Association of
American Medical Colleges
655 K Street, N.W., Suite 100, Washington, D.C. 20001-2399
T 202 828 0400
www.aamc.org

September 28, 2023

The Honorable Bill Cassidy, MD
Ranking Member
Health, Education, Labor, and Pensions Committee
United States Senate
Washington, DC 20510

Dear Ranking Member Cassidy:

On behalf of the Association of American Medical Colleges (AAMC), I write to share the perspectives of academic health systems, teaching hospitals, and faculty physicians in response to your recent request for information (RFI) on Improving Americans' Health Data Privacy. The AAMC appreciates your leadership in engaging stakeholders on how best to improve health privacy protections to safeguard sensitive information in balance with supporting advancements in medical research. We agree that privacy is an essential element in our health care system, and individuals must trust that their health information is protected.

The AAMC is a nonprofit association dedicated to improving the health of people everywhere through medical education, health care, medical research, and community collaborations. Its members are all 157 U.S. medical schools accredited by the Liaison Committee on Medical Education; 12 accredited Canadian medical schools; approximately 400 academic health systems and teaching hospitals, including Department of Veterans Affairs medical centers; and more than 70 academic societies. Through these institutions and organizations, the AAMC leads and serves America's medical schools, academic health systems and teaching hospitals, and the millions of individuals across academic medicine, including more than 193,000 full-time faculty members, 96,000 medical students, 153,000 resident physicians, and 60,000 graduate students and postdoctoral researchers in the biomedical sciences. Following a 2022 merger, the Alliance of Academic Health Centers and the Alliance of Academic Health Centers International broadened participation in the AAMC by U.S. and international academic health centers.

AAMC member health systems, hospitals, and faculty physicians have been leaders in ensuring that patient information is protected and are committed to ensuring use of such information is consistent with federal and state privacy laws. These health care providers are invested in the transformation to delivering value-based health care and recognize the role of health information exchange and patient engagement in that effort. The AAMC supports policies to improve patient engagement in their care and remove obstacles to efficient care coordination and case management while preserving the privacy of patients' protected health information (PHI), as required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

The AAMC believes removing barriers to the exchange of health information for coordinating care among providers, payers, and others involved in meeting patients' health-related needs will have a positive impact on patient care and health outcomes. To that end, we strongly support giving patients greater access to and control over their own health records. However, we remain deeply concerned about the increasing role of entities not bound by HIPAA, such as personal health application (PHA) developers, in accessing and using sensitive information about an individual's health. Until such entities are subject to privacy and security standards commensurate with HIPAA rules, there is a real threat that the lack of appropriate patient privacy protections will erode any gains in patient engagement.

Our comments are broken into three main areas in response to the RFI: what is working under HIPAA, what is not working under HIPAA, and what is not necessary under HIPAA by not improving privacy while adding burden.

What's Working

HIPAA Covered Entities (CEs) Stewardship of Health Data

Prior to the adoption of the HIPAA statute and subsequent development and implementation of the HIPAA Privacy Rule, CEs did not necessarily view themselves as stewards of patients' health data. **Through implementing requirements under the Privacy Rule, there has been a sea change in health privacy – with CEs adopting principles of stewardship and fairness in the handling of sensitive health information.** Across the board, from health care treatment, operations, and research – meaningful change has been realized to protect an individual's privacy rights when managing personal health information.

What's Not Working

Increasing Role of Unregulated Actors

When the HIPAA Privacy Rule was finalized in 2000, federal policymakers could not have foreseen the rapid expansion of entities that would access, use, and exchange sensitive health information, including personal health application developers, social media and internet advertising companies, pharmaceutical companies, medical device manufacturers, personal health wearable technologies, etc. The Privacy Rule only applies to a limited set of CEs – health plans, health care clearinghouses, and health care providers, and their business associates. With the increased role of unregulated actors managing and using individual's health information, there is an increasing obligation placed on CEs to enforce privacy protections through downstream contracts. This will remain true unless actions are taken to ensure more entities are held to similar privacy stewardship standards as CEs are under HIPAA.

For example, social media companies and internet advertising companies are not HIPAA-regulated actors, though their dominance in developing critical website functionalities through pixels and trackers, has led to a significant challenge for CEs. The HHS Office for Civil Rights

(OCR) issued guidance on December 1, 2022, in a Bulletin[1] stating that to be HIPAA compliant, CEs must have appropriate business associate arrangements with such companies to use functional website tools, including so-called online tracking technologies. To date, nearly all such tech companies refuse to enter these contractual arrangements and accept a HIPAA level of responsibility for privacy stewardship.

This in turn leaves health care providers in a difficult situation, as increasingly, individuals are using the internet to search and find out information about health care. It is critical that individuals using the internet obtain health information that is accurate and from trustworthy sources. Teaching health systems and hospitals and their physician faculty provide important, credible information on their websites to assist patients as they seek this information. Through their websites and apps, they provide information to individuals throughout the country, including in underserved areas that may not have access to this information. Under the online tracking guidance, an IP address is protected even if the consumer is not actually seeking medical care. This policy applies HIPAA protections when consumers search for general health information on websites about vaccines, symptoms of an illness, office hours, facility locations, credentials and experience of physicians, and other topics on a teaching hospital and health systems website. In many cases, these individuals browsing the website are not patients, but rather are individuals simply seeking information. If the current framework remains in place, teaching health systems face tough choices on how to balance website functionality, free access to health information resources, and their obligations under HIPAA. Given the impact of this policy, we believe this Bulletin should be rescinded, and Congress should direct OCR to follow the required notice and comment rulemaking process if it would like to make changes to the HIPAA privacy rule related to on-line tracking technologies.

Inadequate De-Identification Standards

Currently, under the HIPAA Privacy Rule there are standards for determining when PHI is de-identified and thus no longer subject to stringent privacy protections. This has been critical to the use of anonymized data sets to foster advancements in medical research. Unfortunately, the rules have not kept up with technology and data science, and many have proven that de-identified datasets can be reidentified. Conversely, there are cases where the deidentification standards remove critical identifiers and render a dataset unusable for research purposes where other privacy protections would suffice. In some spheres, de-identification has been phased out as a method for anonymizing data, and use of privacy-enhancing technologies and privacy by design strategies have been adopted instead. Actions should be taken to understand better policy solutions for protecting personal information in balance with the use of data to advance innovation in health care.

Expansion of Consumer Data Protections

There are myriad state and international privacy laws that may or may not interact with or conflict with the HIPAA Privacy Rule. Actions should be taken to reduce complexity and better align these privacy frameworks.

---

[1] Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associations (December 1, 2022) https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

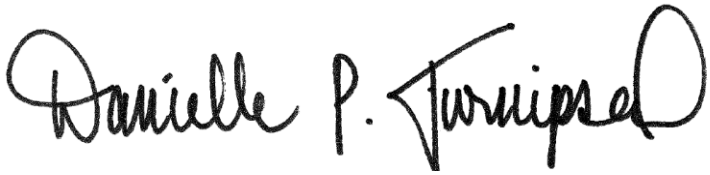
What's Not Necessary

Accounting for Disclosures

In 2011, the HHS OCR issued a notice of proposed rulemaking (NPRM) that would require covered entities to provide a full accounting of disclosures when requested. We strongly supported the withdrawal of the Accounting for Disclosure NPRM and continue to recommend the withdrawal of this policy. Our members receive very few requests for such an accounting – generally fewer than one per year. The proposed access report requirement would create undue burden without providing meaningful information to individuals. In most cases, when a request is made it is because of a fear that someone has "snooped" into the record, and that can be handled through an internal investigation instead. Our members routinely monitor medical records for inappropriate access and have in place policies and procedures for dealing with inappropriate access. Furthermore, any access in violation of the Privacy Rule is subject to the breach notification provisions thereby ensuring that patients are informed of the access and disclosures most of interest to them, without the need for a request of an accounting. There also are substantial concerns about ensuring the safety and privacy of staff when their names are released to a patient.

Again, thank you for your leadership and commitment to enhancing health care data privacy protections. The AAMC appreciates the opportunity to share the perspectives of the nations' teaching hospitals, health systems, and faculty physicians. If you have any further questions, please contact Len Marquez, Senior Director, AAMC Government Relations and Legislative Advocacy, at lmarquez@aamc.org.

Sincerely,



Danielle Turnipseed, JD, MHSA, MPP
Chief Public Policy Officer
Association of American Medical Colleges

CC: David J. Skorton, MD
President and CEO
Association of American Medical Colleges