Bipartisan Policy Center

VIA ELECTRONIC SUBMISSION - healthprivacy@help.senate.gov

September 28, 2023

Senator Bill Cassidy, M.D.
Ranking Member Co-Chair
Senate Health, Education, Labor, and Pensions Committee

RE: Improving Americans' Health Data Privacy

Dear Senator Cassidy:

The Bipartisan Policy Center (BPC) appreciates the opportunity to submit comments on steps needed to leverage technology to improve patient care, while safeguarding patient privacy.

BPC is a nonprofit organization founded in 2007 to combine the best of ideas from both parties to promote health, security, and opportunity for all Americans. Through our recommendations, BPC's Health Program strives to develop bipartisan policies across a variety of health issues that improve the nation's health outcomes, reduce rising health care costs, improve equity in health services, and make quality health care available, affordable, and accessible for all.

BPC recently responded to the Federal Trade Commission's proposed Health Breach Notification rule regarding health data (August 2023) and your Request for Information on Artificial Intelligence (September 2023). Our remarks below draw heavily from both these comments.

Patient privacy regarding medical information has been a consistent focus for BPC for the past decade. BPC released a white paper in 2013, which discussed the significance of information technology in health care and conducted a summit in 2013, addressing the utilization of big data in health care. BPC's work on broader data privacy includes analyses of federal and state-level legislation, including comprehensive and youth data privacy bills, and the privacy implications of specific emerging technologies, including smart homes and face recognition technologies.

BPC appreciates the opportunity to comment and please do not hesitate to contact Mikayla Curtis (mcurtis@bipartisanpolicy.org) if you would like to connect with BPC Health Program staff for additional information.

Sincerely,

Tom Romanoff

Marilyn Serafini
Executive Director, Health

Julia Harris
Associate Director, Health

Tom Romanoff
Director, Technology

Privacy in Health Care

Over the past year BPC undertook an extensive effort to develop evidence-based, federal policy recommendations for the effective use of Remote Patient Monitoring (RPM) technology. The use of telehealth, digital apps, and other mobile tools has increased exponentially since the COVID-19 pandemic and adoption is only expected to increase as the technology continues to improve and health care providers and patients become more familiar with these products. Despite this growth, Congress has not passed a comprehensive consumer data privacy law.

The United States has no single overarching privacy law. The main health-related privacy statute is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA protects patient information when held by certain covered entities, including health providers, health insurers, and the business associates of those individuals or organizations. Yet HIPAA was enacted the same year the Motorola flip phone and Palm Pilot were introduced to the market. Since then, computing power, adoption of electronic health records, and delivery of health care services have all changed dramatically.

In the absence of strong, overarching, national privacy laws, state legislatures have taken action to protect their citizens' privacy:

- Virginia's Consumer Data Protection Act gives consumers the right to access their personal data and request that it be deleted by businesses.
- The Connecticut Data Privacy Act gives residents certain rights over their personal data and establishes responsibilities and privacy protection standards for data controllers that process personal data.
- California was the first state to enact a consumer privacy law, the California Consumer Protection Act, which creates an array of consumer privacy rights and business obligations regarding the collection and sale of personal information.
- The Colorado Privacy Act provides residents with the right to opt out of targeted advertising, the sale of their personal data and certain types of profiling.
- Utah consumers have the right to: (1) know or confirm processing activity; (2) access personal data; (3) obtain a copy of personal data in a portable and readily usable format; (4) delete personal data; (6) opt out of targeted advertising and sales of personal information; and (7) avoid discrimination as a result of exercising their consumer rights.
- Washington's Governor signed a health data privacy law earlier this year which aims to protect personal health data that falls outside of HIPAA.
- Oregon's Consumer Privacy Act provides numerous rights to consumers, including the (1) Right to Know (2) Right to Correction (3) Right to Deletion (4) Right to Opt Out (5) Right to Data Portability (6) Sensitive Data Protections and (7) Special Protections for Youth.
- The Iowa Act Relating to Consumer Data Protection extends data privacy rights to consumers and gives the Iowa Attorney General exclusive authority to issue civil investigative demands, conduct enforcement actions and seek the imposition of injunctive relief and/or civil penalties for violations.

- Tennessee's Information Protection Act is the first to "require notification of any breach, regardless of whether the information is encrypted or not."
- The Indiana Consumer Data Protection Act, which will effective in 2026, provides the following set of rights for consumers: the right to access, the right to correct, the right to portability, the right to delete, the right to opt out of certain processing, the right to opt out of the sale of personal data and the right to opt in for sensitive data processing.
- The Montana Consumer Data Privacy Act, similar to Connecticut's law, provides consumers the right to revoke their consent to data processing; allows consumers to opt out of sales and targeted advertising, and permits a consumer to request deletion of all personal data.
- The Texas Data Privacy and Security Act provides similar rights to other privacy bills, but applies more broadly – to both individuals and companies doing business in Texas.
- Florida's Digital Bill of Rights contains similar consumer rights to those found in most data privacy legislation, is aimed only at large tech companies.

HIPAA must be updated to reflect the current status of health data while allowing for future innovation.

Additionally, there are data outside the scope of HIPAA that are protected by the Federal Trade Commission (FTC). The FTC enforces the prohibition on unfair or deceptive acts or practices and has promulgated the Health Breach Notification Rule, which requires companies that have a data breach to share a notification publicly.[1,2] BPC commented on FTC's recently proposed rule to expand the types of data and entities subject to the Health Breach Notification rule.

BPC supports the expansion of the definition of health care providers to include nontraditional sources of health care services or supplies, including app developers. Expanding the definition of health care services or supplies to include not only direct medical services but also wellness products—such as sexual health, sleep, or diet apps—is more consistent with the type of intimate personal information users disclose in these applications. However, these data are not included in the revised definition of "personal health record identifiable information," exposing a possible gap in the protections provided under the Health Breach Notification rule.[3] Fertility, sleep, wellness, and location data can include personally identifiable health information that users would prefer to be kept confidential, as noted in the proposed rule.[4]

BPC also recommends that the definition of personal health record identifiable information clearly include health care services or supplies. The revised definition of a personal health record now includes an electronic record that has the "technical capacity to draw information from multiple sources" and that is managed, shared, and controlled by or primarily for the individual. The previous definition of a personal health record was limited to electronic records that utilized those functions. Expanding the personal health record definition to include those capable of doing so expands the protection of personal health information. Users may have multiple devices or multiple sets of data coordinated by their personal devices, such as a smartphone or their providers' device(s). Due to the inherent connectivity of these devices, there is a risk of an unintended breach.

There are an increasing number of underdefined areas of privacy in health care. For example, HIPAA may not apply to user-generated data or data generated by remote monitoring devices. Such user-generated data can sit outside the provider/payer setting and are not covered by HIPAA.[5]

One article described the situation this way: "Rather than providing care themselves, telehealth companies often act as middlemen connecting patients to affiliated providers covered by HIPAA."[6] As a result, information collected during a telehealth company's intake may not be protected by HIPAA, while the same information given to the provider would be. Additionally, patients who are monitored or managed at home using a health system's technology likely do not have strict privacy and cybersecurity safeguards in place.[7]

Cybersecurity is a major concern for healthcare providers and device manufacturers. The FDA, at Congress's direction, has begun evaluating cybersecurity in its review of medical devices. At a recent Senate hearing, one witness said that "there is an increasing amount of personal health information that is circulated and not regulated based on wearable technologies and home medical technologies, and there have been groups other than ours that are looking into what kinds of data are being shared that are not under some kind of regulatory scrutiny."[8]

There have been reports regarding tracking technologies embedded in a hospital's patient portal, as well as studies showing that health apps have shared users' personal information.[9,10] The FTC has engaged in enforcement against digital health companies such as Flo, Prenom, and GoodRx under its existing authority.[11,12,13]

Lastly, there are few, if any, safeguards preventing law enforcement from obtaining health information. This gap is illustrated through accounts of law enforcement using archived newborn screening blood samples to find criminal suspects. As the definition of health data expands to include location, sleep, and other non-traditional medical information, this data should be subject to the same judicial review needed by law enforcement to access private property.

BPC recommends that a comprehensive consumer data privacy law is needed to protect the individual data that is collected from a growing number of digital health tools.

Artificial Intelligence

When implemented correctly, AI could revolutionize the health care landscape. It has the potential to bridge gaps in health care inequities, alleviate provider burnout, improve patient care, streamline administrative processes, and reduce health care expenses. It also comes with privacy challenges and other risks. For instance, AI systems could inadvertently de-identify individuals and amplify the risk of data breaches. Tailored policies are needed to tap into AI's transformative potential and mitigate risks. Regulatory bodies like FDA have a crucial role to play in steering the integration of AI in health care and mitigating privacy concerns.

Privacy in AI

Ongoing concerns about patient privacy have increased with the rise of digital technologies and the advancement of AI applications in health care. The existing framework for patient privacy, mainly enumerated under HIPAA, is not sufficient for today's information flow. There are many types of products and data that HIPAA does not cover, such as certain apps and consumer devices.[14] Developers of AI tools may turn to these third-party apps for data to train their algorithms. However, the use of AI can, in fact, make it easier to re-identify patients, putting their health privacy at risk.[15] And tools like AI chatbots are Open AI, putting all information a provider enters into the public realm.[16]

The right to be forgotten in these systems is particularly difficult to operationalize as many of the training sets are compounded from many sources. For healthcare data, the challenge is on the input side. If a user discloses health data, willingly or unwillingly, that information gets incorporated into future training sets. Products will also log inquiries in their systems for record-keeping purposes. If these records include sensitive health information, there is little a user can do to retrieve or delete that information.

BPC recommends that FDA update its regulatory framework to address the unique risks—including privacy concerns—of medical devices that incorporate AI software. AI medical devices, with their ability to evolve and update based on new data, present unique privacy concerns. FDA has cleared AI devices that rely on "locked" algorithms, in which consistent inputs yield consistent outputs.[17] AI devices that rely on "adaptive algorithms" can update based on new data, posing challenges related to data security and patient privacy.

Over the last few years, FDA has taken steps to address AI devices that rely on "adaptive" algorithms. The FDA's recent draft guidance is an important step, yet significant challenges remain.[18] The practical applications and potential challenges of this framework in real-world scenarios have yet to be fully realized, and FDA has acknowledged the difficulty in regulating devices that are designed to change over time.

It will be critical to consider the potential benefits and rewards of these applications when developing governance frameworks that impose requirements on health-related AI use cases. Determining which AI use cases are high-risk and which are high-reward can help policymakers develop broader AI governance frameworks that effectively address risks—including to patient privacy—and maximize the benefits that AI technologies can pose in the health sector.[19]

BPC recommends that FDA promote transparency in the performance information of medical devices. Given the unique complexities of many AI-enabled products—and the inherent privacy concerns—it is essential that the performance data of these tools is available.

BPC's extensive research on RPM technologies revealed that even FDA approved or cleared devices do not always share full performance information. In 2018, FDA published guidance for industry on reporting age, race, and ethnicity data for medical devices, however it focused on devices for which there are clinical studies, and many devices do not undergo clinical trials before coming to market.[20] In 2022, FDA approved only 22 devices through the premarket approval (PMA) process and more than 3,000 devices through the 510(k) pathway, the majority of which did not undergo clinical trials. FDA-approved labels should specify the populations on which the device was tested and how it performs across races, ethnicities, and sexes.[21]

Open communication about device limitations is essential to ensure safe usage and avoid unintended consequences, such as breaches of data privacy. The In Vitro Diagnostics (IVD) rule offers a model for transparent device labeling, mandating the disclosure of performance characteristics, opening instructions, and calibration procedures.[22] Performance characteristics should include, but not be limited to, the analytical performance of the device, the error rate, and the relevant population on which the device has been tested. FDA should have a labeling requirement that also highlights information regarding performance drift and the timeframe over which the devices are likely to be accurate. Other options include developing something akin to a "nutrition facts label" for AI.

[1] 15 U.S. Code § 45. Available at: https://www.law.cornell.edu/uscode/text/15/45

[2] 16 C.F.R. §318.1. Available at: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318

[3] "As revised, "PHR identifiable information" would be defined as information (1) that is provided by or on behalf of the individual; (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; (3) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (4) is created or received by a health care provider, health plan, employer, or health care clearinghouse." FRN https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_proposed_hbnr_for_posting_only_.pdf

[4] "The Commission also requests comment on the following scenario: a third party service provider, such as an analytics firm, receives PHR identifiable health info (e.g., device identifier and geolocation data from which health information about an individual can be inferred) and then sells it to another entity without the consumer's authorization." https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_proposed_hbnr_for_posting_only_.pdf

[5] "HIPAA doesn't apply to medical device manufacturers or patients, so physicians must be extra diligent when evaluating how to incorporate information from those sources." AMA RPM Playbook available at https://www.ama-assn.org/system/files/ama-remote-patient-monitoring-playbook.pdf

[6] Katie Palmer, Todd Feathers, and Simon Fondrie-Teitler, "'Out of control': Dozens of telehealth startups sent sensitive health information to big tech companies," *STATNews,* December 13, 2022. Available at: *https*://www.statnews.com/2022/12/13/telehealth-facebook-google-tracking-health-data/

[7] Bill Siwicki, "Is remote patient monitoring the new cybercrime target?" *HealthcareITNews,* March 21, 2022. Available at: https://www.healthcareitnews.com/news/remote-patient-monitoring-new-cybercrime-target

[8] U.S. Congress. Senate. Committee of Homeland Security and Government Affairs. *Hearing on Cybersecurity Risks in Health Care,* 118th Congress, March 16, 2023. Available at: https://www.c-span.org/video/?526750-1/hearing-cybersecurity-risks-health-care

[9] Annie Burky, "Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies," *Fierce Healthcare,* October 20, 2022. Available at: *https*://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3

[10] Katie Palmer, Todd Feathers, and Simon Fondrie-Teitler, "'Out of control': Dozens of telehealth startups sent sensitive health information to big tech companies," *STATNews,* December 13, 2022. Available at: https://www.statnews.com/2022/12/13/telehealth-facebook-google-tracking-health-data/

[11] https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc

[12] U.S. Federal Trade Commission, "Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order," May 17, 2023. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc

[13] U.S. Federal Trade Commission, "FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising," February 1, 2023. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

[14] Office of Senator Mark R. Warner, "Cybersecurity is Patient Safety: Policy Options in the Health Care Sector," November 2022. Available at: https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf

[15] Price, W. Nicholson, Problematic Interactions between AI and Health Privacy, U. Mich. Law Repository (2021) available at https://repository.law.umich.edu/articles/2331

[16] Kanter, G., and Packel, E., Health Care Privacy Risks of AI Chatbots, JAMA (2023) available at https://jamanetwork.com/journals/jama/article-abstract/2807169.

[17] U.S. Food and Drug Administration, "Proposed Regulatory Framework for Modifications to Artificial Intelligence/ Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback," Available at: https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf

[18] U.S. Food and Drug Administration, "CDHR Issues Draft Guidance on Predetermined Change Control Plans for Artificial Intelligence/ Machine Learning," March 2023. Available at : https://www.fda.gov/medical-devices/medical-devices-news-and-events/cdrh-issues-draft-guidance-predetermined-change-control-plans-artificial-intelligencemachine

[19] Gabrielle Shea and Sabine Neske, "Defining High-Risk, High-Reward AI," April 2023. Available at : https://bipartisanpolicy.org/explainer/high-risk-high-reward-ai/

[20] U.S. Food and Drug Administration, "Evaluation and Reporting of Age-, Race-, and Ethnicity-Specific Data in Medical Device Clinical Studies," September 2017. Available at https://www.fda.gov/media/98686/download

[21] Claudia Wallis, "Fixing Medical Devices That Are Biased against Race or Gender," *Scientific American*, June 1, 2021. Available at: https://www.scientificamerican.com/article/fixing-medical-devices-that-are-biased-against-race-or-gender/

[22] 21 C.F.R. §809.3. Available at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=809&showFR=1