March 04, 2025

Anthony Archeval, Acting Director
Office for Civil Rights
U.S. Department of Health and Human Services
Washington, DC 20001

RE: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Acting Director Archeval:

On behalf of the American College of Physicians (ACP), I am pleased to share our comments on the Department of Health and Human Services (HHS) HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information proposed rule. The College is the largest medical specialty organization and the second-largest physician group in the United States. Our members include 161,000 internal medicine physicians, related subspecialists, and medical students. Internal medicine physicians are specialists who apply scientific knowledge and clinical expertise to the diagnosis, treatment, and compassionate care of adults across the spectrum from health to complex illness. We look forward to continuing to work with HHS to implement policies that support and improve the practice of internal medicine.

ACP recognizes the growing threats to our health care delivery system posed by cyberattacks and commends HHS's steadfast commitment to protecting Americans' health care data. Following the Change Healthcare incident, we were vocal about our concern for the ongoing rising cybersecurity and privacy risks within the health care infrastructure and their adverse impacts on physicians and the care they deliver. The College strongly supports robust privacy protections for patients' personal health information (PHI), as outlined in our 2021 position paper, Health Information Privacy, Protection, and Use in the Expanding Digital Health Ecosystem. This policy emphasizes building trust within the patient-physician relationship, protecting patient privacy, and maintaining transparency.

While ACP acknowledges that updates to HIPAA are long overdue and supports the intentions behind this proposed rule, we are concerned about the feasibility of implementing these policies. The time and financial investments required for compliance, especially for smaller, rural, and independent practices, are substantial and could divert resources away from patient

care. Over the past decade, there has been a significant shift in the physician workforce from independent practices to employed physicians. Increased workloads and declining reimbursement rates have primarily driven this change. While ACP supports enhancing cybersecurity protections, **we caution against implementing regulations that could unintentionally pressure smaller practices financially, making it difficult for them to remain independent.**

ACP appreciates HHS's commitment to easing the burden on clinicians and regulated entities by adding a specified transition period for existing contracts with business associates. This extended compliance period provides much-needed flexibility, particularly for smaller practices with limited financial and time resources. ACP encourages HHS to also be mindful of the compliance challenges larger health systems may face. These cautions should be balanced with the commitment to improving the cybersecurity of critical infrastructure. Allowing flexibility in the compliance period could assist physicians with fewer resources and business associates in implementing necessary updates, ultimately advancing HHS's efforts toward enhancing cybersecurity in the health care sector.

The College also supports HHS's aim to establish greater data protection and mandatory enforcement of critical security measures such as multi-factor authentication (MFA). ACP supports MFA to strengthen health data security, but we are concerned about the potential impact on physician workflows. Without implementation specifications in the timing, location, and frequency of MFA, we are worried about the burden this might place on physicians and potential disruptions to patient care. Requiring authentication each time a physician opens a patient record or enters a new room could delay the physician from engaging directly and attentively with the patient. **ACP supports a balanced approach and asks HHS to clarify that MFA should not be burdensome or hinder efficient patient care.**

Additionally, HHS has several proposals focused on workforce training and data security. ACP supports varying access levels in response to changes in employment status and requests further guidance on enforcement practices in these situations, particularly concerning the differences between voluntary and involuntary employment changes. We are also encouraged by the introduction of role-based training requirements, as these help tailor information and minimize overall burden. To further enhance the efficacy of these training initiatives, **ACP urges HHS to develop training resources specifically aimed at smaller and rural practices, which often lack the in-house IT staff to provide necessary training**.

ACP is strongly encouraged by HHS's attention to addressing new and emerging technologies, including artificial intelligence (AI). We agree that these new technologies provide opportunities for greater care efficiency, but believe that AI is best utilized as a complement to clinician

decision making rather than a replacement. In our paper, *Artificial Intelligence in the Provision of Health Care: An American College of Physicians Policy Position Paper*, ACP calls for transparency in the development, testing, and use of AI for patient care. AI developers, implementers, and researchers should prioritize the privacy and confidentiality of patients and clinician data. We applaud HHS's involvement in this area and continue to call for regulatory oversight, a coordinated federal AI strategy, and performance monitoring throughout a model's lifecycle. Regulatory measures are essential to maintaining rigorous safety standards for patients and physicians.

The College appreciates HHS's commitment to modernizing data security and strengthening patient protections. ACP believes it is essential that federal agencies administering and enforcing HIPAA are adequately resourced, staffed, and funded to better address ever-increasing cybersecurity threats to the health care sector. We appreciate the opportunity to provide feedback on this proposed rule and look forward to continued collaboration with HHS and the administration. Please contact Nadia Daneshvar, JD, MPH, Health IT Policy Associate, at ndaneshvar@acponline.org with comments or questions about the content of this letter.

Sincerely,

Ross W. Hilliard, MD, FACP
Chair, Medical Informatics Committee
American College of Physicians