

233 N. Michigan Ave., 21st Fl., Chicago, IL USA 60601-5809

| 312.233.1100

September 28, 2023

The Honorable Bill Cassidy, M.D. Ranking Member Health, Education, Labor, and Pensions Committee US Senate 455 Dirksen Senate Office Building Washington, DC 20510

RE: Response to Request for Information on Safeguarding Health Data Privacy

Submitted via email to healthprivacy@help.senate.gov

Dear Ranking Member Cassidy:

Thank you for the opportunity to provide feedback on safeguarding patient and consumer health data privacy. The increase in ways to share health data, both in and out of traditional healthcare settings, as well as the expansion of wearable devices, smart devices, and health and wellness apps have made protecting the privacy and integrity of health data more complex than ever.

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. The AHIMA mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and clinicians. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide. AHIMA members also bring the expertise and knowledge around health data that is necessary to inform investments in our healthcare system.

We appreciate the commitment to addressing challenges associated with building a framework to address the current privacy needs related to health data. We must ensure that the US has frameworks in place to protect both data covered by the Health Insurance Portability and Accountability Act (HIPAA), as well as non-HIPAA covered data, and that those frameworks are specific to the needs of both types of data. Health information professionals directly manage patient health information within the health ecosystem and have unique insights into the way health data should be regulated. AHIMA offers the following feedback in response to the Request for Information.

General Privacy Questions

What is health data?

There are multiple types of health data, including information covered under HIPAA, and health information that is considered personally identifiable information (PII) but not covered under HIPAA. HIPAA has long provided privacy protections for health data held by covered entities and business associates defined under HIPAA. However, health data held by HIPAA non-covered entities requires an appropriate oversight and enforcement to help ensure an individual's health information is kept private, confidential and secure. As we discuss the term "health data held by HIPAA non-covered entities" or "health information held by HIPAA non-covered entities," AHIMA defines this health information held electronically as "electronic health information" as defined at 45 CFR 171.102.¹

Health Information Under HIPAA

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

While AHIMA supports the current HIPAA framework to regulate health data held by covered entities, there is a gap in the privacy of HIPAA-covered health information that must be addressed: the lack of a national strategy on patient identification and matching. This gap is the direct result of the inclusion for more than two decades of Section 510 within the Labor, Health and Human Services, Education, and Related Agencies (Labor-HHS) appropriations bill that prohibits the US Department of Health and Human Services (HHS) from spending any federal dollars to promulgate or adopt a national unique patient health identifier standard. The removal of this ban, supported by more than <u>150 healthcare</u> <u>organizations</u>, would allow HHS to work with the healthcare sector to consider all potential solutions for a national strategy on patient identification and matching.

The committee should also support steps to bring us closer to a national strategy on patient identification and matching, including improved standards around the collection of demographic information within certified health IT. Improving standards that increase patient match rates will directly contribute to fewer overlaid records that may jeopardize individuals' privacy.

Collection and Sharing of Health Data

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? How should information about data collection practices be conveyed to patients?

AHIMA recommends that Congress develop a framework to regulate health data held by HIPAA noncovered entities, and enforcement should fall under the Federal Trade Commission (FTC) to protect consumer privacy. AHIMA recommends the regulatory framework must:

- 1. Guarantee individuals' access to their health information regardless of where it travels.
- 2. Improve accountability. Data holders must develop, document, communicate, assign, and be held accountable for their privacy policies and procedures.

¹ "Electronic health information" means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in the designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity. EHI does not include psychotherapy notes (as defined in 45 CFR 164.501) or information compiled in reasonable anticipation of, or for use in a civil, criminal or administrative action or proceeding.

- 3. Enhance communication and transparency. Data holders must communicate to individuals what information will be collected and maintained and generally how the data may be processed and disclosed, including whether data will be sold or commercialized.
- 4. **Limit the collection, use, and disclosure of health information.** Data holders must limit the amount of health information collected, used, and disclosed to the minimum necessary.
- 5. **Ensure the accuracy and integrity of health information.** Any framework must encourage the completeness, accuracy, and integrity of health information.
- 6. **Prioritize the protection of health information** against various privacy and security risks, including breaches and unauthorized disclosures.
- 7. Address health information retention concerns by ensuring that health information is retained no longer than necessary by data holders.
- 8. Facilitate disposition and destruction of health information.
- 9. Assign appropriate oversight and enforcement responsibilities including designating and adequately funding oversight and enforcement responsibilities.

Artificial Intelligence

What privacy challenges and benefits does the use of artificial intelligence pose for entities that collect, maintain, or disclose health care data?

The management of health data is integral to our healthcare system. In August, AHIMA undertook a survey of health information professionals in collaboration with NORC at the University of Chicago. The survey sought to understand the specific workforce challenges that impact the HI profession and assess the role that emerging and evolving technologies like AI and ML will have on the HI workforce.

The use of AI and ML in the management of health data has a direct impact on patient safety and privacy, including the accuracy and quality of data found in patient medical records. In its survey, AHIMA asked HI professionals about their use of the following AI or ML technologies:

- autonomous coding
- computer assisted coding
- algorithms for patient matching
- Al risk adjustment;
- healthcare utilization management
- administrative workflow assistance
- chatbots (such as ChatGPT).

Of the respondents that reported their department used one or multiple AI tools identified above, a number reported the technology improved the quality of individuals' health data, including 66% of respondents who reported that algorithms for patient matching increased data quality. Increased data quality related to patient matching not only protects patients' safety, but increases patient privacy, reducing the risk of overlaid records where two or more patients' medical records are combined.

State and International Privacy Frameworks

How should the federal government proceed, considering the existing state patchwork?

AHIMA supports the Beyond HIPAA Privacy Principles developed by the Confidentiality Coalition, whereby privacy and security requirements for health data, whether it is held by HIPAA-covered or HIPAA-non covered entities, should be set at the federal level to create a single uniform national standard. This will reduce confusion and uncertainty, and improve compliance with privacy standards.

AHIMA thanks Ranking Member Cassidy for his leadership in the conversations around the health data privacy and for the opportunity to provide feedback. We look forward to working with you to ensure a system that protects patient and consumer privacy. Should you or your staff have any additional questions or comments, please contact Kate McFadyen, Director, Government Affairs, at <u>kate.mcfadyen@ahima.org</u> or (202) 480-6058.

Sincerely,

and the

Lauren Riplinger Chief Public Policy & Impact Officer