January 14, 2019

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Submitted Via Electronic Mail at privacyframework@nist.gov

Re: Developing a Privacy Framework / Docket Number 181101997–8997–01

Dear Ms. MacFarland:

We appreciate the opportunity to comment in response to the National Institute of Standards and Technology's (NIST's) Request for Information for developing a Privacy Framework. The notice was published in the *Federal Register* on November 14, 2018 (83 Fed. Reg. 56824).

America's Health Insurance Plans (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.

We fully support NIST's Privacy Framework initiative and we believe that a "forward-thinking" approach will support consumer protections, business innovations and alignment of policy, technological, and legal approaches to data collection, storage, use, and sharing. Our members have relied upon the companion NIST Framework for Cybersecurity and the Privacy Framework may serve as a similar model for both public agencies and private entities.

AHIP appreciates the collaborative and transparent processes that NIST has implemented in developing industry guidance and we plan to engage along with other stakeholders as the Privacy Framework is developed. We appreciate NIST's leadership role by setting the example for guidance developed through a consensus-driven and open, transparent process. We recognize NIST's collaboration of soliciting public comments and holding events. We stand ready to continue our dialog and to help shape this important work.

Promoting Consumers' Trust
AHIP supports public and private efforts that promote consumers' trust. Health insurance providers are committed to respecting consumers' interests, helping them understand what is

happening with personal data, and working with their providers and caretakers to make health care decisions. Our members have been at the forefront of designing business structures to protect the privacy and security of health data. We have also kept pace with global privacy requirements and new business trends to further strengthen and refine policies and processes.

We agree that technologies and processes should consider diverse privacy needs in an increasingly connected and complex environment. AHIP members are accustomed to protecting the privacy and security of consumers' data. The Privacy Framework should incorporate information on how current and cutting-edge technologies (e.g., mobile devices, social media, the Internet of Things, 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.

Evaluating Existing Legal Requirements and Consumers' Needs
Protecting consumers' privacy in the healthcare sector is a complex process. State and Federal laws and regulations govern business policies and decisions, and in many cases a thorough legal analysis must be completed by entities when implementing any new privacy system or process.

Within the healthcare sector, laws such as the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, and the Gramm-Leach-Bliley Act have served as a solid foundation for privacy and security requirements. Under implementation of these and other laws, privacy implementation is based on legal compliance requirements and outcomes rather than a flexible framework. Our preference is for a customizable framework based on risk assessments that can evolve based on industry trends and consumer needs. Our members' extensive experiences have demonstrated that while privacy and security requirements are complementary and co-dependent, protecting privacy is a unique objective because it requires administrative, technical, and physical components that are largely influenced by the people and processes that structure their environments.

Despite the stacked layers of regulations with which healthcare entities comply, 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. 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.

Using a Risk-based Approach
Protecting information privacy is vitally important when evaluating risk areas and ways to protect data. Risk-based flexibility is a critical component that should be part of any future Privacy Framework. Organizations are in the best positions to design their information technology systems and business processes to promote consumers' needs and privacy

expectations. As stated above, NIST can best work with private organizations by promoting a voluntary framework.

We support the proposed goal of developing a framework that includes and identifies common practices across contexts and environments and is structured to help organizations achieve positive privacy outcomes. Referring to the HIPAA Privacy Rule can help identify key elements for future work. We note, however, that the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) recently issued a Request for Information in the *Federal Register* to improve care coordination.[1] The Privacy Framework should be flexible to allow for regulatory changes. In addition, NIST should work in tandem with OCR to stay current with emerging public policies and regulatory requirements.

Organizational Considerations
Public and private entities have similar goals of protecting privacy and yet different objectives have been implemented to meet consumer privacy expectations and legal requirements. Often legal requirements serve as a baseline. Contractual requirements, information system abilities and limitations, site locations, operating environments, leadership decisions, corporate culture, and past compliance challenges can all provide a rationale for developing new and complex privacy practices in a business setting.

When developing a Privacy Framework, NIST should ensure proactive methods through voluntary, outcome-based, non-prescriptive structures that assess risk and allow entities to customize a Privacy Framework based on consumer needs, available resources, and scalable solutions. We continue to support solutions that are non-prescriptive and vendor-neutral.

Structuring the Privacy Framework
The Privacy Framework will need to be broad enough to be applicable to all entity types. It will need to be robust enough to be effective. And it will need to be flexible so that it can accommodate legal and business process changes. We recognize that developing a Privacy Framework is a comprehensive undertaking by NIST involving complex legal and policy considerations.

Consumer needs is one key area that NIST should explore as part of this process. At AHIP we are engaged in a number of consumer-focused initiatives and we look forward to learning more about consumers' views through the Privacy Framework development process. Understanding what consumers perceive privacy needs to be will be a first step, which should be followed by a cost-and-benefit analysis to help evaluate whether a privacy proposal should be implemented, or whether the cost would be a burden on public and private entities when compared to the resulting

[1] Department of Health and Human Services. Request for Information on Modifying HIPAA Rules to Improve Coordinated Care. Published 12/14/2018. https://www.gpo.gov/fdsys/pkg/FR-2018-12-14/pdf/2018-27162.pdf

benefit. We recommend that NIST convene public events to promote dialog on this important issue and solicit a variety of viewpoints from diverse stakeholders.

Recommendations
We encourage NIST to continue to work collaboratively in an open, transparent way moving forward with the Privacy Framework. We recommend that NIST begin by evaluating how a Privacy Framework can:

(1) accommodate diverse needs and operating environments while ensuring consistency across different business sectors with varying legal requirements;

(2) recognize that the healthcare sector is unique and healthcare data may require special considerations that non-healthcare entities need not employ;

(3) promote uniformity and reducing the patchwork of requirements while striving for consistency and best practices across different industries and entities; and

(4) avoid duplication of existing consumer privacy requirements while ensuring that effective laws and regulations such as HIPAA remain intact.

We appreciate the opportunity to provide comments on this important topic.

Sincerely,

Marilyn Zigmund Luke
Vice President, Policy and Strategy