March 7, 2025

The Honorable Robert F. Kennedy, Jr.
Secretary
Department of Health and Human Services
200 Independence Ave. SW
Washington, D.C. 20201

The Honorable Anthony Archeval
Acting Director
Office for Civil Rights
200 Independence Ave. SW
Washington, D.C. 20201

Submitted electronically via regulations.gov

RE: RIN 0945–AA22; HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Secretary Kennedy and Acting Director Archeval:

On behalf of the American Academy of Family Physicians (AAFP), which represents 128,300 physicians and medical students nationally, I write in response to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) notice of proposed rulemaking (NPRM) to amend the Security Standards for the Protection of Electronic Protected Health Information (''Security Rule'') under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The AAFP supports several of the goals outlined in this proposed rule and appreciates HHS attempting to update existing standards to better protect the confidentiality, security, and availability of electronic protected health information (ePHI) for patients nationwide.

Confidentiality and privacy are foundational elements of the patient-physician relationship and are particularly important in family medicine, where long-term relationships facilitate continuity of care and build trust. Only in a setting of trust can a patient share the private feelings and personal history that enable their family physician to provide whole-person care through accurate and timely prevention, diagnosis, and treatment. While clinicians and health care organizations must follow

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

the Security Rule which guards against disclosures of ePHI, the proposed changes outlined here are intended to increase cybersecurity for ePHI, thereby better protecting patient data and strengthening patient trust.

The AAFP has long supported policies that guarantee the appropriate security of protected health information while working to improve patients' access to their data, as well as the ability to share patients' health information across their chosen care team. We are strongly supportive of making data reliably interoperable while maintaining patient confidentiality, and we acknowledge that ensuring health data privacy long-term is going to require a federal citizen data privacy law and regulatory framework. The AAFP agrees with HHS that updating the Security Rule and improving cybersecurity for ePHI is critically needed. **However, the AAFP has serious concerns regarding some of the provisions outlined in this proposed rule, especially those that may disproportionately impact small and independent physician practices, including unrealistic compliance timelines and requirements with significant financial implications. We strongly urge the Department not to finalize this rule as proposed, as we do not believe it is possible for physician practices to successfully implement it as written. Instead, the AAFP urges HHS to either make significant changes or withdraw the proposed rule. We stand ready to collaborate with HHS, OCR, and all other stakeholders to find effective, achievable, and affordable ways to improve the security of ePHI for the benefit of patients, family physicians, and the entire health care system.**

The combined depth and breadth of these proposed requirements on an extremely short timeline presents significant challenges, and the unfunded mandates outlined in this regulation would cause financial strain for physician practices and hospitals of every size. Additionally, the potential economic impact of this proposed rule should not be overlooked. The financial burden imposed by these new requirements could have far-reaching consequences on the health care system, which comprises more than 15 percent of the nation's economy.[i] Increased costs for compliance would likely lead to higher health care costs for patients, reduced investment in other critical areas, and the undermining of patient access—particularly in rural areas. The AAFP is concerned that the condensed timeline and rigid requirements proposed here could

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

hinder the creation and adoption of new technologies and workflow practices that seek to improve patient care and operational efficiency, directly conflicting with HHS' stated goals.

Among other recommendations detailed below, **the AAFP urges HHS to**:

- **Not eliminate the categories of "addressable" and "required" implementation specifications, which would cause all implementation specifications to be required for all physician practices and remove physician autonomy;**
- **Significantly extend the compliance period outlined in this regulation and utilize a phased approach, such as offering different compliance timelines for practices of varying sizes; and**
- **Provide physician practices with hands-on technical assistance – such as the support offered by Regional Extension Centers (RECs) – in addition to providing financial and educational resources that will enable practices to afford and successfully navigate implementation of cybersecurity enhancement provisions.**

Eliminating "Addressable" Implementation Specifications

HHS proposes to update HIPAA implementation specifications so as to remove the current categories of "addressable" and "required" and instead clarify that compliance with all implementation specifications included in this rule would be required. The Department believes some regulated entities "proceed as if compliance with an addressable implementation specification is optional—and that where there is an addressable implementation specification, that compliance with the relevant standard is also optional." HHS states that compliance with implementation specifications that are currently classified as "addressable" is not optional and should not be interpreted as such. The Department believes eliminating the category of "addressable" implementation specifications will provide regulated entities with increased clarity and specificity regarding how to fulfill their obligations.

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

Expanding physicians' administrative burdens by increasing requirements while eliminating practices' ability to implement the cybersecurity features that are most appropriate for their individual situations is not an effective way to improve the cybersecurity of ePHI. **The AAFP believes that the significant majority of regulated entities are complying with addressable implementation specifications as they deem reasonable and appropriate, and we disagree with HHS' assertion otherwise. We strongly urge the Department not to move forward with this change, as we believe it is essential for practices to have the flexibility to assess the requirements and implement the solutions most reasonable and appropriate for their particular circumstance**.

Administrative functions and regulatory compliance already overburden family physicians at the point of care and after patient care hours, making it one of the driving factors fueling health care consolidation and forcing many primary care practices to either sell or close their doors altogether. Studies have estimated that primary care physicians spend nearly 50 percent of their time on cumbersome administrative tasks.[ii] As proposed, federal cybersecurity standards applicable to multibillion-dollar health plans and information clearinghouses would be identical to those that apply to small and rural physician practices. **Though the AAFP is deeply supportive of updating HIPAA standards to better protect the confidentiality, security, and availability of ePHI for patients nationwide, we do not believe it would strengthen cybersecurity in health care to significantly increase the number of regulatory requirements applicable to physician practices while limiting their autonomy in implementing solutions**.

In addition to administrative workload concerns, this regulation change would markedly increase the information technology (IT) needs and costs for small practices. Many small and rural clinics do not have the financial resources to have a full-time IT employee on staff. Instead, a small practice might hire an IT contractor on a part-time basis, where the contractor would be on-site at the practice only a few days a month, if at all. If the number of required implementation specifications suddenly increased, particularly on the condensed timeline proposed in this rule, each physician practice with a part-time IT contractor would then need significantly

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

more of that person's time—an unanticipated and not incidental expense. **The AAFP urges HHS not to increase financial and administrative burdens on physician practices and to instead leave addressable implementation specifications in current form**, with choices to: 1) implement the addressable implementation specifications; 2) implement an alternative security measure to accomplish the same purpose; or 3) not implement either an addressable implementation specification or an alternative, if deemed reasonable and appropriate. The choice is required to be documented, clarifying the regulated entity's thought process, and this existing flexibility allows physician practices to make the cybersecurity decision that is most appropriate for their circumstance.

Compliance Timelines

The Department proposes a compliance timeline of 180 days from the effective date of the final rule. HHS believes that most of the existing Security Rule's obligations for regulated entities would not be significantly altered by the proposed changes outlined here, making the standard 180-day compliance period appropriate. Additionally, the Department proposes offering regulated entities a transition period, which is separate from the 180-day compliance period, to modify business associate agreements (BAAs) or other written arrangements. This transition period would last until: 1) the BAA's renewal date (on or after the compliance date); or 2) a year after the effective date of the final rule.

The AAFP believes the compliance timeline outlined here is overly ambitious and not realistically achievable, regardless of a practice's size or available resources. We strongly urge HHS not to finalize these changes as proposed and to instead extend the compliance period to allow regulated entities more time to implement required changes. We recommend a phased approach to compliance, with hospitals and large health systems required to comply first and small, independent, physician-owned practices given the longest implementation timeline. Alternatively, the Department could use a multi-deadline phased approach, with different deadlines for various requirements within the rule.

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

Conducting thorough risk assessments, updating BAAs, implementing rigorous cybersecurity measures, and training staff on new protocols all require significant time and effort. For many practices, especially those with limited financial and technological resources, meeting the proposed timeline would prove extremely challenging. **If HHS chose a phased approach based on practice size, the AAFP would support a compliance timeline of no less than one year for hospitals and large health systems, physician-owned practices with 10 or more physicians given a timeline of no less than two years, and physician-owned practices with nine or fewer physicians given a three-year timeline in which to comply. If the Department instead chose staggered deadlines for different components of the rule, the AAFP would support the first deadline being no less than two years from the effective date of the final rule**.

The AAFP is supportive of the outlined transition period for updating BAAs and other written agreements **only if** the compliance timelines are extended or phased in as we proposed in the preceding paragraph. Given the extensive challenges physician practices would face in adhering to the compliance timelines the Department has proposed in this regulation, we do not feel it would be appropriate to layer other timelines on top of it.

Cost of Implementation

In the Regulatory Impact Analysis (RIA) section of this proposed rule, HHS estimates that if adopted, it "would impose mandates that would result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of more than $183 million in any one year."

The AAFP does not agree with the cost estimate conclusions in the RIA, and we are confused by the extreme disparity between what's been published in this proposed rule and what the public has otherwise been told regarding the cost of these proposals. The AAFP believes the actual costs associated with implementing the proposals in this regulation would be significantly higher than what's outlined here and agrees that updating these standards would likely cost billions of dollars—"an

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

estimated $9 billion in the first year, and $6 billion in years two through five," according to a December 2024 quote from a former administration official.[iii]

While we recognize the necessity of cybersecurity enhancements to protect ePHI, the AAFP is concerned about the financial burden these new requirements would place on family physicians, particularly in smaller physician-owned practices, many of which provide essential care in rural communities. The proposed requirements, such as conducting comprehensive risk analyses, encrypting all ePHI, and implementing multi-factor authentication would necessitate significant investments in technology upgrades, staff training on new cybersecurity systems, and annual maintenance protocols. Many physician practices operate on limited budgets, and the costs associated with these proposed system upgrades may be prohibitive for some.

If the Department moves forward with finalizing this rule, the AAFP strongly urges HHS to provide practices with financial resources so that they will be able to afford to implement these provisions. We also strongly recommend the Department offer comprehensive technical assistance for implementation and educational resources to all practices so these new regulations can be navigated without the need to hire additional IT help or incur excessive costs. We encourage HHS to target such resources for physician-owned practices who often lack the capital or operating margins to cover these expenses—particularly on such a short timeframe. Education, resources, and services that are developed for use in small and independent practices can often be modified to work in larger and more integrated practice environments, while the reverse is less applicable. We encourage HHS to prioritize the development of specific resources for small practices with a physician audience in mind, given that many solo practitioners and rural practices do not have consistent access to IT expertise.

Clarifying Business Associate and Health IT Vendor Obligations

Though current HIPAA regulations are robust, privacy and security protections are limited to covered entities, such as physician practices, and their business associates through BAAs. This framework places an undue burden on practices to ensure compliance across multiple business associates via individual agreements, requiring

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

staff time and financial resources many practices do not have to spare. As health care continues to evolve and the proliferation of digital health technologies increases, the number of entities interacting with ePHI has grown exponentially, causing the traditional BAA mechanism to become increasingly cumbersome and inadequate in managing the comprehensive privacy and security of ePHI. Many covered entities, particularly small practices, lack the expertise to manage the cybersecurity practices of their business associates. We recommend the Department consider how best to enforce accountability for business associates, rather than shifting this responsibility to practices.

Additionally, the AAFP encourages HHS to examine the practical limitations of a covered entity's control over certain technical safeguards. For instance, many physician practices rely on vendors for IT updates and protections to firmware and anti-malware. Given how few physician practices can afford to have full technical infrastructure and expertise in-house, we recommend the Department clarify that health IT vendors bear primary responsibility for ensuring timely and effective technical updates. Particularly for high-impact situations, such as a vendor ceasing operations or discontinuing support for critical systems, mechanisms need to be established to mitigate any investments in new technology physician practices may need to make to replace outdated or unsupported systems.

Definitions

In Section 160.103, HHS proposes to revise and expand the definition of "electronic media" to reflect the increased role technology now plays in the storage and transmission of health data as compared to 2013, when the Security Rule was last updated. The updated definition would clarify that "electronic media" includes any media on which data may be recorded, maintained, or processed, as well as include a list of "electronic storage material" examples to account for future technologies where data could be stored or processed. The Department also proposes to modify the description of "transmission media" to clarify that almost all health data is transmitted via technology today, including data transmitted via fax or telephone, and that only data handwritten on paper and hand-delivered or mailed would be excluded from the updated definition of "electronic media".

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

The AAFP appreciates the clarity provided in this updated definition, and we support these proposed changes. Far too many exchanges of health data still occur via fax and telephone, and patients deserve their data to be as secure when transmitted through these modes as it would be if transmitted from one electronic health record (EHR) system to another. We believe health IT and the health care data ecosystem must facilitate efficient information sharing without undue financial or administrative burden on physician practices. These proposed changes will help facilitate safe, timely information sharing for patients and physicians.

In Section 164.304, HHS proposes to modify the definitions of 15 terms used in the Security Rule, as well as proposing to add and define ten new terms. The Department believes these updates would modernize or otherwise clarify how regulated entities should apply Security Rule standards and specifications.

While we are generally supportive of these proposed definitional changes and additions, the AAFP remains concerned that federal agencies use a variety of definitions for key terms, including "electronic information system", "multi-factor authentication", and "electronic media". Disparate definitions for the same terms across different health IT and other regulations can create confusion and add to the burden for physician practices working to ensure they are in compliance. **We urge HHS to collaborate with its counterparts across the agencies to align terms and definitions used in rulemaking with other health and IT regulations**.

Conclusion

Thank you for the opportunity to provide comments on this proposed rule; the AAFP appreciates HHS' ongoing efforts to strengthen the security, integrity, and availability of ePHI. We again urge this regulation either be withdrawn as soon as possible or finalized only if the significant changes outlined above are incorporated. The AAFP looks forward to continuing to partner with the Department and other stakeholders to increase cybersecurity standards in the health care system, reduce physician administrative burdens, and improve patients' access to their health data. Should you have any questions, please contact Mandi Neff, Regulatory and Policy Strategist, at 202-655-4928 or mneff2@aafp.org.

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org

Sincerely,

Steve Furr, M.D., FAAFP

Steven Furr, MD, FAAFP
American Academy of Family Physicians, Board Chair

[i] https://www.kff.org/health-policy-101-health-care-costs-and-affordability/?entry=table-of-contents-how-has-u-s-health-care-spending-changed-over-time
[ii] Berg S. (2020). Physician Burnout: Which medical specialties feel the most stress. AMA. Retrieved from https://www.ama-assn.org/practice-management/physician-health/physician-burnout-which-medicalspecialties-feel-most-stress
[iii] Vicens, A. J. (2024, December 27). Biden administration proposes new cybersecurity rules to limit impact of healthcare data leaks. Reuters. https://www.reuters.com/technology/cybersecurity/biden-administration-proposes-new-cybersecurity-rules-limit-impact-healthcare-2024-12-27/

1133 Connecticut Ave., NW, Ste. 1100
Washington, DC 20036-1011

info@aafp.org
(800) 794-7481
(202) 232-9033 www.aafp.org