ADA American Dental Association®

1111 14th Street, N.W.
Suite 1200
Washington, DC 20005

T 202.898.2400
F 202.898.2437
www.ada.org

September 28, 2023

The Honorable Bill Cassidy, M.D.
Ranking Member
United States Senate
Senate Committee on Health, Education,
Labor and Pensions
428 Senate Dirksen Office Building
Washington, DC 20510

Dear Ranking Member Cassidy,

On behalf of the more than 159,000 members of the American Dental Association (ADA), thank you for the opportunity to respond to your request for information about how data that is not currently protected by the Health Insurance Portability and Accountability Act (HIPAA) can be secured as new technologies are utilized in health care. America's dentists make patient data privacy a priority in their practices every day and welcome your interest in how data privacy can continue to be protected from emerging threats.

As you seek to understand how to update HIPAA to respond to new technologies, we urge you to avoid any new regulation that would further burden small businesses, like most dental practices. Like other small businesses, most dental practices do not have the ability to hire staff needed for new compliance concerns.

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?

Health data is any data related to an individual which helps us understand a person's past, present, or future health, their health risks, and how their health is managed. Much of health data is generated and managed by the entities and actors named in HIPAA or involved in direct patient care however, health data can also be collected through engagement by patients with non-covered entities such as self-reported data via mobile applications or websites. There is also a growing collection of data which using geo-location tracking, behavior monitoring, and other consumer insights, that it is possible that an individual's health could be inferred.

In dental medicine, oral microbiome testing and salivary diagnostics have gained popularity. When administered by a health professional there is an assumption of privacy, however, many of these products are available by mail and consumers are often not well informed on how their biologic data may be used, shared or the security of this health information.

Additional transparency for consumers on what is covered by HIPAA as well as privacy warnings or labeling for health products or technology that collect health data that are not governed by HIPAA should be considered.

Additionally, we would like to see Congress clarify and better align the confusing and sometimes-conflicting confidentiality and privacy requirements of HIPAA and Part 2 of Title 42 of the Code of Federal Regulations. Part 2 governs the disclosure of patient records relating to substance use disorders.

There is usually little need for dentists to have detailed information about a patient's substance use disorder. Prior to surgery, a dentist may ask if a patient uses illicit substances or has (or is at risk of developing) an addiction. The information may shape decisions about administering anesthesia and/or prescribing controlled substances. A dentist may also voluntarily screen patients for potential substance use disorders and provide a brief intervention and referral for appropriate treatment. However, access to that information has historically (and sufficiently) been governed by HIPAA.

Rarely, if ever, would there be a need to obtain a Part 2 record from a substance abuse treatment facility or other provider holding a Part 2 record.

The Department of Health and Human Services is currently exploring whether the additional confidentiality and privacy requirements of Part 2 should be extended to providers whose primary function is *not* to provide substance abuse treatment and who are *not* licensed for that purpose. We urge Congress to work with the Department to clarify and better align Part 2's confidentiality and privacy requirements with HIPAA.

Health Information Under HIPAA

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

HIPAA compliance, training and best practices continue to be a challenge for many dental offices. Ongoing support for small businesses and independent practices to ensure that providers are able to maintain compliance and understand their obligations. The American Dental Association makes many resources and tools available to ease the burden of compliance, including the recently published, "Complying with the HIPAA Breach Notification Rule: A Guide for the Dental Office." Nevertheless, the ADA encourages Congress to provide funding for training of compliance staff whenever Congress places new compliance burdens on health care providers

We also urge that an exception be made under HIPAA to allow dentists and other health care providers to disclose patient information in response to an online review without violating the HIPAA Privacy Rule or the FTC Act prohibition against unreasonable and deceptive trade practices, provided the disclosure is limited to the scope of the topics addressed in the review. In addition, a dentist or other health care professional should be allowed to confirm whether a reviewer is, in fact, one of their patients. HIPAA privacy regulations are intended to protect patients from unauthorized disclosure of patient health information, not as a loophole for bad actors who want to harm health care practices without repercussion.

Allowing dishonest and unfair reviews to go without response because of privacy regulations negatively impacts the health of patients and consumers seeking trustworthy information about where to seek care. Dishonest and unfair reviews can also cause serious injury to businesses and healthy competition. Additionally, dental practices in the process of being sold could see their valuation affected by dishonest reviews.

Should Congress update HIPAA?

Careful consideration should be taken prior to updating HIPAA. In the health care regulatory space, many significant changes pertaining to health information technology and data exchange are currently being considered. Additional regulatory changes that would impact providers are likely to place additional burden on already struggling practices. Any updates to HIPAA should only be considered if they will have significant benefits to patient privacy, burden reduction, or address data governance by currently non-covered entities. Updates to HIPAA should also allow reasonable periods of time for compliance to reduce the substantial financial burden placed on small businesses, like dental practices.

Should Congress expand the scope of HIPAA? What specific information should be included in the HIPAA framework?

Expansion of the scope of HIPAA to entities not currently covered by HIPAA is a complex topic, with the potential to be a boon to medical practice, but also with the danger of adding further compliance burdens on providers, patients, and industry. Before making any significant expansions of the scope of HIPAA, Congress should devote resources to an agency like the National Committee on Vital and Health Statistics (NCVHS) with the appropriate expertise to study the need for HIPAA scope expansion, as well as how it might be best accomplished.

Collection of Health Data

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

HIPAA already includes a requirement for a Notice of Privacy Practices. However, no such requirement exists at the federal level for information about privacy practices for non-HIPAA covered data. While we believe it is important for Congress to consider how to regulate currently non-HIPAA covered data, we also believe this need must be balanced by limiting the burden of HIPAA compliance on dentists and patients.

While the ADA does not have extensive policy on specific disclosure of data collection practices, dentists prioritize data privacy for their patients and themselves. We also encourage Congress to consider privacy principles established by other health care professional groups.[1]

Artificial Intelligence

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?

The ADA urges Dental AI Developers to safeguard the privacy of patients and secure their personal and medical information. Financial burden of additional security technology should be considered for small businesses.

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?

AI developers must abide by the same privacy practices for which providers are held, as well as security and breach notification. Additionally, standardized AI security protections should be established to protect end users and patients. Funding should be made available for provider education on privacy when using AI, while consumers and patients should be offered educational opportunities promoting transparency in the use of AI supported diagnostics.

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?

Providers first must be made aware of all technologies and business relationships in which AI is using shared patient data, including de-identified data such as a picture or radiographic image or scan. Developers and industry must be transparent in their use of AI, and must facilitate for providers an efficient mechanism for a patient to give informed consent or opt out of their data being used for algorithmic development

[1] See the American Medical Association's "AMA Privacy Principles," https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf. Accessed September 25, 2023.

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?

Dental practices, many of which are small businesses, may need to comply with a variety of federal and state data privacy and security laws, such as HIPAA, state laws that are not contrary to HIPAA, state laws that are contrary to and more stringent than HIPAA, and the FTC Act[2]. These complex laws and their complex regulations may change from time to time, causing a compliance challenge, particularly for small dental practices without compliance departments.

Because of the complexity of the legal and regulatory framework for HIPAA enforcement, we would urge Congress to seek to simplify the framework to ease the burden of compliance for covered entities.

Thank you once again for the opportunity to respond to your questions about data privacy, and for your leadership on this important issue. The ADA looks forward to working with you both to protect patient data privacy and to reduce the burdens of HIPAA compliance on health care providers and their patients.

Should you have any further questions about our response, please contact Ms. Natalie Hales at 202-898-2404 or halesn@ada.org.

Sincerely,

George R. Shepley, D.D.S.
President

Raymond A. Cohlmia, D.D.S.
Executive Director

GRS:RAC:nh

[2] https://www.ftc.gov/business-guidance/resources/sharing-consumer-health-information-look-hipaa-ftc-act. Accessed September 22, 2023.