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

December 6, 2024

The Honorable Ron Wyden
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mark Warner
703 Hart Senate Office Building
Washington, DC 20510

Dear Senator Wyden and Senator Warner:

On behalf of the 159,000 members of the American Dental Association (ADA), we write to comment on S. 5218, the Health Infrastructure Security and Accountability Act of 2024. America's dentists have made securing their patients' health information a priority,[1] [2] and commend you for offering solutions that address the growing problem of cyber-attacks. Cyber-security is essential for healthcare providers, payers, patients, and the rest of the healthcare industry. However, it is also essential that legislators and regulators take into account the burden of regulation on small businesses.

The ADA comments on the Health Infrastructure Security and Accountability Act of 2024 focus on Title 1, Strengthening and Increasing Oversight of, and Compliance with Security Standards for Health Information, and the importance of taking into consideration the challenges small providers, like many dentists, might face when implementing this legislation.

Section 101. Security Requirements

The ADA strongly urges dental practices to familiarize themselves with HIPAA's requirements for protecting patient health records, including electronic patient information. In addition to comprehensive guides for practice on complying with HIPAA,[3] the ADA has more recently emphasized safeguarding patient information through website security and accessibility controls,[4] complying with the HIPAA Breach Notification Rule,[5] and tips on how dental practices can be protected from computer hacking.[6] The ADA's Standards Program has also recently adopted a number of robust standards for dental practices related to patient records and data.[7]

Section 101 would require the Secretary of Health and Human Services to adopt enhanced security requirements to protect health information, protect patient safety, and to ensure the availability and resiliency of health care information systems and health care transactions. The Secretary would be required to adopt these enhanced requirements within two years of the passage of the bill, and would also be required to update the requirements at least every two years.

The ADA would support the adoption of enhanced security requirements, but only if the Secretary allows the necessary time for dental practices and other providers to comply through technology updates, training, and other required means. Most dental practices, and many other healthcare providers, are small businesses that are already heavily burdened with complying with existing HIPAA regulations. As you also know, several final and pending health information technology-related rules

---

[1] American Dental Association. Response to Request for Information on Improving Americans' Health Data Privacy from Senate Health, Education, Labor, and Pensions Ranking Member Sen. Bill Cassidy. September 28, 2023.
[2] American Dental Association. Statement for the Record for House Energy and Commerce Subcommittee on Health Hearing, "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack." April 15, 2024.
[3] American Dental Association. HIPAA Resources for Members.
[4] American Dental Association. Safeguarding Patient Information, Website Security and Accessibility.
[5] American Dental Association. Complying With the HIPAA Breach Notification Rule. 2023.
[6] American Dental Association. Tips to Safeguard Your Practice from Computer Hackers.
[7] American Dental Association. Dental Informatics: Standards, Technical Specifications, and Technical Reports.

are expected to be implemented throughout the next five years. Congress and the relevant regulatory agencies must take into account the cost constraints faced by these small providers who would be faced with complying with new security requirements every two years, should this legislation pass.

Section 102. Security risk management, reporting requirements, and audits for covered entities and business associates.

This section would require annual independent cybersecurity audits for covered entities. It would also require stress testing to ensure that covered entities are able to restore service promptly after an incident. The requirement to perform a stress test could be waived by the Secretary if "the burden on the [covered] entity or [business] associate significantly outweighs the benefits [of the stress test], taking into account the revenue of the entity or associate, the volume of protected health information or healthcare transactions processed by the entity or associate, and such other factors as the Secretary determines appropriate."

While the ADA strongly supports high cybersecurity standards for dental practices, and throughout the healthcare industry, we also strongly urge you to consider the challenge small providers, including many dentists, would face when implementing independent cybersecurity audits and stress tests. While small practices may qualify for a waiver from the Secretary based on the qualifications listed in the legislation, it is important that any requirement to audit practice cybersecurity or to perform stress tests explicitly exempt small practices[8]. If small practices must implement audits and stress testing, resources and funding must be offered to these practices so that they are not overly burdened with the costs of implementation. One way of avoiding over-burdening smaller practices may be to allow the Secretary to implement new security audit and stress testing requirements in stages, with appropriate incentives offered for compliance at each stage. It is also crucial that any legislation that makes such requirements requires the Secretary to educate covered entities on the availability of waivers. Finally, audits should have a remediation period included for any finding before penalties are assessed.

The ADA also encourages Congress to define more specifically how long larger covered entities have to "recover essential functions" after a cybersecurity incident, as this bill only requires that stress tests "evaluate whether such entity has the capabilities and planning necessary to recover essential functions… following a cyber incident…" Change Healthcare has only recently gotten some of their dental services back online, despite their cyber incident occurring over seven months ago. This has exposed small providers with business interruptions to significant financial damages, and the ADA strongly urges Congress to offer financial protections to small providers if they suffer damages due to such a cybersecurity breach with systemic effects.

****

The ADA once again would like to thank you for the opportunity to comment on S. 5218, the Health Infrastructure Security and Accountability Act of 2024, and for your leadership on cybersecurity issues in healthcare. America's dentists stand ready to work with you to safeguard patient records and data, including through preparing dental practices to protect themselves and their patients from cyberattacks.

If you have any questions, please contact Natalie Hales at 202-898-2404, or at halesn@ada.org.

[8] "Small practice," as defined by the Affordable Care Act for purposes of certain exemptions and waivers of its requirements, is a practice with 50 or fewer employees.

Sincerely,

/s/

Brett Kessler, D.D.S.
President

/s/

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