October 23, 2023

Senator Bill Cassidy, M.D.
Ranking Member
Senate HELP Committee
Washington, DC 20510

Dear Ranking Member Cassidy:

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to provide feedback on your health data privacy request for information (RFI) that was released on September 7, 2023.

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders in hospitals, health systems and other healthcare settings across the country. Consisting of 2,850 members in 60 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 950 healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

Our members are committed and have a legal obligation to protect and secure patient information with which they have been entrusted pursuant to the Health Insurance Portability Accountability Act (HIPAA) and they take this responsibility very seriously. Similarly, patients expect and trust their healthcare providers to keep their information private.

Responses

CHIME has long expressed concerns about the treatment of health data held by entities not governed by HIPAA and appreciates the Senate HELP Committees' interest in this topic given the proliferation of third-party applications (apps) and growing use of generative artificial intelligence (AI), a type of AI capable of generating text, images and other forms of media.

General Privacy Questions

What is health data? Is health data only data governed by HIPAA, or are there other types of health data not governed by HIPAA? Should different types of health data be treated differently? If so, which? How? If not, why not?

Under HIPAA, there are eighteen pieces of information[1] that, when not de-identified are considered protected health information (PHI). Health data is essential for healthcare providers to care for patients. The vast amount of data used in healthcare organizations to care for patients continues to expand. It is crucial to handle this data with care and respect individuals' privacy and confidentiality.

From our perspective, most data can be considered health data in light of the fact that the aggregation of enough data points can pinpoint an individual. This becomes especially true once you have Global Positioning System (GPS) location data. A 2019 New York Times article[2] had this to say about location data:

> *Every minute of every day, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files.*
>
> *"D.N.A….is probably the only thing that's harder to anonymize than precise geolocation information."*
>
> *Location data is also collected and shared alongside a mobile advertising ID, a supposedly anonymous identifier about 30 digits long that allows advertisers and other businesses to tie activity together across apps. The ID is also used to combine location trails with other information like your name, home address, email, phone number or even an identifier tied to your Wi-Fi network.*
>
> *The data can change hands in almost real time, so fast that your location could be transferred from your smartphone to the app's servers and exported to third parties in milliseconds. This is how, for example, you might see an ad for a new car some time after walking through a dealership.*

[1] Names; all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code; all elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met.

[2] One Nation, Tracked, New York Times, December 19, 2019.

That data can then be resold, copied, pirated and abused. There's no way you can ever retrieve it.

Which entities outside of HIPAA Covered Entities should be accountable for the handling of health data (not necessarily HIPAA-covered data)? Should different types of entities have different obligations and privileges? Please explain using examples.

CHIME has long expressed concerns about the treatment of health data that is held and stored by entities not governed by HIPAA. We believe that entities outside of those currently regulated under HIPAA should absolutely be held accountable for the handling of health data. There is often a false sense of security among consumers that their health data is protected under HIPAA by the mere assumption that since it is health data it is protected, when in fact that is not the case. Once health data – including PHI – is shared willingly or without a consumer's knowledge with entities outside of HIPAA – these protections end.

Too many entities not governed by HIPAA are using health data in ways never envisioned or understood by consumers, and in many instances doing so without their consent or knowledge. A recent estimate by IQVIA Institute for Human Data Science[3] pegged the number of health-related apps at 350,000. Given the explosion in mobile apps and data aggregation practices, it is not only entirely plausible, but likely, that the amount of health data held by entities who are not required to comply with HIPAA exceeds the data held by those who are covered entities (CEs) under HIPAA.

In terms of whether there should be different obligations and responsibilities for entities handling health data, with the rapidly emerging field of generative AI, and the catastrophic implications for consumer privacy, the short answer is yes. It is imperative that Congress adopt a national data privacy law to bring much-needed order to the chaos around the unregulated use of consumer information. Oversight of the use of non-HIPAA entities' handling of health and "wellness" data (e.g. a mobile app that tracks fertility or sleep) should continue to be overseen by the Federal Trade Commission (FTC).

Should any or all of these entities have a duty of loyalty to consumers/patients?

The resounding answer is yes. Non-HIPAA regulated entities should be bound by a duty to responsibly handle consumer data. Products that touch, collect and have any type of access to health and wellness data should be developed with privacy-by-design and security-by-design principles at the outset.

Consumers have little leverage or awareness – if any – when it comes to how their data is being used. We need to return a greater level of control to consumers, so they have a say in the way their data is handled, processed, protected and sold. Furthermore, even when consumer privacy policies exist, the average privacy policy is lengthy and full of legal jargon that is difficult for most American consumers to understand.

[3] Murray Aitken & Deanna Nass. (2021, July). Digital Health Trends 2021: Innovation, Evidence, Regulation, And Adoption. In https://www.iqvia.com

An opinion piece in the New York Times concluded[4]:

> *The vast majority of these privacy policies exceed the college reading level. And according to the most recent literacy survey conducted by the National Center for Education Statistics, over half of Americans may struggle to comprehend dense, lengthy texts. That means a significant chunk of the data collection economy is based on consenting to complicated documents that many Americans can't understand.*

We recently reviewed the terms and conditions of a child's wearable sold by a phone carrier and learned that the carrier placed certain limits and restrictions on the way the child's data is used in the wearable's privacy policy. However, it becomes clear that data is being shared with a variety of third parties when the wearable is tied to an adult's (i.e., parent's) account. Thus, it is very confusing about where child data protections start and adult data sharing ends. Since wearables and smart phones contain GPS tracking, aggregating a few data points together with GPS results in the ability to ascertain identity. It thus becomes clear how important GPS data is when establishing what has been referred to as a digital fingerprint.

Health Information Under HIPAA

How well is the HIPAA framework working? What could be improved?

HIPAA rules have been in place for nearly three decades and healthcare providers have spent significant time and resources learning and complying with them. As with any law, there are certain entities that may not follow the rules or utilize "gray areas" to their advantage – sometimes to the detriment of our healthcare system. For years, our members have reported to us that they experience challenges with some medical device manufacturers refusing to sign business associate agreements (BAAs). Our members, as HIPAA-covered entities, are required to enter into BAAs with any third-party that handles PHI. Some of these medical devices contain PHI, and/or provide the manufacturers with access to PHI. Providers come to the "bargaining table" as the underdog and often find their requests to have business associates sign BAAs flatly turned down.

We are grateful Congress passed the PATCH Act last year[5] – legislation supported by CHIME – under your leadership. This important legislation gave the Food and Drug Administration (FDA) greater authority to regulate the cybersecurity components of medical devices. However, we remain concerned that unless all device manufacturers are fully fulfilling their obligations as BAAs under HIPAA, the burden, cost, and reputational damages that result from breaches will continue to fall solely on our members.

[4] We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, Opinion, New York Times, June 13, 2019

[5] The Protecting and Transforming Cyber Health Care Act of 2022 (PATCH Act) was signed into law on December 29, 2022 as a part of the 2023 Consolidated Appropriations Act.

Another area related to HIPAA oversight that merits additional attention concerns online tracking technologies. Recently, HHS' Office for Civil Rights (OCR) and the FTC[6] have taken the position of telling hospitals that even when a consumer - who may not even be an existing patient – accesses their website, this could violate HIPAA if the data is shared with data analytics companies in the absence of a BAA. If there is to be a more equitable distribution of responsibility handling patient data involving internet services and analytics companies, we believe they must be explicitly required to sign BAAs with providers. While we recognize that healthcare organizations must take a more proactive role in ensuring they are in full compliance with HIPAA related to patient data released as a result of using a healthcare organization's website(s), this too must be a shared responsibility. OCR should also recognize that healthcare organizations have no control over internet service providers. Even when a healthcare organization turns off all trackers, they still need an internet hosting site.

When making any potential changes to HIPAA, there must be a joint responsibility across stakeholders throughout the entire ecosystem of healthcare – not simply a subset. Otherwise, it inadvertently shifts more burden onto providers, many of which are already severely strained, understaffed, and under-resourced.

Should Congress update HIPAA?

HIPAA was created to ensure the appropriate sharing of healthcare information within the healthcare system. Rather than trying to exert significant changes to HIPAA, we believe Congress should consider alternative approaches, such as:

- Implementing a national data privacy law. As stated in a stakeholder letter sent to Senate Commerce, Science, and Transportation and House Energy and Commerce leadership in January, "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."

- Adequately funding the FTC. The FTC is the primary federal agency responsible for protecting consumers' privacy and security and their funding should not be predicated on the passage of a national privacy law. The Commission's Health Breach Notification Rule (HBN Rule) requires vendors of personal health records ("PHRs") and related entities that are not covered by HIPAA to notify individuals, the FTC, and, in some

[6] Assistant Secretary for Public Affairs (ASPA). (2023, July 31). HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies. *HHS.gov*. https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html

cases, the media of a breach of unsecured personally identifiable health data. CHIME's response strongly supporting the FTC's Notice of Proposed Rulemaking (NPRM)[7] to amend the HBN Rule can be found here. Our comments noted that, as many Americans turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas, this Rule is more important than ever. Consumers as patients can use both mobile medical apps and mobile apps to manage their own health and wellness, such as to monitor their caloric intake for healthy weight maintenance, while other apps are created to help healthcare providers improve and facilitate patient care.[8] Entities not covered by HIPAA offering these services should take appropriate care to secure and protect consumer data.

CHIME believes it is time vendors of PHR and PHR-related entities with lax data security – and sometimes blatant disregard of the law – continue to be reminded of their ongoing obligation to be transparent about breaches and unauthorized disclosures under the Rule. Further, under FTC's HBN policies the FTC not only holds bad and unsecure actors accountable, but it also creates a disincentive that urges all businesses with PHR and PHR-related entities to strengthen their data security practices. Adequate funding of the FTC will provide the much-needed staff and resources to fully investigate and enforce those that violate the HBN Rule.

- Enforcing HIPAA: Enhancing the enforcement of HIPAA such that there is more shared responsibility around privacy and security and not a unilateral burden on healthcare providers.

What challenges would legislative reforms to HIPAA create?

Any future changes to federal laws and regulations – especially those that have been in place for as long as HIPAA has been – must not be overly burdensome for providers and every precaution should be taken to ensure that existing regulations and mandates are not duplicative.

How should the sharing of health data across state lines be structured to account for different legal frameworks?

CHIME supports federal preemption of state law when it comes to HIPAA. As Congress considers a national privacy law, we believe federal preemption will bring certainty to the marketplace, reduce administrative burdens, foster better and appropriate information sharing, and reduce confusion.

Collection of Health Data

[7] *Health Breach Notification rule*. (2023, June 9). Federal Register. https://www.federalregister.gov/d/2023-12148
[8] Device Software Functions Including Mobile Medical Applications. (2022, September 29). U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobile-medical-applications

How should consumer/patient consent to an entity to collect information be structured to minimize unnecessary data gathering? When should consent be required and where should it be implied?

CHIME has long expressed concerns about the treatment of health data by entities not governed by HIPAA. The regulatory oversight framework governing those covered by HIPAA and those who are not has created a separate and parallel but unequal universe which is at the heart of the privacy debate in healthcare. Most patients-turned-consumers are completely unaware of how an app or a website intends to use their data, and many are under the false assumption that their data will continue to be safeguarded under HIPAA. Our members take the protection of their patient's healthcare data seriously regarding it not only as a legal obligation, but their mission. Maintaining the privacy and security of patient data is crucial for maintaining trust in the patient-provider relationship; ensuring that patient data remains safe even when they are outside of the four walls of the hospital or other healthcare setting only helps strengthen that bond.

The FTC has also proposed to amend the definition of "breach of security" under the HBN Rule by adding the following sentence to the end of the existing definition: "A breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach ***or an unauthorized disclosure*** [emphasis added]."

The proposed definition is intended to make it clear to the marketplace that a breach includes an unauthorized acquisition of identifiable health information that occurs as a result of a data breach or an unauthorized disclosure, such as a voluntary disclosure made by the PHR vendor or PHR related entity where such disclosure was not authorized by the consumer. CHIME continues to strongly support these proposals – and believes that any federal legislation should align with these policies.

CHIME believes that there is more that can be done before a consumer's data is sold or a breach happens, and we encourage Congress to consider these options – including supporting the FTC's enforcement of real-world and stringent privacy and security protections on companies to better protect consumer data. That includes making sure consumers understand what they are agreeing to prior to using a company's technology. CHIME believes the use of plain language for consumers is crucial when it comes to meaningful consent. For instance, consumers should be able to easily ascertain whether an entity is selling their data or using it for marketing purposes, and if they choose, opt-out of their data being used.

How should information about data collection practices be conveyed to patients (i.e. plain language notice prior to consent, etc.)?

As referenced earlier, plain language must be used to communicate complex legal policies so that most consumers understand how their data is being treated. According to the AHRQ Health Literacy Universal Precautions Toolkit, "The average adult reads at the 8th or 9th grade level, and 20% read at the 5th grade level or below. Therefore, to ensure wide understanding, it is

best for materials to be written at the 5th or 6th grade level."[9] The Centers for Medicare & Medicaid Services (CMS) has guidelines for effective writing[10] and Medicare requires their contractors to draft language at the 8th grade reading level.[11] We believe that these are helpful starting points.

The European Union (EU) General Data Protection Regulation (GDPR) requires entities that collect personal data to delete it under certain circumstances if a consumer makes such a request. Should non-HIPAA covered entities be required to delete certain data at a consumer/patient's request?

Where practicable, legislation should require non-HIPAA covered entities to provide individuals with the ability to amend incorrect information. Furthermore, consumers should have the option that if they choose to delete their account (e.g., in an app or on a website), they should have the choice to permanently delete any related information, and this information should not be retained.

How should consumer online searches about health conditions (i.e., diabetes, in-vitro fertilization) be considered when part of health data?

When a consumer searches for information regarding health conditions online, their search history can include health data. Congress could protect this information under a national privacy law. According to a 2017 CNN article[12], "Your browser history is for sale, here's what you need to know," it states:

> *Many have said they will not use "sensitive" information, like medical records, children's data and banking details without consent. However a simple browsing history can reveal those personal details, such as symptoms... There are concerns that it would be possible to identify people based on this detailed information.... an internet provider can infer a lot about you based just on your browsing. In addition to basics like age and gender, they might know who your friends are, if you're a recovering alcoholic, or where you went to school. In theory, they could create an in-depth profile of you*.

As one of only a handful of federal privacy laws protecting consumers' health information, the FTC's HBN Rule plays a vital role in holding companies accountable for how they disclose consumers' sensitive health information. As previously mentioned, CHIME supports the FTC's proposed revisions to several definitions in order to clarify the HBN Rule and better explain its application to health apps and similar technologies not covered by HIPAA. Since FTC has called for regulating websites for non-HIPAA covered entities, additional guidance will be needed from

[9] AHRQ Health Literacy Universal Precautions Toolkit, 2nd Edition
[10] Guidelines for effective writing | CMS
[11] 419_A2.PDF (cms.gov)
[12] https://money.cnn.com/2017/04/05/technology/online-privacy-faq/#:~:text=It's%20official%3A%20Your%20browsing%20history,before%20selling%20your%20browsing%20history.

OCR to better explain where a provider's responsibilities end, and a non-HIPAA covered entity's begin.

Genetic Information

How should genetic information collected by commercial services be safeguarded?

Genetic information collected by any commercial service should be safeguarded to the same standard that any health and wellness data should be – including requiring the companies that collect it to develop privacy-by-design and security-by-design principles at the outset. If they do not have privacy and security standards in place, they should be required to.

Further, sharing genetic data with hostile nation states should be prohibited since it is contrary to national security. The Director of National Intelligence has flagged this as a significant security issue in a 2020 bulletin.[13] FBI Supervisory Special Agent in the FBI's Weapons of Mass Destruction Directorate, Edward You, has addressed this issue at length and was featured on 60 Minutes in 2021 discussing the significant issues surrounding sharing genetic data with China.[14]

Sharing of Health Data

HIPAA permits the sharing of protected health information (PHI) under limited circumstances, provided the information is deidentified. Should this permissive framework be extended to the sharing of non-HIPAA covered data and what guardrails should be imposed?

We again reiterate our comments regarding the FTC's HBN Rule and our comment letter regarding the proposed amended changes. Transparency for consumers around how data is being shared and the possibility for re-identification should be communicated clearly and concisely to consumers.

State and International Privacy Frameworks

Nine states have passed data or privacy laws since 2018. What have been the greatest challenges in complying with these frameworks for the governance of health data? Have there been any lessons learned as states have implemented these laws on best practices to safeguard health data? How should the federal government proceed, considering the existing state patchwork?

CHIME supports a national data privacy law. Our members must wrestle today not only with changing and burgeoning state privacy laws but also with state laws pertaining to health data. This adds further complexity to the process of sharing this health data and children's health data

[13] No_1_FINAL_NCSC_Safeguarding_our_future-DNA27_May_2020.pdf (dni.gov)

[14] https://www.cbsnews.com/video/us-officials-tell-60-minutes-that-china-is-trying-to-collect-americans-dna/

across state lines. Varying sets of state laws present complexity, burden and added costs to the healthcare system.

Enforcement

OCR has primary authority over enforcement of HIPAA. However, other federal agencies such as the Federal Trade Commission (FTC) have oversight of certain health data that can implicate HIPAA. To what extent should these agencies have a role in the safeguarding of health data? What duplication or conflict currently exists between how different agencies enforce violations of health laws?

As noted above, we do not believe healthcare organizations should be saddled with navigating the complex landscape that is website tracking and pixel use. This must be the responsibility of those companies that are implementing these technologies. We believe there is a need for OCR to provide additional guidance, and time for compliance related to utilization of analytics and online tracking technologies. Currently, providers are being penalized without full clarity on this issue. It is crucial to establish this guidance without placing the full responsibility on organizations already governed by HIPAA. Entities not currently under HIPAA's umbrella, such as online tracking technology companies, should fall under the forthcoming definition proposed in the FTC's HBN Rule upon its finalization.

Please share challenges with compliance and enforcement of existing health data privacy and general data privacy laws. How should these challenges be overcome?

As noted above, the complexity of various state laws is staggering.

Conclusion

CHIME appreciates the opportunity to help inform the important work being done by the Senate HELP Committee. Should you have questions about our position or if you would like to speak directly to one of our members with expertise in health data privacy, please contact Mari Savickis, VP of Public Policy, at mari.savickis@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME