Hearing: Promoting U.S. Innovation And Individual Liberty Through A National Standard For Data Privacy

House Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
Statement for the Record of Morgan Reed
President, ACT | The App Association and Connected Health Initiative

Dear Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee:

Thank you for the opportunity to provide input for this hearing on data privacy, one of the most important pillars of the internet age. ACT | The App Association's (the App Association's) Connected Health Initiative (CHI), is a multistakeholder coalition with a shared interest in ensuring the public policy landscape enables and encourages the use of digital health tools that improve outcomes and help control the costs of care. CHI's interest in federal privacy law under the Subcommittee on Innovation, Data and Commerce's (IDC's) jurisdiction has grown in concert with the expansion of digital health information that is created or transferred outside the scope of the Health Insurance Portability and Accountability Act (HIPAA). In the latter days of a global pandemic that forced virtual care adoption and in the middle of a crushing physician shortage set to increase to up to 122,000 by 2032,[1] digital health tools like remote monitoring and telehealth platforms are playing a more important role than ever. Patients, providers, and consumers must be able to trust that innovators in this space are protecting the security and privacy of sensitive personal information.

Introduction

The App Association has long called for a strong national data privacy law, and CHI has also put forth principles for a federal privacy law of general applicability. The biggest problem with the privacy landscape is the mismatch between consumers' expectations of their privacy and the reality of how many entities buy, sell, and use their data. We have all experienced the phenomenon of discussing a topic with friends and getting served a targeted ad shortly after. While we feel as though our phones are spying on us, companies are actually using our online behavioral data to predict other things in which we might be interested. We willingly consent to the collection and use of our data in this way through the terms and conditions of signing up for nearly any online account—for rideshare apps, social media sites, online retail, and web-enabled consumer health products, to name just a few. And we rarely think about the implications of these conditions afterward.

[1] Assoc. of American Medical Colleges, "New Findings Confirm Predictions on Physician Shortage," press release (Apr. 23, 2019), *available at* https://www.aamc.org/news-insights/press-releases/new-findings-confirm-predictions-physician-shortage.

A comprehensive national privacy policy would help consumers understand where their data is located, who has access to it, and what their rights are surrounding the sale or use of it. Especially in the health care space, consumers need to be protected from actors looking to misuse their data and expose them to risk. Many consumers misunderstand the protections afforded to them by existing laws like HIPAA or Federal Trade Commission (FTC) regulations. Instead of modifying or expanding these existing laws and regulations, Congress should create a new, privacy-focused law that covers all kinds of consumer data.

Consumers and Companies Alike Usually Misunderstand HIPAA

At its core, HIPAA focuses on the portability and interoperability of health data. Congress designed it to ensure that consumers can change insurance providers or primary care physicians without having their data hoarded by those entities. The original text of the law did not include a privacy requirement, but instead required the Department of Health and Human Services (HHS) to promulgate a rule on privacy standards three years after enactment if Congress failed to pass a national set of privacy requirements for entities regulated under HIPAA.[2] Since HHS promulgated the Privacy Rule under the existing, limited authorities granted to it under the original HIPAA statute, it could break no new ground on protecting privacy and only worked within its interoperability-driven mandate. This legislative and regulatory history helps explain why the HIPAA Privacy Rule exhibits otherwise surprising levels of permissiveness and interoperability rather than protection and patient control of personal health data. And now, the explosion of health data held by a wide variety of entities not covered under HIPAA means that much of our health data is not covered by a Privacy Rule that is not a good fit for it in the first place.

Most consumers do not understand this misalignment. A 2019 Pew Research study found that 63 percent of Americans say they understand very little or nothing at all about the laws and regulations that are currently in place to protect their data privacy.[3] To complicate the picture further, there are many cases that consumers might think are covered but are not because of the construction of the HIPAA Privacy Rule. For example, HIPAA rules mostly do not apply to vendors of public health records (like fitness trackers), payment processors (like banks), and even some doctors who do not bill through electronic claims to insurance plans.[4] These are all instances where Americans without an understanding of the limitations of the HIPAA privacy rule could reasonably expect their data to be protected, but it is not.

---

[2] *Health Insurance Portability and Accountability Act of 1996* (P.L. 104-91).
[3] https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
[4] HIPAA Privacy Rule, 45 CFR 160 and 45 CFR 164 subparts A and E.

HIPAA regulations are difficult for companies to understand as well. The definitions of "covered entity" and "business associate" have many nuances, and it is often hard for small businesses like App Association members to determine whether they are subject to the regulations. To help our members and other similar organizations, the App Association created a resource to check for whether they are a covered entity or a business associate. If a business focused on healthcare data has difficulty in understanding its legal obligations, it is not reasonable to expect consumers to understand their rights and protections under the law.

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. 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.

Notwithstanding its shortcomings as a federal privacy law of general applicability, HIPAA requires robust protections for patients tailored to healthcare that should be maintained. Patients have come to rely on a federal healthcare regime that generally keeps their health records out of circulation. However, despite its interoperability roots, HIPAA's de-emphasis on patient control over health records helped contribute to a situation where, perversely, patients have struggled to bring their records with them to new providers efficiently. But more relevantly here, it also rendered patients essentially unable to port their health information outside the HIPAA umbrella. Responding to this unintended consequence, Congress enacted the 21st Century Cures Act, which required the sub-agency that enforces HIPAA, the Office of Civil Rights (OCR), to prohibit "information blocking" by HIPAA covered entities and business associates. Although OCR is not yet enforcing the information blocking rule, it is already applying additional pressure on Congress to establish a privacy framework to address risks to health information once a patient requests its transfer to non-HIPAA entities as the information blocking rules contemplate. To help orient patients, providers, and consumers to those risks—and to bolster FTC enforcement in these scenarios—CHI suggested that the information blocking rules require any non-HIPAA covered entities receiving health information on behalf of patients make a few high-level attestations as to their privacy and data security practices. This approach is no substitute for a federal privacy law. However, it would help address the perceived and actual privacy and security disparities between the HIPAA environment and the rest of the American economy. For the information blocking rules to work as intended, Congress should enact a federal privacy framework.

Some advocates have proposed that, instead of working out compromise general privacy protections, Congress should expand HIPAA to cover health-related data collection and processing activities across the rest of the economy. However, as alluded to above, policymakers would need to rework HIPAA extensively to support such an expansion. Rules around covered entities, business associate agreements, types of data covered, and reasons for triggering coverage would all need to be radically altered. In addition, the HIPAA Privacy Rule is not law but an agency rule and could be changed if the agency chooses. HHS also does not have the budget, personnel, or authority to oversee a large expansion of the scope of the HIPAA Privacy Rule. Because of the permissiveness of the original law, the limited circumstances covered by it, and the difficulty in understanding requirements, expanding HIPAA—and OCR—to police the entire economy is not likely to be the best approach. We need a comprehensive privacy law that would protect all kinds of data, including sensitive health information. Similarly, a federal law of general applicability should avoid accidentally imposing its requirements on Protected Health information (PHI) subject to HIPAA, which would result in unintended consequences explored in more detail below.

Data use disclosures do not work for consumers

While not federally required (except in the case of users under 13 years of age), many websites and apps have privacy policies and terms and conditions of data collection and use. They notify consumers of those policies primarily through long documents, sometimes hiding the fact that many companies generate significant revenue through the sale and collection of data. Sometimes, apps or websites will push a shorter notification to a user's device to inform them of the applicability of a certain part of the policy. While none of the available methods is a perfect way of conveying dense information quickly, the in-time notices tend to be more effective since they appear more seamlessly in the context of the consumer's engagement with an online service. However, there is no easy way to increase the usefulness of such notices without a clear and universal privacy law that would outline the basic requirements of such disclosures. To operate in an increasingly online world, consumers should understand how their data is being collected, what it is being used for, and who has access to it. A national privacy law would take steps toward ensuring this future.

We need strong federal privacy protections

This Committee has made significant progress in negotiations toward a compromise federal privacy bill over the past few years. The remaining disagreements are understandable, but I 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 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 (HHS), to enforce

industry-specific privacy and security requirements. Left to its own devices and with incomplete authorities from Congress, the FTC is working with limited resources, such as interpreting its data breach notification requirements to cover privacy harms.[5] 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.[6] 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.

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. As you 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.

---

[5] 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-notificationrule/
statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[6] 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).

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 or improve 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).

The App Association believes American Data Privacy and Protection Act (ADPPA, H.R. 8152, 117th Cong.) strikes a reasonable balance on several of its main provisions. I hope that my testimony has made it clear that modification of the existing laws at the expense of a national statute would lead only to additional complications. Congress should act on a strong, bipartisan, national framework for data privacy that draws from our evolving understanding of the needs of businesses and consumers.