	ID.RA-P, GV.MT-P1	More information is needed related to how an organization would quantify assigning values to problematic data actions. Likewise, it is unclear how such values interact with or impact the elements (i.e., would an entity have discretion to prioritize priorities and relevant matters to the organization based on past experiences, current known practicies and risks, and future/developing threats?).	NIST should clarify these sections.	Technical
8	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	4	145	101	The framework is silent with respect to established global privacy frameworks, such as the Organisation for Economic Co-operation and Development (OEDC), the European Convention on Human Rights, the European Union Charter on Fundamental Rights, and other potentially applicable requirments that can apply in global operations. NIST may seek to explain how U.S. privacy standards can be aligned with global standards.	Understanding that the framework is agnostic to specific laws, NIST may consider referencing global privacy frameworks in the introduction. If the Privacy framework is intended for U.S.-specific use, then NIST may want to include a clarification in the introduction.	General
9	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	12	405	2.3	Please advise of the rationale for why organizations should try and achieve Tier 2. It is unclear why this is the preferred level to achieve.	NIST could provide an example to assist the reader better understand why and how Tier 2 should be achieved by organizations.	General

10	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	6	202	1.2.1	NIST should expand two sections (1.2 and 1.2.1) in the next version of the document.	While the model also allows organizations to better integrate privacy risks with other business and operational risks within the organization, more clarification would be helpful. For example, 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 beyond cybersecurity. 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 or supplemented with a diagram that correlates information security risks with privacy risks.	Editorial
11	AHIP	Marilyn Zigmund Luke mzluke@ahip.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.	NIST should add a new subsection, "Relationship Between Privacy Risk and Other Business Risks." This discussion could include 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
12	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	7	284	1.2.2	It is premature 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.	NIST should discuss this comment and application in future versions of the Framework.	General
13	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	9	312	2.1	Modification of Figure 4	NIST should 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	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	9	314	2.1	Key functions that organizations need to consider when addressing privacy breaches should be added.	We recommend including three additional functions related to managing privacy breaches: 1) Detect; 2) Respond; and 3) Recover.	Editorial/Technical
15	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	9	335	2.1	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.	NIST should modify future versions of the Framework to address the comment.	General
16	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	9	335	2.1	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.	NIST should evaluate how to alleviate dispatities in scoring and reporting as different sectors have different legal requirements.	General and Editorial

17	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	10	373	2.2	The Framework outlines that an organization should develop a current profile and a target profile to identify needed improvements. However, smaller entities without subsidiaries or regional operational differences or regional systems or state laws could have difficulty applying a selected profile against the entire organization's privacy activities.	Future versions of the Framework should provide examples of a small, medium and large entity application of the profile.	Editorial
18	AHIP	Marilyn Zigmund Luke mzluke@ahip.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 there should be Profiles added to address these three new Functions.	Editorial/Technical
19	AHIP	Marilyn Zigmund Luke mzluke@ahip.org	11	397	2.3	The four Tiers need more detail and clarification.	NIST should expand a description of each of the four proposed Tiers, similar to the descriptions of the proposed Functions in the earlier sections.	Editorial/Technical
20	AHIP	Marilyn Zigmund Luke mzluke@ahip.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 would benefit from clarifying language for "buying and any other externally contracted services."	Editorial
21	AHIP	Marilyn Zigmund Luke mzluke@ahip.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.	NIST should include the topic of ""flexibility"" and how the model can be used by organizations to add industry-specific categories, sub-categories, and additional functions. Additionally, industry-specific examples or "use cases" may be added as Supplemental information in additional appendices to the Framework document.	General/Editorial