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

March 26, 2025

The Honorable Brett Guthrie
Chairman, Energy and Commerce Committee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Joyce, M.D.
Vice Chairman, Energy and Commerce Committee
U.S. House of Representatives
2102 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Guthrie and Vice Chairman Joyce,

As the leading authority on oral health in the United States, the American Dental Association (ADA), representing over 159,000 dentists across the country, appreciates the opportunity to provide input to the Privacy Working Group regarding the development of a federal comprehensive data privacy and security framework. Protecting sensitive personal information is critical to patient trust and high-quality care. As representatives of the dental profession, we recognize the importance of safeguarding data while ensuring that new regulatory requirements are practical, scalable, and aligned with existing health privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA).

Roles and Responsibilities

Regulation should encourage proactive engagement in the adoption of cybersecurity tools and best practices. Overly burdensome regulation requirements that do not account for business structure and capacity may lead to involuntary non-compliance and closures due to financial costs to meet compliance measures. Dental practices, which range from solo practitioners to larger health systems, primarily function as covered entities under HIPAA and should not be subjected to duplicative or overly burdensome regulations.

Any comprehensive policy should assess the entity's position as critical infrastructure. For example, the regulatory burden placed on large health systems would not be appropriate to apply equally to individual private practices.

Personal Information, Transparency, and Consumer Rights

Current requirements for business associates fall short of ensuring regulatory compliance and shift the burden to small businesses. A central authority should provide and maintain model language for Business Associate Agreements (BAAs) regarding privacy, cybersecurity, and contingency plans. Small companies (covered entities) should be allowed a safe harbor if a security breach results from a business associate's failure to adhere to regulations and best practices.

Existing Privacy Frameworks & Protections

Federal comprehensive privacy law should consolidate resources (e.g., NIST, CISA, etc.) and provide a singular authority, as the current environment is far too complex for many

regulated entities to track. Privacy and security regulations should improve security and be responsive to emerging threats, not create needless paperwork that reduces efficiency. Policies should retain the distinction between addressable and required implementation specifications, which may make compliance easier for small, covered entities and business associates, who would otherwise be required to comply with all implementation specifications that may not directly apply to the services provided or rendered.

Data Security

Data security must be a priority, but we would recommend starting with a focus on education, not enforcement, at least for the time being. Then, make it clear what regulated entities need to do, segmenting changes by the regulated entity's technical complexity, ability, and risk. New regulations and provisions for privacy and security should be staggered, and enforcement should be based on business purpose and relation to critical infrastructure and scaled to appropriate levels based on size and risk assessed.

Accountability & Enforcement

A safe harbor may encourage businesses to take voluntary action to improve their cybersecurity practices. A company that can demonstrate that it reasonably implemented and maintained a cybersecurity plan based on industry best practices should have some protection against legal and punitive damages due to a breach. Audits and compliance testing should be used for assessing effectiveness, allowing entities to resolve outstanding issues and improve their policies without costly enforcement actions unless there is a failure to remediate ongoing system issues.

A singular privacy and security entity could use its authority to create systems to assist in bringing the industry to compliance. Maintaining voluntary audit programs, establishing free or low-cost security tools, and establishing accreditation and certification programs that build trust in the products and services used by businesses.

****

The ADA appreciates the opportunity to contribute to this critical discussion on federal data privacy and security. We encourage the Privacy Working Group to adopt a balanced, risk-based approach that both safeguards patient data and allows dental practices to operate effectively. The ADA looks forward to continued engagement on this issue and welcomes further collaboration. We stand ready to provide additional insights or participate in stakeholder discussions to help shape a practical, effective regulatory framework. Thank you for your consideration. Please do not hesitate to contact Natalie Hales at halesn@ada.org if you have any questions.

Sincerely,

Brett Kessler, D.D.S.
President

Elizabeth Shapiro, D.D.S., J.D., C.A.E.
Interim Executive Director