STRENGTHENING HEALTH DATA PRIVACY FOR AMERICANS:

ADDRESSING THE CHALLENGES OF THE MODERN ERA

Senate Committee on
Health, Education, Labor & Pensions
Senator Bill Cassidy, M.D. , Ranking Member

Introduction

Health care information is unique among types of data and plays a distinctly important role in our society. It can be used to increase access to care, support research for new diagnostics and treatments, improve care quality and outcomes, and lower care costs. However, this information faces heightened risk of misuse over other types of data. If disclosed inappropriately, a patient's identifiable health information, like their cancer diagnosis or history of substance use disorder, cannot be changed and hostile actors can use this information to interrupt care to harm patients and breach their privacy.

As technology proliferates and health data interoperability increases, we have greater opportunity to improve care and patients' access to their health information. Yet, increased access can lead to increased vulnerability for inappropriate data disclosures and a greater pool of data for hostile actors to exploit for nefarious purposes.

The digitization of sectors of our economy, not just in health care, have led to broader calls to create comprehensive data privacy frameworks. 13 states and 137 countries have passed data privacy laws. Yet to date, the United States does not have a comprehensive data privacy law; Congress needs to act to fill this gap. As Congress examines data privacy, the health care sector will need to play a distinct role with distinct considerations. The Senate Committee on Health, Education, Labor, and Pensions (HELP Committee), of which I am Ranking Member, will need to be at the forefront of this work.

As such, the Committee released a request for information (RFI) in September 2023 asking interested parties to provide responses to a spectrum of questions on health data privacy. Respondents included trade associations, hospitals, electronic health record vendors, health technology companies, and think tanks. Having gleaned a number of themes from the responses received, this paper includes a number of proposals for possible legislative action. They fall into the following three categories:

1. Updates to the existing health privacy framework (i.e., updates to the Health Insurance Portability and Accountability Act (HIPAA));
2. Health data in the HIPAA "gray area"; and
3. Data outside of HIPAA.

I look forward to discussing these proposals in more detail and working with my colleagues on the HELP Committee, in Congress, and across the country, to consider legislation to advance health privacy law into the next era.

The Existing Health Privacy Framework

Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to "improve [the] portability and continuity" of health care and "simplify the administration of health insurance."[1] In 2000, the Department of Health and Human Services (HHS) built upon this framework and issued the HIPAA Privacy Rule to "address the use and disclosure of individuals' health information," known as "protected health information," or "PHI."[2] Entities who must comply with the HIPAA statute and associated regulations are known as "covered entities." Covered entities are defined as health care providers that transmit health information in electronic form, health plans, and health care clearinghouses.[3]

The protections and permissive nature written into the HIPAA statute have worked to create a robust privacy

[1] 100 Stat. 2548.
[2] 45 C.F.R. 160, 45 C.F.R. 164 (2001).
[3] 45 C.F.R. 160.103 (2013).

framework for over 30 years. HIPAA-covered entities report that they are largely able to comply with privacy requirements and have struck a good balance between safeguarding patient privacy and allowing information sharing under appropriate circumstances, such as improving patient care and supporting clinical research. However, respondents shared areas where HIPAA should be improved to account for a more technically advanced and digital health care system. While a major rewrite of HIPAA could upset decades of case law and established precedent, leading to a disruption patient care, discrete updates and clarifications to the existing framework would better enable HIPAA to function for the future.

Minimum Necessary

One of the most important safeguards established by the HIPAA framework is creating limitations on how much PHI should be shared. The "minimum necessary" standard requires covered entities to limit the use and disclosure of PHI to the most limited information that would fulfill a request.[4] This standard is intended to limit inadvertent unauthorized disclosure of PHI by restricting the amount of information transferred between health care parties. For example, a provider reviewing a patient's medical history should generally not have access to a patient's Social Security number. The minimum necessary standard does, however, permit limited exemptions to limit information sharing, such as for treatment purposes or with the patient's express authorization.[5]

While this standard has been a useful safeguard to limit unauthorized disclosure of PHI, the increased digitization of health care information has created technical challenges for compliance. When a covered entity shares information in paper format (i.e., printed or by facsimile), they typically redact the information not considered relevant to the request. However, stakeholders have reported challenges with segmenting certain data in a patient's electronic health record (EHR) to permit a similar redaction.[6] Covered entities have become reluctant to share information for fear of over-disclosure, leading ironically, to under-disclosure. While the minimum necessary standard is based on an individual covered entity's interpretation, it can be unclear whether violations of this standard are judged based on the requestor's interpretation or the covered entity's.[7]

Flexibility is necessary to provide some regulatory reassurance for fulfilling PHI requests for health care purposes; however, Congress needs to clarify the minimum necessary standard to better allow for a more digital health care system. Specifically, Congress should direct the HHS Office for Civil Rights (OCR) to provide clear guidance on how the minimum necessary standard aligns with other regulatory requirements, including health data system interoperability requirements mandated by the 21st Century Cures Act. This would continue to balance protecting against unnecessary disclosures of PHI, while providing more certainty to stakeholders that they can share information to improve patient care.

Release of Information/Third Party Directive

One of the core tenets of the HIPAA framework is that every American patient has the right to review and obtain a copy of their medical records. This right, known as the "patient right of access" under HIPAA requires covered entities to provide access to a patient's information within 30 days of being requested.[8] The patient is required to

---

[4] 45 C.F.R. 164.502(b) and 45 CFR 164.514(d) (2013).

[5] 45 C.F.R. 164.502(b)(2) (2013).

[6] Letter from William Stead to Sylvia Burwell, Secretary, U.S. Department of Health and Human Services (Nov. 9, 2016), https://ncvhs.hhs.gov/wp-content/uploads/2018/03/2016-Ltr-Privacy-Minimum-Necessary-formatted-on-ltrhead-Nov-9-FINAL-w-sig.pdf.

[7] Melissa Martin, Testimony of the American Health Information Management Association to the NCVHS Privacy, Confidentiality, and Security Subcommittee on HIPAA and Minimum Necessary, American Health Information Management Association (June 16, 2016), https://ncvhs.hhs.gov/wp-content/uploads/2016/05/Martin-combined.pdf.

[8] See supra Note 1, Section 264 (An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a covered entity's designated record set.); 45 C.F.R. 164.524.

pay the fees imposed by the covered entity for the production of the records.[9] That fee must be "reasonable" and "cost-based" to cover labor, supplies, and postage.[10] In lieu of calculating the actual cost, covered entities may charge a flat fee for all individual patient requests for electronic copies of PHI, generally not to exceed $6.50.[11] This amount has come to be known as the "patient rate." An individual patient may also have their provider or health plan send their individual PHI to a designated third party.[12] These requests may include patients sending hospital records to their primary care providers, patients requesting one provider send their records to another of their providers, or patients requesting their specialty care records be sent to a health application on their phone. Since that request is from a patient on their own behalf, the patient rate applies.

The HITECH Act of 2009 updated this framework by creating a "third party directive" for other parties to initiate requests from covered entities with written authorization from individual patients.[13] For records transmitted to third parties, such as law firms and health insurance companies, the patient rate and other fee limitations do not apply, and covered entities and their contractors could charge fees permissible under state law.[14] The fees charged are typically based off of time and resources expended to compile, extract, scan, and send the records, often from numerous sources within a health system.

Covered entities have generally contracted with specialized release of information (ROI) service companies to fulfill these requests. This involves the contractor finding, compiling, and sending records in response to the many thousands of requests that covered entities receive. Nearly 80% of providers contract out these services.[15] Oftentimes, requesters ask for records that exist across electronic platforms, in paper records, are text-based and image-based, all to be sent via digital format, facsimile, or CD-roms. Covered entities have preferred to contract with ROI companies to relieve themselves of the burden and cost of performing these services and complying with right of access requirements. The business model of these companies is to charge the requesters their applicable rates and leave the covered entities out of it, enabling the covered entities to comply with HIPAA without the hassle and cost of performing the service themselves.

In some cases, fraudulent and abusive actors take advantage of pathways for requesting medical records by duping patients into signing lengthy forms that allow them to masquerade as the patient, promising payouts through medical malpractice suits. They aren't truly acting on the patient's behalf, but are still able to receive the low patient rate. Indeed, many third party directive requests deemed patient requests under current HHS rules are perpetrated by scammers and law firm and insurance company phishing expeditions and do not impact the treatment of patients.[16]

The patient right of access framework is intended to give patients control and autonomy over their health care data and health care decision making. However, abuse of this right is not only potentially putting patients' protected health information in the hands of nefarious actors, but it also prevents appropriate recoupment of costs for services provided. In 2020, ROI company Ciox Health sued HHS about which records requests were truly made on behalf of patients and deserved to be charged only the patient rate versus true third party directive requests. Fraudulent requests from phishing firms cost Ciox Health over $10 million per year. However, without

---

[9] 45 C.F.R. 164.524(c)(2)(iii)(B) (2014).
[10] 45 C.F.R. 164.524(c)(2)(iii)(B) (2014).
[11] Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. 164.524, Department of Health and Human Services (Oct. 20, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
[12] 45 C.F.R. 164.524(c)(3)(ii) (2014).
[13] Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. 164.524, Department of Health and Human Services (Oct. 20, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
[14] *Id.*
[15] Angie Comfort, The staggering financial burden of a proposed HIPAA rule, STAT News (Mar. 17, 2023), http://www.statnews.com/2023/03/17/hipaa-privacy-rule-changes-staggering-financial-burden/.
[16] Ciox Health v. Alex Azar, 435 F. Supp. 3d 30 (D.D.C. 2020).

the ROI industry, health systems and health plans may be forced to take on the costly work of retrieving and disseminating patient records, estimated to cost over $1 billion annually.[17]

The uncertainty in HIPAA's "third party directive" must be fixed. Congress should more clearly define which requests should be eligible for the patient rate to ensure only true requests on behalf of patients receive that benefit.

Align Treatment of All Health Data

HIPAA was designed as a "permissive" framework to allow providers to see the full clinical profile of a patient. An incomplete medical record leaves providers without the ability to properly treat a patient and may lead to inappropriate care. Data segmentation required by inconsistent legal treatment of data creates confusion and complications. Congress took a large step forward under the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 by removing antiquated and complicated barriers for the sharing of substance use disorder medical history among treating providers, known as "Part 2" data.[18] Prior to passage of the CARES Act, Part 2 data was subject to a higher use and disclosure burden, including requiring written consent to allow patient information to be disclosed. The CARES Act largely aligned the treatment of this data with all other health data within the HIPAA construct, with one exception: it required initial patient consent for that data to enter into the flow of health data among HIPAA-covered entities. Congress should continue in these efforts and ensure a full alignment of all health data within HIPAA.

In 2022, the Biden administration proposed a rule that would enact barriers to sharing certain reproductive health records in response to the Supreme Court's Dobbs v. Jackson Women's Health Organization decision.[19] The administration's intent is to shield abortion providers who offer elective abortion in states where they are illegal and limit the sharing of any "reproductive health" information if used for an investigatory purpose. HIPAA already has guardrails to permit sharing protected health information related to an investigation. For example, a court order, such as a subpoena or a grand jury summons, is generally required in order to obtain identifiable patient information.[20] HIPAA should treat all health data the same and should remain the federal floor for protecting medical records. Treating certain health data differently creates uncertainty and confusion, and could lead to inappropriate withholding and disclosure of health information from providers who need it. HIPAA preempts state law where conflicts exist with HIPAA, and otherwise acts as a federal floor, allowing for more stringent state laws.[21]

Patient Ownership of Health Data

A patient's autonomy over their own health information is one of the most important tools for building trust in the health care system. For patients to have confidence using new digital technologies, they need to have confidence in their autonomy over their health information. Congress needs to clarify how patient health information can and cannot be used for research to give patients this confidence. Generally, researchers are able to use patient health information for research purposes without being subject to the HIPAA Privacy Rule,

---

[17] Letter from Zach Perry to Robinsue Frohboese, Acting Director and Principal Deputy, Office of Civil Rights, U.S. Department of Health and Human Services (May 4, 2021), http://www.regulations.gov/comment/HHS-OCR-2021-0006-1036.

[18] 134 Stat. 281.

[19] Press Release, U.S. Department of Health & Human Services HHS Proposes Measures to Bolster Patient-Provider Confidentiality Around Reproductive Health Care (Apr. 12, 2023), https://www.hhs.gov/about/news/2023/04/12/hhs-proposes-measures-bolster-patient-provider-confidentiality-around-reproductive-health-care.html; Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022)

[20] 42 C.F.R. 164.512 (2004).

[21] 45 C.F.R. 160.202. (2013).

provided that information is de-identified.[22] HHS requires de-identified data to exclude any information that could be used to identify a specific patient, such as name, geographic location, and biometric identifiers.[23] De-identified data has been used for research purposes for over 20 years, helping to create artificial intelligence tools (AI) that improve early detection of cancer and predictive analyses to reduce disparities in care delivery.[24]

As AI continues to develop, robust data will be needed to improve algorithmic determinations, specifically by building datasets that encompass a wide amount of health care information. However, some stakeholders have raised concerns that allowing health information to be used, even though de-identified, in future datasets to build AI tools may undermine patient ownership and autonomy over the use of their health data. Studies have highlighted the potential risk that AI applications may be able to re-identify health information.[25] This would create significant privacy risks and contradict the intent of the HIPAA framework. Congress should examine whether the existing exemptions permitting de-identified data to be used for research should consider a patient's ability to opt-in or opt-out of participation. We must also examine the risk of re-identification to ensure that patient information for research can never be personally identified without explicit consent.

Additionally, Congress should examine whether patients should have the right to be compensated for sharing their identifiable data, a more valuable form of data in dataset and AI tool development. Creating a similar framework to how patients are compensated for clinical trial participation may further encourage information sharing while continuing to emphasize a patient's control over their own data.

Health Data in the HIPAA "Gray Area"

While respondents to the RFI largely felt that the existing HIPAA framework has functioned well to protect PHI, they also shared that there are many gaps between patient and consumer privacy expectations and actual protections in place. There are many different types of health information not explicitly covered by HIPAA, but can have significant privacy and health implications for patients. Congress should legislate to provide clarity for companies and patients to address these "gray areas." These gray areas are: intake services, the removal of health data from HIPAA, patient generated wellness data, sensor generated data, and direct-to-consumer collected genetic data.

Intake Services

American patients are experiencing increasing access to home health care and personalized treatment through explosive growth in the telehealth and virtual care services industries.[26] For many patients, the first step in accessing many of these new virtual platforms is locating the right providers. Digital health companies leverage platforms that facilitate patients filling out intake forms that enable them to be matched with providers to meet their individual needs (i.e., medical specialty, located within a certain state, expertise in treating a particular age demographic). These forms often collect extensive data about a patient's individual medical history, just as a traditional first encounter intake form at an in-person doctor's office. Yet, since the services collecting the medical information are not a HIPAA-covered entity, the information they collect are not protected by HIPAA's

[22] 45 C.F.R. 164.504(a) (2013).
[23] *Id.*
[24] Erin McNemar, Understanding De-Identified Data, How to Use It in Healthcare, HealthITAnalytics (Aug. 27, 2021), https://healthitanalytics.com/news/understanding-de-identified-data-how-to-use-it-in-healthcare#:~:text=What%20is%20De%2DIdentified%20Data,%2C%20medical%20record%20information%2C%20etc.
[25] Preserving Privacy in Artificial Intelligence: Applications through Anonymization of Sensitive Data, Deloitte (Feb. 2022), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte_Trustworthy%20AI%20_Data%20Anonymization_Feb2022.pdf.
[26] Robert Pearl and Brian Wayling, The Telehealth Era Is Just Beginning, Harvard Business Review (May 2022), https://hbr.org/2022/05/the-telehealth-era-is-just-beginning.

regulations.[27]

When a patient fills out an intake form in a doctor's office, that information, collected by the covered entity provider, is protected by HIPAA. This is a confusing inconsistency that reveals gaps in how patient information is collected at initiation of services and an inconsistency not understood by most American patients. Indeed, this inconsistency led to enforcement action in 2023. The Federal Trade Commission (FTC) entered into a settlement with an online mental health company over allegations that the company was sharing certain information, such as whether a potential patient had previously been in therapy, with social media companies to use for targeted advertising.[28] Patients expected their data was protected, as though they were filling out intake forms in their doctors' offices. While HIPAA-covered PHI was not shared in this instance, the case study demonstrates the need for Congress to provide greater clarity by ensuring HIPAA protections include intake information. This would make it clear that this information is always protected and ensure that health information collected through virtual means receives the same level of protection as in-person treatment.

Patient Notification Upon Removal of Health Data from HIPAA

As more patients leverage health data interoperability to access to their medical records (for using new smartphone software applications, smartwatch functionality, and to take advantage of record portability) they authorize their software to download their records through the HIPAA right of access. Unbeknownst to most patients, doing this removes their data from the protections of HIPAA's regulations. Software applications are not HIPAA-covered entities and are thus not obligated to comply with those rules.

However, not all entities with access to data that patients might consider health information should be covered by HIPAA. Respondents raised concerns that covering such entities as HIPAA- covered entities could generate compliance challenges with how it would be included in the current HIPAA framework. It would impose new regulations on non-traditional entities, like big technology companies that develop and maintain these software applications. Instead, many comments supported "HIPAA-like" protections for this data and increased transparency requirements for how it is being used. This would include informing consumers how their HIPAA-covered data could be used as well as considering any opt-ins for using such data for research purposes.

Software applications should provide notifications to users when transferring health information generated under the HIPAA framework from HIPAA-covered entities into environments where those protections would no longer legally apply. Additionally, software applications should provide plain language descriptions in advance of how an individual's data would be collected and shared as well as requiring express patient consent before selling or disclosing their data to third parties.

Patient Notification When They Generate Wellness Data

The proliferation of wellness applications (app) and devices has led to an explosion in the generation of non-HIPAA health data. The rise of wellness applications and devices has created many large databases of consumer health information held by individual companies. Some of these applications are marketed as health applications and generally fall into the category of collecting wellness data (i.e., information about fitness, nutrition, sleep, etc.). A recent study found that 63% of adults in the United States used a mobile health app. Approximately 60%

[27] When Do Online Forms Need To Be HIPAA-Compliant? LuxSci (Aug. 22, 2023), https://luxsci.com/blog/online-forms-hipaa-compliant.html.

[28] Press Release, Federal Trade Commission, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising (Mar. 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook.

of those consumers use those apps on a daily basis.[29] While a broad number of Americans use these products, they generally misunderstand the privacy protections of their data.[30]

Despite consumer expectations, data generated by wellness apps does not typically fall under the HIPAA framework. Patients have the right to use these applications however they choose and Congress should not limit these products without cause. However, patients should be made aware of how their information is being collected and shared by entities who develop these products. Congress should require developers of these products to make clear to consumers that any information generated from using a wellness app is not covered by the HIPAA framework. This information should be clearly delivered to the consumer and allow them to decide whether they are comfortable using a particular wellness app.

Sensor Data

Consumer data is increasingly collected via sensor tools as the use of wearable technology spreads. These technologies include menstruation trackers, step counters, and smart watches with accelerometers and sensors for sudden falls. A 2020 study found that approximately 21% of Americans wear a smartwatch or fitness tracker.[31] This data is also not generally protected under the HIPAA framework or considered PHI. This data can be purchased and used by employers to make inappropriate and discriminatory determinations for hiring, firing, and employee location tracking, based on this data. For example, a smartwatch with a built-in accelerometer that senses trips and falls might be used by an employer to speculate that an employee has an early onset medical condition and deny them certain benefits.

The Stop Marketing And Revealing The Wearables and Trackers Consumer Health (SMARTWATCH) Data Act, which I co-led with Senator Jacky Rosen (D-NV) last Congress included elements that would ensure the collection of informed consent from consumers before their sensor data is sold to data brokers.[32] Congress needs to prevent discrimination of consumers based on collection of this identifiable wellness data, often misunderstood by consumers as data protected by HIPAA.[33]

Genetic Data

Direct-to-consumer (DTC) companies that collect genetic data are not HIPAA-covered entities and thus the genetic data they collect through patient provided samples is not subject to HIPAA protections. Companies that handle this data fall under general FTC regulation by default. Genetic data is contained in all patient samples; it is collected, stored, and can be used to determine a range of health conditions about a patient far beyond the scope of the intended use of the initial sample collection. Respondents to the RFI are concerned that this information is being sold to data brokers and employers who might use it to discriminate against current and prospective employees and other nefarious purposes without meaningful consumer notice or consent and even though employer use for discrimination is against the law. DTC genetic testing companies have also pursued

---

[29] Rajiv Leventhal, Nearly two-thirds of US consumers are mobile health app users, Insider Intelligence (Feb. 21, 2023), https://www.insiderintelligence.com/content/nearly-two-thirds-of-us-consumers-mobile-health-app-users.

[30] Steve Alder, Majority of Americans Believe Health App Data is Covered by HIPAA, The HIPAA Journal (July 26, 2023), https://www.hipaajournal.com/americans-mistakenly-believe-health-app-hipaa/.

[31] Emily Vogels, Research Associate, About one-in-five Americans use a smart watch or fitness tracker, Pew Research Center (Jan. 9, 2020), https://www.pewresearch.org/short-reads/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/.

[32] S.500 - 117th Congress (2021-2022): SMARTWATCH Data Act, S.500, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/500.

[33] Hilary Noonan, As Wearable Health Devices and Apps increase, So Do Consumer Health Data Concerns, Tealium (Mar. 3, 2020), https://tealium.com/blog/data-governance-privacy/as-wearable-health-devices-and-apps-increase-so-too-do-consumer-health-data-concerns/.

partnerships with pharmaceutical companies to share collected information to support drug development.[34] DTC genetic testing companies should be required to disclose to consumers that the genetic data they collect is not subject to HIPAA protections, as they might believe, due to the sensitive nature and health implications of this data. HHS already has experience regulating genetic information through the Genetic Information Nondiscrimination Act (GINA), which prohibits employers or health insurance from using genetic information to discriminate against individuals.[35]

Congress should legislate appropriate notice and consent requirements and safeguards to protect consumers and meet their expectations. Ten states have enacted a model bill as of December 2023 that reiterates a number of principles for the treatment of genetic data, including patient consent for each individual use of their data.[36] These principles are a good place for Congress to begin consideration. Americans deserve greater transparency into how their information is collected and shared and deserve to have more autonomy and control over the disclosures of their genetic information.

A number of DTC genetic testing companies have already voluntarily adopted these principles in their own business activities; expanding them to non-participating entities would create a uniform, predictable framework to protect Americans' genetic data.[37]

Congress should also consider how to expand research protections to genetic data collected by DTC genetic testing entities. This could include implementing certain human subject protections, similar to those in place for research conducted through the Common Rule.[38]

Preemption

Health data does not recognize geographic borders; patients travel across state lines for medical care. As Congress develops privacy legislation we must be mindful of existing state frameworks that govern health data. As of December 2023, 13 states have passed comprehensive data privacy laws, some with health data specific provisions.[39] The federal HIPAA framework serves as a floor for health privacy protections and does not completely preempt state law in this field. We must respect the role of states in crafting their own regulations and also recognize the challenges health care organizations face in complying with 50 different health data privacy frameworks. HIPAA as a federal floor has been a successful model. Ten of the states that have passed data privacy laws fully exempt HIPAA-covered entities from complying with other privacy requirements.[40] Only three states that have passed data privacy laws take a more limited view, instead only exempting information collected under HIPAA rather than exempting the covered entities themselves.[41] Congress should consider a similar model to create a federal floor for health data in the gray area to provide more regulatory certainty but allow states to continue to supplement requirements to meet individual state needs.

---

[34] Press Release, GlaxoSmithKline, GSK and 23andMe sign agreement to leverage genetic insights for the development of novel medicines (July 25, 2018), https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines/.

[35] 122 Stat. 881

[36] U.S. Biometric Laws & Pending Legislation Tracker, Bryan Cave Leighton Paisner (June 2, 2023), https://www.bclplaw.com/en-US/events-insights-news/us-biometric-laws-and-pending-legislation-tracker.html.

[37] Carson Martinez, Privacy Best Practices for Consumer Genetic Testing Services, Future of Privacy Forum (July 31, 2018), https://fpf.org/blog/privacy-best-practices-for-consumer-genetic-testing-services/.

[38] 45 C.F.R. 46.116 (2017).

[39] F. Paul Pittman, US Data Privacy Guide, White & Case (Sept. 20, 2023), https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide#:~:text=Currently%2C%20a%20total%20of%20thirteen,Montana%2C%20Oregon%2C%20and%20Delaware.

[40] Esperance Becton et al., State Privacy Law Roundup: What Health Care Companies Need to Know, SheppardMullin (July 26, 2023), https://www.sheppardhealthlaw.com/2023/07/articles/privacy-and-data-security/state-privacy-law-roundup-what-health-care-companies-need-to-know/.

[41] *Id.*

Enforcement

Creating a robust enforcement framework to safeguard against unauthorized disclosure of health data is essential to build trust in any privacy framework. Currently, OCR has primary enforcement authority over HIPAA violations, such as auditing health care organizations in order to protect HIPAA-covered data and levying fines against health care organizations for noncompliance with the HIPAA regulations. Respondents to the RFI generally stated that working with OCR on enforcement actions has been predictable, though they raised concerns that OCR's interpretations of HIPAA have not kept up with a more digitized health care system. Congress should examine specific areas where OCR's guidance has been insufficient and needs updating.

While OCR has primary authority over regulating health data, the Federal Trade Commission (FTC) has taken an increasingly active role in regulating health entities as well. FTC has used its authority under the Health Breach Notification Rule that requires health care entities not covered by HIPAA to report breaches of electronic health information.[42] However, since the rule was finalized in 2010, it has only been used twice to levy penalties on health care entities.[43] More recently, FTC has sought to expand the scope of this rule to include a wider universe of information, including, "any online service… that provides other health-related services or tools."[44] While FTC's mandate is to pursue claims of unfair or deceptive acts or practices, this expansive enforcement framework creates uncertainty by requiring duplicative reporting and compliance with both FTC and OCR requirements. Congress should consider how to best balance this enforcement framework and continue to recognize OCR as the primary enforcement body over health data.

Data Outside of HIPAA

What is health information? Much data generated by Americans outside of the health care setting may have implications on individual health and privacy. This information includes geolocation data (did you visit an HIV clinic or an opioid treatment facility?), financial data (did you spend a lot of money at the pharmacy or at fast food restaurants?), internet searches (did you look up how to quit smoking?), and biometric data (did you sign up for expedited security at the airport by having your eyes scanned?). These types of data face the legal "wild west" treatment in the United States. Congress needs to act. Yet, we cannot subject these types of data to many sets of rules as each sector may see fit. We need comprehensive data privacy reform.

In this vacuum, many bodies are attempting to regulate these types of data. Ten states have their own data privacy laws and various federal agencies initiate enforcement actions and release proposals for regulating such data. OCR recently proposed ways to regulate some of this data under its umbrella to enforce health privacy, treating some information with a higher degree of sensitivity and imposing greater protections over it. This is a dangerous path to take.

These proposals would be unworkable and risk creating a tiered system of protecting certain types of health data more than others. This data can also be used for non-health purposes, including for national security, and should be generally regulated by non-health authorities, like the FTC. We cannot risk exacerbating the patchwork of privacy laws in the United States. Senate committees of jurisdiction should tackle this problem promptly, taking care to account for health privacy equities formulating their own general data privacy proposals. The HELP Committee stands ready to partner to tackle these complicated matters.

---

[42] 16 C.F.R. 318 (2009)

[43] Press Release, Federal Trade Commission, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), 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?utm_source=govdelivery.

[44] Health Breach Notification Rule, 88 Fed. Reg. 37819 (proposed June 9, 2023) (to be codified at 16 C.F.R. pt. 318).

Postscript on Interoperability

It cannot go without saying that advancements have been made in health data interoperability as the realization of the health technology provisions of the 21st Century Cures Act of 2016 continues. While this paper does not specifically address health data interoperability, protecting health data goes hand in hand with promoting interoperability. As health care organizations become more interoperable with one another, the risk of inappropriate data disclosures increases as more entities have access to patient information. Indeed, regulations issued by the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) have recognized the importance of data privacy in supporting interoperability.[45] ONC National Coordinator Micky Tripathi has specifically pointed to the importance of privacy, raising it as one of the top challenges to improving information sharing.[46] Creating a health data privacy framework will encourage further interoperability and create a framework that balances data access with privacy and safety concerns. Congress needs to create guardrails around how health data not covered by HIPAA is shared to ensure interoperability does not sacrifice patient privacy and create a more sustainable framework for future information sharing.

[45] Dan Goldstein and Kamal Govindaswamy, Health care interoperability: Preparing to meet new privacy and security obligations, International Association of Privacy Professionals, Aug. 25, 2020, https://iapp.org/news/a/health-care-interoperability-preparing-to-meet-new-privacy-and-security-obligations/.

[46] Ben Leonard, Reports of the fax machine's death are greatly exaggerated, Politico, Apr. 27, 2022, https://www.politico.com/newsletters/future-pulse/2022/04/27/reports-of-the-fax-machines-death-are-greatly-exaggerated-00027923.