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

November 8, 2018

Submitted Via Email to privacyrfc2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Docket No. 180821780– 8780–01

Dear Sir or Madame:

We appreciate the opportunity to comment in response to the National Telecommunications and Information Administration's (NTIA's) notice on ways to protect consumer privacy while advancing prosperity and innovation. The notice was published in the *Federal Register* on September 26, 2018 (87 Fed. Reg. 48600).

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 support 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 encourage the NTIA to continue its efforts to identify sectoral laws (e.g., the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act) and corresponding regulations, to understand whether new requirements might duplicate or conflict with existing privacy requirements, and to exempt private entities from new, conflicting requirements. Existing federal, state, and international privacy requirements for health insurance providers are complex and comprehensive. The NTIA can benefit consumers by maximizing its resources and focusing new privacy requirements on entities that do not have strong, existing and

long history of effective requirements. In addition, the NTIA can also drive uniformity and reduce the patchwork of requirements.

We support the Administration's goals of reducing fragmentation nationally, and of increasing harmonization and interoperability nationally and globally. Otherwise, fragmentation will disincentivize innovation and increase implementation costs for U.S. businesses and the consumers they serve.

In reviewing the regulatory proposals, we offer the following recommendations for future public policies and regulatory requirements:

- **Support for a risk-based approach.** Risk-based flexibility is a critical component that should be part of any future privacy proposals. Organizations are in the best positions to design their information technology systems and business processes to promote consumers' needs and privacy expectations. This includes allowing consumers an opportunity to decide how their information is used and disclosed, when feasible and reasonable.

- **Security and Cybersecurity.** Organizations that collect, store, use, or share consumers' personal information should be required to employ safeguards to protect data. In addition, public and private organizations should keep pace with new developments and emerging threats to ensure that protections for data meet or exceed legal requirements and industry best practices. We encourage the NTIA to look toward frameworks and business models from the National Institute of Standards and Technology and the HITRUST CSF® to garner more information for how to approach technical challenges and design business systems and processes in response.

- **Consumer Rights to Change Data.** Several of the key "individual rights" required by the HIPAA Privacy Rule allow consumers the ability to access, request amendment, and receive an accounting of data disclosures. We support these consumer processes in the context of protected health information and believe the HIPAA provisions can serve as a conceptual baseline for other, non-regulated industries.

  We note that access and an ability to correct data should be reasonable and made in the context of electronic data interfaces and exchanges, made at different time intervals and for a variety of purposes. Permanently changing data or destroying data elements can pose significant risks to individuals' comprehensive health records, present patient safety issues, and complicate audits and compliance processes for businesses that adhere to record retention rules. We encourage the NTIA to consider practical policies that balance data uses with change processes. We recommend a flexible approach for entities and consumers to work together to promote accurate information exchanges.

- **Transparency.** Consumers should be able to obtain information about how an organization collects, stores, uses, and shares their information. Our members are currently required to provide a Notice of Privacy Practices to help inform consumers. We support NTIA efforts that would streamline notices describing a company's privacy practices at a consumer's initial point of interaction with a product or service. We support consumer-centric efforts focused on readability, availability in different languages, and the elimination of "legalese" whenever feasible. Model notices that can be customized for business needs have been helpful in the health care industry (e.g., model notices developed by the U.S. Department of Health and Human Services, Office for Civil Rights).

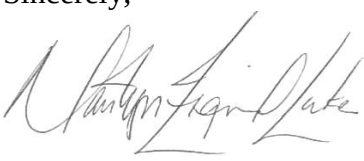
- **Key Definitions.** The NTIA can look to existing terms when drafting definitions for future privacy proposals. HIPAA regulations, NIST documents, and industry sources such as HITRUST certification processes serve as key sources for this information. The NTIA can best utilize available resources by drafting key terms for entities and industries that do not have existing, comprehensive requirements. Such work has already occurred within the health care industry (e.g., key terms for protected health information, minimum necessary).

- **Enforcement.** Effective enforcement should be designed based on each industry's functional regulator. For example, GLBA empowers state insurance authorities for oversight, HIPAA empowers OCR, and the FTC serves as the functional regulator for enforcing certain consumer privacy protections. Future NTIA proposals should take steps to delineate the existing statutory authorities and avoid duplication of enforcement of consumer privacy requirements.

We appreciate the opportunity to provide comments on this important topic. We stand ready to assist the NTIA with the next steps in this process to effectuate the previously discussed user-centric privacy outcomes in line with the high-level goals.

Please contact me at (202) 861-1473 or mzluke@ahip.org if you need additional information.

Sincerely,



Marilyn Zigmund Luke
Vice President