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

April 15, 2024

The Honorable Brett Guthrie
Chair, Health Subcommittee
U.S. House of Representatives
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member, Health Subcommittee
U.S. House of Representatives
Committee on Energy & Commerce
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chair Guthrie and Ranking Member Eshoo,

On behalf of the more than 159,000 dentist members of the American Dental Association (ADA), we are writing to provide insights and recommendations for your hearing on the Change Healthcare cyberattack.

As you are aware, the cyberattack on Change Healthcare, one of the largest healthcare technology companies in the United States, has had significant repercussions for many sectors, including dental practices. The lack of transparency surrounding the financial impact of this incident is concerning and we believe full financial impact assessments by the industry are imperative.

Our members have reported delayed claims, additional expenses incurred due to resorting to physical mailing, and increased office staff time spent on call centers and troubleshooting. In the nearly ten weeks since the cyber-attack, dental services have yet to be fully restored. This means provider credentialing, claims and claim attachments processing and tracking, practice analytics and revenue cycle insights, and automation of business functions (eligibility and benefits verification, payment remittances, etc.) are experiencing ongoing disruptions.

Due to the unprecedented magnitude of this attack, we recommend the below measures that we believe are crucial to ensuring the resilience of our healthcare infrastructure in the face of cyber threats.

1. **Comprehensive Financial Impact Assessments**: Urgently conduct comprehensive financial impact assessments across the industry to ascertain the extent of the damage inflicted by the cyberattack. These assessments should encompass not only direct financial losses, but also indirect costs incurred due to disruptions in practice operations.
2. **Enactment of Prompt Pay Legislation**: The enactment of “prompt pay” laws would mandate insurance companies to promptly reimburse healthcare providers for services rendered. This is pivotal to ensuring the financial stability of systemically important healthcare institutions, which include dental practices, amidst increasing cyber incidents and other emergencies.
3. **Enhanced E-Prescribing Standards**: Strengthen e-prescribing standards implementation and interoperability to ensure seamless continuity of care and medication access for patients during cyber-related disruptions. Standardized e-prescribing and systems to access to Enhanced Prescription Drug Monitoring Program (ePDMP) improve patient safety and alleviate administrative burdens on dental practices.
4. **Health Insurance Portability and Accountability Act (HIPAA) Compliance Enhancement**: HIPAA compliance can help safeguard protected health information from cyber threats. Strengthening HIPAA compliance measures so that health IT vendors that enter in business associate agreements with covered entities are held to the same standards

under HIPAA as covered entities is imperative for protecting patient confidentiality and mitigating cybersecurity risks.

5. **Cybersecurity Support for Dental Practices**: As critical small healthcare businesses, dental practices often lack the resources and expertise to implement robust cybersecurity measures independently. Providing for enhanced cybersecurity support and resources to fortify defenses against cyber threats could include access to cybersecurity training, assistance in implementing cybersecurity frameworks, and other collaboration with cybersecurity experts.
6. **Mitigation of Potential Price Gouging**: Price transparency measures such as price caps and stringent oversight mechanisms are essential to prevent opportunistic pricing practices that could exploit vulnerabilities in the healthcare system.
7. **Payer Responsibility and Collaboration**: Holding payers accountable for facilitating uninterrupted access to reimbursement and financial support for healthcare providers during cyber incidents. Payers should collaborate with providers, industry stakeholders, and government agencies to develop robust contingency plans and expedite claims processing to minimize disruptions.

We believe these proposals can aid policymakers as they seek to take proactive steps towards long-term resilience in the face of future cyber threats to dental practice and the broader health care system. In addition to addressing the immediate aftermath of this cyberattack, we urge the Committee to consider any legislative measures that would improve options for healthcare providers impacted by cyberattacks and that attempt to prevent such incidents in the future. We are particularly interested in policies addressing gaps in cybersecurity regulations and enforcement mechanisms such as measures to enhance penalties for cybercrimes, streamlining transparency on incident reporting requirements, support for contingency planning and facilitating information sharing among law enforcement agencies and healthcare providers.

We appreciate the Committee holding a hearing on this critical issue and would be happy to provide any further information or assistance. The ADA remains committed to collaborating with policymakers to safeguard the integrity and security of our healthcare infrastructure.

****

The ADA looks forward to continuing to work with you and we would welcome the opportunity to speak with you in more detail and answer any questions you have regarding these comments. Please contact Ms. Natalie Hales at 202-898-2404 or Halesn@ada.org to facilitate further discussion.

Sincerely,

Linda J. Edgar, D.D.S., M.Ed.
President

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

LJE:RAC:nh