March 7, 2025

The Honorable Robert F. Kennedy, Jr.
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Re: Health Insurance Portability and Accountability Act Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Secretary Kennedy:

On behalf of our medical group practices, the Medical Group Management Association (MGMA) thanks you for the opportunity to comment on the Office for Civil Rights' proposed Health Insurance Portability and Accountability Act Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information. While we appreciate the general intent of this proposal, it is far too burdensome to implement in practice and represents such government overreach, it threatens the very sustainability of medical groups in this country. Low reimbursement coupled with onerous government regulations have already driven 80% of physicians in the U.S. into employment arrangements with larger healthcare entities. Proposals like this will only exacerbate this troublesome trend, and we urge you to withdraw it in its entirety.

With a membership of more than 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 group medical practices ranging from small private medical practices to large national health systems representing more than 350,000 physicians. MGMA's diverse membership uniquely situates us to offer the following perspectives.

Overview

During President Trump's first term, MGMA valued the opportunity to collaborate with the administration on initiatives that focused on prioritizing patients over paperwork. Unfortunately, this proposed update to the HIPAA Security Rule is not only a departure from the administration's commitment to reducing burdensome regulations but is also an example of government overreach. While we agree with the importance of strengthening cybersecurity, this Biden-era proposal does not inherently create a better system for securing electronic protected health information (ePHI).

Medical groups are already facing financial hardship, and the proposed requirements would only increase the number of administrative and financial burdens that distract providers from focusing on what matters most - helping patients. Many medical groups do not have the staff to implement the proposed requirements. To meet these compliance standards, they would have to significantly increase their investment in internal staffing and third-party information technology (IT) experts. We believe the estimated cost to states, local and tribal governments, and the private sector provided in the Regulatory

Impact Analysis (RIA) of $183 million in any one year is a woefully inaccurate estimate and that the actual cost would be in the billions of dollars. The estimates of time and money needed to implement various requirements outlined in the proposed rule are concerningly low and underestimate the investment regulated entities would need to make. Medical groups are not the only healthcare stakeholders who would be negatively impacted by the proposed changes. In February, MGMA joined a diverse group of organizations calling for the withdrawal of the proposed rule (see Exhibit A). We appreciate the administration's steadfast support of medical groups and urge you to withdraw this overreaching rule.

Key Concerns

While the proposed rule includes many burdensome requirements and examples of government overreach, MGMA is especially concerned about the following components:

- *Removal of key flexibilities:* The proposed rule changes previously designated "addressable" implementation specifications to be required, removing a critical flexibility and option for innovation. For years, medical groups have appreciated the opportunity to evaluate whether an addressable implementation specification is reasonable and, as needed, adopt alternative measures to best fit their organization. Addressable standards are not chances for covered entities to cut corners; they are critically important opportunities for flexibility, given that there are no one-size-fits-all approaches to cybersecurity. It would be inefficient for medical groups to replace their successful implementation strategies with a government-prescribed specification.

- *Annual audits*: The proposed rule includes new annual audit requirements that would impose significant financial and administrative burdens on medical groups. Since the inception of the HIPAA Security Rule, medical groups have managed their evaluations of systems and risks to comply with the existing requirements to protect ePHI. While there is value in regular audits, organizations already conduct risk analyses and should independently determine the cadence and process that best fits their needs. Moreover, it would be prohibitively expensive for medical groups to hire third-party auditors annually to assess their systems.

- *Technology asset inventory and network mapping:* The proposed rule calls for all covered entities to create a technology asset inventory and a map of their IT systems that documents the movement of ePHI through, into, and out of each system. This mapping exercise would be complex and require a level of expertise that many medical groups do not have internally, creating yet another instance of having to pay a third party to help ensure compliance. For the technology inventory, even if a practice has the internal staff necessary to complete this task, creating an inventory list of every IT asset with the appropriate level of detail would be a significant administrative undertaking.

- *Annual business associate verification:* The proposed rule requires covered entities to collect annual verification from business associates to confirm the associates have implemented the required technical safeguards. This extraordinarily burdensome administrative task does not improve cybersecurity. At a minimum, the valuable time staff would have to spend contacting business associates, requesting the required information, verifying the accuracy of an associate's documentation, and following up annually would take significant time away from supporting patient care. It is a massive administrative burden on medical practices.

- *Compliance date:* The proposed rule underestimates the complexity of the required changes and calls for a compliance date 180 days after a final rule. It would be unfeasible for medical groups to implement the multitude of requirements proposed in this rule in less than six months.

Organizations would need time to plan, budget, and staff their offices before they can even start implementing the required changes. Many medical groups would be unable to make the financial and administrative investments to ensure full compliance with the rule in such a short period.

These are just some of the most concerningly burdensome aspects of the proposed rule. We believe in the importance of strengthening cybersecurity across the healthcare industry, but this proposed one-size-fits-all approach fails to meaningfully improve security and is detrimental to the sustainability of medical groups. Under current law, medical groups are already fully accountable for complying with HIPAA. They know the best methods and processes for ensuring strong cybersecurity practices within their organizations and should not be subject to additional, overly prescriptive government requirements. MGMA strongly urges you to withdraw this proposed rule and not finalize any of its components.

We look forward to working collaboratively with the Office of Civil Rights and the administration to find meaningful ways to support medical groups' efforts to improve cybersecurity. If you have any questions, please contact Madison Hynes, Associate Director of Government Affairs, at mhynes@mgma.org or 202-558-0972.

Sincerely,

/s/

Anders M. Gilberg
Senior Vice President, Government Affairs