Consumer
Technology
Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

October 3, 2023

The Honorable Bill Cassidy, MD
Ranking Member
Senate Health, Education, Labor & Pensions Committee
428 Dirksen Senate Office Building
Washington, DC 20510

Dear Ranking Member Cassidy:

Thank you for your leadership and opportunity to respond to questions regarding health data privacy. As a trade organization that represents both covered and non-covered entities under the *Health Insurance Portability and Accountability Act* (HIPAA), this issue is a top priority.

As North America's largest technology trade association, the Consumer Technology Association (CTA®) is the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the most influential tech event in the world. CTA is the trade association representing the more than 1000 companies in the U.S. technology industry. Eighty percent of CTA companies are small businesses and startups; others are among the world's best-known brands. We provide members with policy advocacy, market research, technical education and standards development.

CTA's Health Division strives to advance the use of consumer-based technology enabled health solutions to deliver better health outcomes and reduce overall healthcare costs. The Division, which includes some of the most well-respected thought leaders in the healthcare and technology sectors, provides policy advocacy, healthcare market research, and standards initiatives that advance the appropriate use of consumer technologies in the healthcare context.

Unlike most trade associations, CTA is accredited by the American National Standards Institute (ANSI) as a Standards Development Organization (SDO), and we have a long history of voluntary national standards development. Among the wide range of topics addressed by our standards program are mobile health, digital therapeutics, cardiovascular technology solutions and artificial intelligence.

Health data and privacy and security are continually evolving concepts that require a dialogue among technology stakeholders, healthcare providers, patients and regulators—given how quickly technology is advancing. As patient preferences and comfort with technology evolve, so too will products and services. Innovative technologies like artificial intelligence (AI) and machine learning continue to transform health care and the ways in which clinicians and patients use data to improve care coordination, diagnostic accuracy, and quality of care. Consumers increasingly want to be active participants in their own care and want to able to monitor their health and wellness, and share their data with health care providers, applications, caregivers and family members.

CTA believes that collaboration among the health care sector, technology stakeholders and consumers can help drive better patient care and facilitate better coordination. The collection and sharing of health information is critical to improving the quality and safety of health care and advancing health care innovation that can improve the health and wellbeing of consumers. That said, CTA recognizes legitimate consumer concerns regarding the privacy of their personal health data.

General Comments

In 2015, CTA released *Guiding Principles for the Privacy of Personal Health Data* (Guiding Principles). The Guiding Principles were developed, and subsequently updated three times, by a workgroup that included technology companies, telehealth and remote patient monitoring companies, health care providers, commercial payers and other innovators. Intended to be baseline recommendation, the Guiding Principles outline five main voluntary principles recommended for companies to follow:

1. Be open and transparent about the personal health data you collect and why.
    a. Includes recommendations to use clear, concise, and easy to understand language in privacy notices.
2. Be careful about how you use personal health data.
    a. Includes recommendations to allow consumers to withdraw their consent.
    b. Includes recommendations to obtain consent or have a robust opt-in system for the use of personal health data and other personally identifiable information involving third parties.
3. Make it easy for consumers to access and control the sharing of their personal health data and empower them to do so.
4. Build strong security into your technology.
5. Be accountable for your practices and promises.

While we recognize voluntary industry guidelines and standards play an important role, CTA urges Congress to pass a comprehensive and preemptive federal data privacy bill that protects consumers and promotes innovation without incentivizing frivolous lawsuits and creating a patchwork of state privacy laws. In September 2022, CTA President & CEO Gary Shapiro stated that passing a comprehensive, bipartisan privacy bill is the most important action Congress could take on tech this session.[1]

Specific Responses

General Privacy Questions

1. *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?*

Recognizing the need for industry consensus and guidance in this area, CTA released the Guiding Principles. These voluntary consensus-based principles were developed by a working group of CTA

[1] https://www.protocol.com/braintrust/congress-most-important-tech-actions

member organizations reflecting the broader health, payer, and technology ecosystems. In the principles, health data is defined as “any data collected through personal health applications, monitoring devices, websites, and other digital or online tools that specifically relates to a consumer’s health. Personal health data can refer to demographic information (such as a consumer’s age, gender, and ethnicity), fitness information (such as a consumer’s exercise activities or fitness abilities), and medical information (such as medical history, genomic data, vital signs, height, weight, and other physiologic parameters, and patient-reported outcomes).” Given this definition, health data does not just refer to data held by HIPAA covered entities. Such a broad definition reflects how pervasive data related to health has become and the fact that such data is held and transmitted by many organizations outside traditional health care organizations.

3. *Should any or all of these entities have a duty of loyalty to consumers/patients?*
    a. *How could a duty of loyalty be imposed in a way that maximizes the safeguarding of consumer/patient data without creating burdensome implementation challenges? Should requirements of such a duty be based on the sensitivity of collected data? Please explain.*

While CTA supports a comprehensive national privacy law to provide important consumer protection while allowing for innovation, the issues raised in this question can be addressed through voluntary industry consensus-based standards and voluntary industry guidelines, such as CTA’s *Guiding Principles for the Privacy of Personal Health Data* (Guiding Principles). Voluntary industry standards and guidelines are nimbler and can be more reactive to needs in the marketplace than statute or regulations.

For example, CTA’s Guiding Principles suggests “[w]hile use of personal health data can provide you and your consumers with many benefits, you should guard against the possibility that such use could infringe on the privacy rights of consumers. You should use personal health data in ways that consumers would expect you to use it (given the anticipated purpose of the collection) and have requirements and safeguards in place to provide that all who process that personal health data abide by those same expectations.”[2]

Health Information Under HIPAA

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

As previously stated, CTA recognizes there is an increasing amount of health data that is held by non-HIPAA covered entities. For these entities, it is often unclear which privacy laws apply and when. The Federal Trade Commission (FTC) has recently taken actions against non-HIPAA covered health companies using their authority to prohibit deceptive or unfair acts or practices. More recently, the FTC has also proposed changes to the Health Breach Notification Rule that, if finalized, would significantly widen their enforcement authority over companies who hold health data. CTA submitted comments on this proposed rule stating that the proposed changes stretch far beyond the original intent of the statute.[3] To improve this ambiguity in the underlying law, CTA supports a comprehensive federal national privacy law.

[2] https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf

[3] https://cdn.cta.tech/cta/media/media/pdfs/health-breach-notification-rule-nprm-comments-8-8-23.pdf?_gl=1*40kyd9*_ga*MjA1NzY5MDM4My4xNjc4ODkxMDk5*_ga_5P7N8TBME7*MTY5NTc0MTI3OC42OC4wLjE2OTU3NDEyNzguNjAuMC4w&_ga=2.197402031.1497801927.1695646319-2057690383.1678891099

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

CTA believes an important component of a comprehensive federal data privacy law is federal preemption of state privacy laws. CTA advocates for a uniform, technology-neutral, national standard. Consistent protections across technologies, companies, agencies, and state borders are the bedrock prerequisite to ensure consumer trust, continue data-driven innovation, and realize its benefits. A preemptive federal privacy law is the most effective way to achieve such consistency. Further, such a bill should ensure consumers are granted the same protections across the nation. A bill that merely sets one standard and allows states to add different requirements on top of it will lead to both confusion and disparity for consumers. A state-centric approach simply doesn't work in a digital economy, where data flows across borders in a matter of seconds. These laws create compliance costs for business (especially small businesses) and confusion for consumers.

Collection of Health Data

1. *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?*

CTA's Guiding Principles recommend that companies "[m]inimize the personal health data you collect, use and disclose. [Companies] can use techniques such as anonymization or de-identification to minimize the privacy impact your practices have on consumers."

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

CTA's Guiding Principles state that "[c]onsent should be a clear affirmative act that signifies a freely given specific, informed, and unambiguous indication of a consumer's agreement, such as a written statement, checking a box, or other clear, affirmative action."

3. *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?*

CTA's Guiding Principles recognize that consumers now expect the right to withdraw consent and the right to be forgotten when it pertains to identifiable personal health information (versus deidentified). The Guiding Principles recommend that companies "[a]llow consumers to withdraw their consent or opt-in and ensure the process to withdraw is easy to understand and execute."

Sharing of Health Data

1. *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?*

Yes, CTA supports extending this framework of permissive sharing of deidentified information. This is critical to ongoing medical research and medical innovation.

4. *What, if any, framework should be imposed on third parties who use third-party data sources to supplement HIPAA data to uncover an individual's health condition(s)?*

Regarding third parties use of personal health data, CTA's Guiding Principles recommend companies:

- Obtain consent or have a robust opt-in system for the use of personal health data and other personally identifiable information involving third parties.
- Be descriptive and clear about the purpose for which you are collecting, storing and using personal health data. Any activities not included in this description will be considered a secondary purpose.
- Use personal health data only for the purpose(s) for which you collected it. If you want to use personal health data for a secondary purpose, make sure that the secondary purpose is consistent with the initial purpose, or otherwise ensure that the consumer opts into the use of their personal health data for the secondary purpose; or ensure the secondary use occurs under another available pathway under applicable law.

Artificial Intelligence

1. *What privacy challenges and benefits does the use of artificial intelligence pose for entities that collect, maintain, or disclose health care data, whether within the HIPAA framework or without?*

Artificial Intelligence (AI) provides the ability to generate and aggregate meaningful datasets from disparate sources and create algorithms that enable machine learning, data analysis, and decision making based on the datasets collected to make predictions in real time that will greatly enhance patient health care by, among other things, providing new ways to diagnose, treat, or even prevent disease. With respect to AI, HIPAA recognizes that deidentified patient data should be made available for use in research and development without restriction, provided that entities receiving and using the data do not reidentify or attempt to reidentify the individuals whose deidentified data has been shared. AI has the potential to significantly improve the ability to anonymize or deidentify health data while preserving critical attributes for decision making by using algorithmic techniques such as privacy-preserving record linkages. Future frameworks should recognize these existing privacy protections and encourage sharing of deidentified data to further develop AI based healthcare models.

2. *How should artificial intelligence-enabled software and applications implement privacy by design? What can be done to mitigate privacy vulnerabilities when developing algorithms for health care purposes?*

CTA's Guiding Principles recommend that companies:

- If using algorithms or automated solutions to assist in human care decisions, provide a clear description of what is being predicted and what is the expected output of the algorithm or automated solution.

- Should comply with responsible AI practices (such as *The Use of Artificial Intelligence in Health Care: Trustworthiness ANSI/CTA-2090*[4])
- Periodically review algorithms and automated decisions to confirm that they are applied fairly and without prejudice to certain classes of consumers.

3. *To what extent should patients be able to opt-out of datasets used to inform algorithmic development? How could an opt-out mechanism be structured?*

Providing patients with clear and specific information on how their personal health information is used, shared, stored, and managed will promote the consumer trust necessary to encourage trustworthy AI development and use. Individual privacy rights, including opt-out rights, should be balanced against the public good that can be established by developing AI based on deidentified data for health care applications and algorithmic development. Information that has been sufficiently deidentified should be available for use and disclosure without being subject to opt-out mechanisms. This will ensure that legally and ethically sourced data remains useable for algorithmic development and improve health care for everyone.

Conclusion

We appreciate your leadership in ensuring strong federal privacy protections for health data and we look forward to working with you to balance this need with the critical role that data plays in health innovation.

Sincerely,

René Quashie
Vice President, Digital Health

Rachel Nemeth
Senior Director, Regulatory Affairs

Catherine Pugh
Senior Manager, Digital Health

India Herdman
Manager, Policy Affairs

[4] https://shop.cta.tech/products/the-use-of-artificial-intelligence-in-healthcare-trustworthiness-cta-2090