April 7, 2025

Chairman Brett Guthrie
Vice Chairman John Joyce, M.D.
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Guthrie and Vice Chairman Joyce:

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to provide feedback on the data privacy working group's request for information (RFI) that was released on February 21, 2025.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs) and other senior healthcare IT leaders. With more than 3,000 individual members in 58 countries and two U.S. territories and 200 CHIME Foundation healthcare IT business and professional service firm members, CHIME and its three associations provide a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate, exchange best practices, address professional development needs, and advocate for the effective use of information management to improve the health and care in the communities they serve.

Executive Summary

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

As the working group explores the parameters of a federal comprehensive data privacy and security framework, CHIME's top recommendations are:

- **Comprehensive National Data Privacy Law**: The U.S. needs a comprehensive national data privacy law to better protect consumers' sensitive health information and inform consumers of how their data is being used without duplicating what is already required under HIPAA. Varying sets of state laws present complexity, burden and added costs to the healthcare system.
- **Accountability for Non-HIPAA Covered Entities**: Entities outside of those currently regulated under HIPAA should 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 is shared willingly or without a consumer's knowledge with entities outside of HIPAA, these protections end.

Comprehensive National Data Privacy Law

CHIME supports a comprehensive 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 across state lines. Varying sets of state laws present complexity, burden and added costs to the healthcare system. According to the International Association of Privacy Professionals (IAPP), 19 states have signed comprehensive consumer privacy bills into law, while nearly a dozen more are actively considering similar legislation.[1]

As stated in a stakeholder letter sent to Senate Commerce, Science, and Transportation and House Energy and Commerce leadership, "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."

Accountability for Non-HIPAA Covered Entities

Non-HIPAA entities often handle healthcare data. CHIME has long expressed concerns about the treatment of health data that is held and stored by entities that are 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.

HIPAA applies to covered entities (CEs) and business associates (BAs). HIPAA covered entities include healthcare providers (i.e. CHIME members), health plans, and healthcare clearinghouses. CEs must "comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information."[2] A CE may enter into a contract with a BA to assist in performing healthcare functions, with the BA being subject to certain provisions under HIPAA. A BA could be a medical device service provider or a cloud-based software provider, for example. If an entity does not meet the definition of a CE or a BA, it does not have to comply with HIPAA, creating a significant gap in privacy protections. A prime example is the vast majority of consumer health apps, which fall outside of HIPAA's scope. According to the IQVIA Institute for Human Data Science's Digital Health Trends 2024 Report, there are approximately 337,000 health-related apps in use today.[3] Examples of these are apps and technologies that track disease, fitness, fertility, mental health, and weight loss, to name a few. Direct to consumer

[1] https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
[2] Covered Entities and Business Associates | HHS.gov
[3] Digital Health Trends 2024 - IQVIA

genetic testing companies, like 23andMe, are also not covered by HIPAA because they are not a CE. Once health data – including protected health information (PHI) – is shared willingly or without a consumer's knowledge with apps or genetic testing companies – these protections end. This is particularly alarming in the case of 23andMe because the company is filing for bankruptcy with the goal of finding a buyer. This raises serious concerns about what will happen with the sensitive data of millions of consumers.

The other issue is when a third-party refuses to sign what is known as a business associate agreement (BAA) despite handling health data. A BAA is a contract between a CE and a BA that outlines each party's responsibilities when it comes to safeguarding PHI. For years, our members have reported to us that they experience challenges with some vendors like medical device manufacturers refusing to sign BAAs, a situation that is only going to grow as providers begin relying more heavily on artificial intelligence (AI) tools. 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 or met with resistance resulting in less than favorable terms for their providers.

We are grateful Congress passed the Protecting and Transforming Cyber Healthcare (PATCH) Act. 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 completely fulfilling their obligations as BAs under HIPAA, the burden, cost, and reputational damages that result from breaches will continue to fall solely on our members. A report from Black Kite found that the healthcare industry remains the top target for third-party breaches, accounting for 41.2% of third-party breaches.[4] It is imperative that providers have confidence that the data held and/or is accessible to medical device manufacturers remains secure.

Conclusion

In conclusion, a national data privacy law is needed in the U.S. to better protect consumers' sensitive health information. In addition, non-HIPAA regulated entities that handle health data 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.

[4] https://www.hipaajournal.com/41pc-2024-third-party-breaches-affected-healthcare-organizations/

CHIME appreciates the chance to help inform the important work being done by the working group. We look forward to continuing to be a trusted stakeholder and resource to the Committee and continuing to deepen the long-standing relationship we have shared.

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 Cassie Ballard, Director of Congressional Affairs, at cballard@chimecentral.org.

Sincerely,

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