TEXAS MEDICAL ASSOCIATION

Physicians Caring for Texans

March 5, 2025

Marissa Gordon-Nguyen
U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HIPAA Security Rule NPRM
Hubert H. Humphrey Building, Room 509F,
200 Independence Avenue, SW
Washington, DC 20201

RE: RIN 0945-AA22 Comments on HIPAA Security Rule to Strengthen Cybersecurity of Electronic Protected Health Information

Dear Ms. Gordon-Nguyen,

On behalf of the Texas Medical Association (TMA) and our more than 59,000 physician and medical student members, we appreciate the opportunity to comment on the proposed rule intended to strengthen the cybersecurity of protected health information.

TMA is a private, voluntary non-profit association and is the largest state medical society in the nation. It was founded in 1853 to serve the people of Texas in matters of medical care, prevention and cure of disease, and improvement of public health. Today, its vision is "improving the health of all Texans."

The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) proposes regulations to modify the security standards of electronic protected health information (ePHI) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The proposed modifications are intended to better protect the confidentiality, integrity, and availability of ePHI.

Cybersecurity is a national problem and impacts many industries, not just health care. TMA asks OCR to consider a national approach to combatting cybersecurity that does not require every single business, regardless of size, to do all the heavy lifting.

Today more organizations and individuals are vulnerable to data breaches and ransomware as more and more information is in the digital format. **In fact, it was the federal government who initially incentivized physicians and hospitals to move to electronic health records (EHRs)** with the adoption of the HITECH Act, which helped pay for the adoption of EHRs. Physicians were incentivized to adopt an EHR because it was touted to lower cost, improve efficiency, and provide higher quality of care. The one-time federal government investment in subsidizing EHR purchases has not even come close to the extra money physicians have had to spend to maintain, upgrade, protect, and exchange ePHI. **TMA is concerned the proposed rule will continue to increase the cost of protecting ePHI to untenable levels for most physician practices. This would further degrade the viability of the independent physician practice, especially those providing primary care to rural and under-served populations.**

TMA understands the importance of appropriate security measures, policies, and procedures to protect electronic health information, and realizes physicians must take steps to proactively guard against bad actors who want to infiltrate their electronic health tools. However, some of what OCR proposes is an overreach for physician practices already overburdened and underpaid.

In fact, **OCR is going far beyond what the law requires when Congress passed HIPAA in 1996.**

This proposal is a gross over-expansion of the original HIPAA legislation. In fact, the Department of Health and Human Services states, *"The Security Rule does not dictate the specific security measures that a regulated entity must use. Instead, it requires the regulated entity to consider the following factors when selecting security measures that meet the Security Rule's requirements: 1) Its size, complexity, and capabilities; 2) Its technical infrastructure, hardware, and software security capabilities; 3) The costs of security measures; 4) The probability and criticality of potential risks to ePHI."*

Physicians participating in the Center for Medicare & Medicaid's (CMS) Merit-based Incentive Payment System (MIPS) already must attest to completing or updating their security risk assessment annually as part of the Promoting Interoperability category. Physicians already have HIPAA training requirements, and sometimes from multiple health systems where they may be credentialed to practice. There are many resources for physicians to learn about and implement good cybersecurity policies and practices. TMA therefore recommends OCR use existing resources like Assistant Secretary for Technology Policy (ASTP) and CMS tools and requirements rather than adding layers of busy work that may not achieve the lofty results OCR proposes.

In the section on *Regulatory Flexibility Act – Small Entity Analysis*, OCR asserts if the proposed policies are finalized, there would not be a significant economic effect on a substantial number of small entities. TMA respectfully disagrees. **The proposed measures add significant costs and burdens to both small and large practices already strained under daily operational pressures. Physicians continue to suffer Medicare payment cuts year over year as indicated by the physician update in *Figure 1*. Practices simply cannot shoulder the additional burden proposed by OCR.**

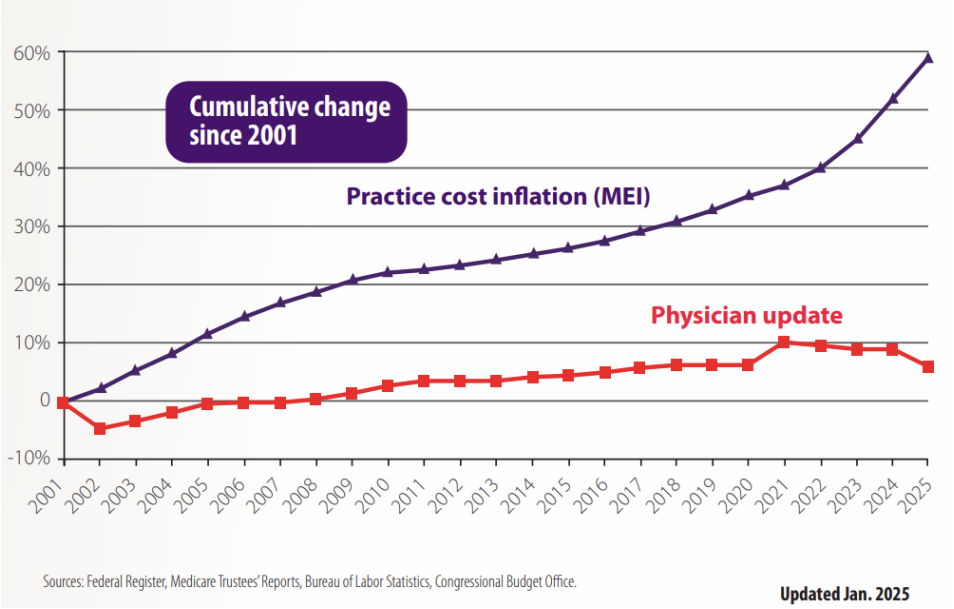

Figure 1

OCR estimates that if this regulation is implemented as proposed, and the number of affected individuals is reduced by 7-to-16%, the cost of implementation would pay for itself. TMA argues that there is no evidence that if the actions proposed are implemented, especially across all health settings, it would have such an impact. Logically there should be some cost savings accrued to some entities but certainly not all, especially with estimated first-year costs of approximately $9 billion and $6 billion annually for subsequent years.

OCR states, "The Department does not view this as a substantial burden because the result of the changes would be annualized costs per regulated entity of approximately $1,235 [=2.3 billion[1004]/1,822,600 regulated entities]. The per-entity costs represent the costs per establishment. As a result, small entities' costs are lower because they have fewer establishments." The cost of implementing what OCR proposes would far exceed $1,235 and TMA believes the methodology OCR used to arrive at this number is flawed. OCR further explains that the cost to small firms would exceed 3% of annual revenue. Spending 3% or more for cybersecurity alone could put some practices out of business, further exacerbating the challenge of patient access to care, especially in rural and underserved areas where it may be the only option for care available to patients. **TMA urges OCR to reconsider the requirements proposed and the actual impact it would have on health care operations.**

The requirements that HIPAA Security already has in place, when implemented properly, will stave off hackers who may be targeting smaller entities. The tools and templates developed by the Assistant Secretary for Technology Policy that are in place to help small practices were carefully created and curated in a way that is feasible for a practice to implement without a large technical team. Many organizations such as TMA and the American Medical Association have tools and resources to assist physicians with cybersecurity protections.

Data breaches and ransomware attacks on small practices are burdensome to those practices. But large scale cyberattacks, like what happened with Change Healthcare, are devastating and have caused severe instability to the health care system through payment interruptions. In fact, the tentacles of Change Healthcare are so far reaching the impact went beyond health care payment systems. **OCR should shift its focus to help cover entities and business associates (including EHR vendors) that impact more than 1 million lives for additional HIPAA security requirements.**

TMA appreciates the opportunity to provide feedback on the HIPAA Cybersecurity proposed regulation. Any questions may be directed to Shannon Vogel, associate vice president of health information technology, by emailing shannon.vogel@texmed.org or calling (512) 370-1411.

Sincerely,

G. Ray Callas, MD
President
Texas Medical Association