March 9, 2020

The Honorable Lamar Alexander
Chairman
Senate Committee on Health, Education, Labor & Pensions
428 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Patty Murray
Ranking Member
Senate Committee on Health, Education, Labor & Pensions
428 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Alexander and Ranking Member Murray:

The undersigned organizations are writing to urge you to develop legislation to create a modern regulatory framework that governs health data privacy and interoperability. As Congress considers new privacy protections for consumers, we urge you to recognize the unique and important differences between health care data and consumer data.

The major federal law governing health data privacy (HIPAA) was written ten years before the iPhone launched, before mobile apps were common and before most companies had an e-commerce presence. Since then, a wealth of new digital tools and platforms have emerged to improve health care. This massive, swiftly evolving system means more health problems can be identified and addressed. But the current system of data creation, aggregation, storage, use, and sharing was never contemplated by the authors of federal and state laws governing privacy and interoperability. As new tools and platforms have emerged, many fall outside of the federal privacy framework. Some states are stepping in to fill some gaps, but this means some patients may have different protections for some data.

We believe it is past time to modernize the health data framework to enhance the use and protection of data to improve health. With these issues in mind, our organizations came together to recommend the following principles that should govern a modern health data framework:

1. **Patient-Centric.** The framework allows patients to access and retrieve their health data, to know how their health data are used, and to manage, direct, and audit their data.

2. **Strong Privacy Protections.** Health data is protected by clear and strong privacy rules that ensure that only those who need to know or who are authorized (either by the individual or by law) can access and use individually identifiable health information.

3. **Trusted and Secure.** Any entity that handles health data must comply with reasonable administrative, physical, and technical safeguards to improve health data accuracy, security and reliability. Entities should use a method for private unique identification to ensure security and accuracy of individual records.

4. **Transparent, Flexible, Consistent, and Sustainable.** All actors know their rights, responsibilities, restrictions, and repercussions for bad acts. The framework is technology neutral in order to support and allow for private sector innovation. Market incentives drive creation, adoption, and use of tools across different settings and devices.

5. **Interoperable.** Health data is electronically and effortlessly shared – from the hospital bedside to a wearable device at home – with the healthcare professionals, technologists, patients, caregivers

and others who need to have it to treat, test, pay, coordinate, and improve care along the healthcare continuum. Key considerations should be made to improve care delivery, quality improvement, value and outcomes, and advance scientific understanding to produce better treatments and cures for diseases.

6. **Consistent Protections Apply to the Data Regardless of Who Holds the Data.** Consistent protections apply to health data based on the intended health care use regardless of what entity handles the data. This promotes clarity and ensures that any entity who uses protected data is covered by the same rules.

7. **Enforcement Incents Better Privacy and Data Stewardship.** Entities who do not meet strong security protocols, or who inappropriately use or disclose patient health data face strict penalties, including civil and criminal penalties. These penalties become more severe the greater the level of risk and actual harm to an individual, including financial and reputational harm.

8. **Nationwide and Uniform.** All patients receive the same high level of protection regardless of where they are, or where their data are stored, used, or shared. The framework is enforced at the federal level and resources are provided to ensure robust enforcement and compliance.

The purpose of these principles is to guide meaningful change that will make health data and related information more useful while ensuring patients' privacy is protected. The ultimate goal of this effort – of which these principles are a first step – is a reworking of the federal data framework to improve the cost, quality and access of health care in this country by improving the use and sharing of critical information while simultaneously protecting patient privacy.

Our organizations envision a future health care system that is transparent, secure, and responsive to individual privacy needs while allowing participants to use data and technology to accelerate innovations that improve care. We look forward to working with you on legislation that would create a regulatory framework to reach these goals.

Sincerely,

3M
American Academy of Ophthalmology
Alliance of Community Health Plans
American Academy of Family Physicians
American College of Cardiology
Center for Medical Interoperability
Ciox
CoverMyMeds
HealthFlow
McKesson Corporation
Parent Project Muscular Dystrophy
Schizophrenia and Related Disorders Alliance of America
TK2 Medical Treatment Foundation
United Spinal Association
Verily