January 31, 2022

The Honorable Maria Cantwell
Chair
Committee on Commerce, Science, and Transportation
United States Senate
Washington, District of Columbia 20510

The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, District of Columbia 20510

The Honorable Cathy McMorris Rodgers
Chair
Committee on Energy and Commerce
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
Washington, District of Columbia 20515

Dear Chair McMorris Rodgers, Ranking Member Pallone, Chair Cantwell, and Ranking Member Cruz:

As stakeholders representing interests from all facets of American healthcare, we thank you for your leadership on privacy and data security issues and encourage you to come to a final agreement on a single federal privacy framework. While many of the entities represented in our coalition fall under the Health Insurance Portability and Accountability Act (HIPAA), we recognize that an increasingly significant set of data collection and processing activities that benefit patients and consumers falls outside of HIPAA's coverage by non-HIPAA regulated entities that we reference herein as "covered companies."

Your committees have made significant progress in negotiations toward a compromise federal privacy bill over the past few years. The remaining disagreements are understandable, but we urge you to find a middle ground on these issues in order to establish long overdue protections for patients and consumers for the processing and collection of their health data. Although the Federal Trade Commission (FTC) takes an active role in enforcing the prohibition on unfair or deceptive acts or practices (UDAP), other agencies also have jurisdiction, such as the Department of Health and Human Services, to enforce industry-specific privacy and security requirements. Left to its own devices and incomplete authorities from Congress, the FTC is working with limited resources, such as interpreting its data breach notification requirements to cover privacy harms.[1] Although this may have some of the deterrent effects the FTC intended, it is ultimately a confusing interpretation of rules Congress drafted to apply in instances of unauthorized access to data—as opposed to situations where health apps share data purposefully with third parties.[2] A more fundamental question is how government should regulate the aggregation and monetization of sensitive health information outside HIPAA's scope and the FTC's limited ability to directly address the associated risks.

[1] Fed. Trade Comm'n, Statement of the Commission on Breaches by Health Apps and Other Connected Devices, (Sept. 15, 2021), *available at* https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.
[2] *See* letter from Morgan Reed, president, ACT | The App Association, to United States House of Representatives Committee on Energy and Commerce, Re: *Flo Health, Inc.*, Fed. Trade Comm'n complaint (Feb. 17, 2021).

Consumers, patients, and innovators in connected health deserve a more certain and comprehensive legal framework for regulations applied to digital health companies to guide their collection and processing activities involving sensitive information like health data. Similarly, explicit privacy prohibitions would better equip the FTC to prevent likely privacy harms involving health data, instead of waiting until harmful conduct has occurred and then seeking to prohibit the activity under its UDAP authority.

HIPAA already requires robust protections for patients tailored to healthcare that should be maintained. Any national privacy legislation Congress passes must avoid overly burdensome, duplicative, and even unsafe requirements for those entities already required to comply with HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Areas where Congress must strike a careful balance in this regard include but are not limited to: 1) stringent privacy and security requirements, including ones that place strict restrictions on the sharing of patient information; 2) prohibitions around the sale and marketing of patient data; 3) requirements for performing risk assessments; and 4) significant penalties for data breaches. The patient-provider relationship makes some of the general privacy provisions in the major bills under consideration inappropriate for HIPAA covered entities and business associates. For example, deletion of data may pose a safety hazard to patients and staff in the context of clinical care. Thus, Congress should keep HIPAA and HITECH in place and carve a general federal privacy law around them. However, we recommend that such a law adopt an approach to sensitive data, including health data, that is roughly consistent with HIPAA's requirements.

As your committees work toward a compromise, we encourage you to keep the following guiding principles in mind with respect to healthcare privacy:

1. **Individual Rights.** Where practicable, legislation should require covered companies to provide individuals access to their data, the ability to amend incorrect information, and to direct entities to not sell their health data that those companies collect or maintain. In some situations, a right to data deletion may be allowed, unless patient safety or other risks are likely. Accordingly, we agree with the drafters of the major privacy bills under consideration in Congress that the obligation to honor data deletion requests should not extend to HIPAA covered entities or business associates, underscoring the need for legislation to carefully exclude data subject to HIPAA and associated privacy requirements. Privacy rights should be honored unless they are waived by an individual in a meaningful way.
2. **Transparency and Consent.** Where appropriate, legislation governing electronic data in apps should require covered companies to obtain affirmative, opt-in consent for sensitive information, including health data, informed by clear disclosures as to how covered companies collect, use, store, protect, and share health data, and for what purpose a covered company collects or processes such data. Terms should be clearly defined and unambiguous, and this should be more than a "check the box" process to use an app.
3. **Civil Rights.** Legislation should clarify the FTC's role in assisting other federal agencies tasked with enforcing discrimination laws, where appropriate, against entities that process health data in a manner that results in harmful bias or discrimination. The FTC should, in

collaboration with those federal agencies, protect individuals' civil rights and work to evaluate the potential risks posed by algorithms, particularly as inferences are drawn from individuals' sensitive health data.

4. **Data Security.** Legislation should require covered companies to maintain a comprehensive security program that is designed to protect the security, privacy, confidentiality, and integrity of health data against risks—such as unauthorized access or use, or unintended or inappropriate disclosure—through the use of reasonable administrative, technological, risk management, and physical safeguards built into the design of their applications, products, or services to appropriately protect the data. These programs should be scalable and technology neutral.
5. **Data Minimization and Access Restrictions.** Legislation should require companies to limit health data processing, transfer, and collection to those activities that are reasonably necessary, proportionate, and limited to provide a product or service specifically requested by an individual, reasonably anticipated within the context of a company's ongoing relationship with an individual, or meeting a particular purpose identified publicly on a company's website or marketing materials. Legislation should also require companies to limit internal access to health data to only those employees or third-party service providers whose access is necessary to provide products or services to the individual to whom the data pertains, within the context of the company's ongoing relationship with the individual.
6. **More Resources.** A federal privacy law should include increased funding authorization levels for the FTC to carry out its expanded obligations and better position itself to address healthcare privacy issues under such a framework.
7. **Rulemaking Authority.** Legislation should provide the FTC with limited, clearly defined Administrative Procedure Act rulemaking authority, enabling the FTC to define needed privacy and security guardrails where they are not already covered by existing laws (e.g., HIPAA and HITECH).

We hope that these principles help underscore where negotiators have already found alignment, while also highlighting the urgency we face now with respect to the need for privacy and security protections for Americans' most sensitive personal data. Establishing a single set of strong, national privacy requirements is a key ingredient to unlocking the value-based innovative potential for life-saving technologies to come to market in a way that puts patient and consumer privacy first. We thank the committees for making great strides toward this goal and look forward to assisting in any way we can going forward.

Sincerely,

American Board of Quality Assurance and Utilization Review Physicians, Inc.
AHIP
College of Healthcare Information Management Executives (CHIME)
The Connected Health Initiative
Digital Therapeutics Alliance
Dogtown Media
Health Tech Strategies
Nova Insights

Particle Health, Inc.
Rimidi Inc.
RxLive, Inc.