March 4, 2025

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

Submitted electronically via www.regulations.gov

Re: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, RIN Number 0945-AA22

The American Academy of Dermatology Association (AADA) appreciates the opportunity to provide comments on the Department of Health and Human Services' (HHS) proposed modifications to the HIPAA Security Rule. The AADA represents more than 17,500 dermatologists nationwide who are committed to excellence in the medical and surgical treatment of skin disease; advocating for high standards in clinical practice, education, and research in dermatology and dermatopathology; and driving continuous improvement in patient care and outcomes while reducing the burden of disease.

We recognize the importance of strengthening electronic protected health information (ePHI) security to address evolving cyber threats and enhance patient data protection. However, the proposed rule, as written, places a significant burden on physician practices, particularly small, independent, and solo practices. The extensive updates—including expanded documentation, security oversight, and technological requirements—would increase administrative and financial strain on physicians without clear evidence that these changes would meaningfully improve cybersecurity.

While updates to the HIPAA Security Rule may be warranted, any finalized requirements must be practical, scalable, and achievable across different practice settings. We strongly

CORRESPONDENCE
PO Box 1968
Des Plaines, IL 60017-1968
EMAIL: mrc@aad.org
WEB: aad.org

ROSEMONT, IL OFFICE
9500 W Bryn Mawr Avenue, Suite 500
Rosemont, IL 60018-5216
MAIN: (847) 330-0230
FAX: (847) 240-1859

WASHINGTON, DC OFFICE
1201 Pennsylvania Avenue, NW, Suite 540
Washington, DC 20004-2401
MAIN: (202) 842-3555
FAX: (202) 842-4355

urge HHS to reconsider the scope and feasibility of the proposed changes to ensure they do not impose unnecessary and unsustainable financial and operational burdens on physicians.

I. Expanded Compliance and Documentation Burdens

In its current form, the proposed rule significantly expands compliance obligations, introducing more frequent risk assessments, mandatory security training, detailed documentation, and technology asset tracking. While updates to security requirements may be necessary to address emerging cyber threats in an evolving healthcare security landscape, any regulatory changes must be practical and balanced against the operational realities of physician practices.

Without modification, the proposed requirements risk placing a significant burden on physician practices with fewer resources to dedicate to compliance. For small and independent practices, which are common in dermatology, these requirements may introduce significant financial strain and operational challenges that may impact patient care.

While documentation, audits, and compliance reporting are essential components of security oversight, they must be structured in a way that effectively enhances cybersecurity without imposing excessive administrative burdens. Compliance efforts should be designed to support meaningful security improvements while ensuring that limited resources remain available for direct patient care and essential operations. If not properly calibrated, the proposed updates to the HIPAA Security Rule could force physicians to allocate significant time and resources toward administrative compliance rather than investing in proactive cybersecurity measures such as real-time threat detection and mitigation.

Further, it is unclear whether the proposed updates would meaningfully enhance cybersecurity protections. Much of the rule's focus is on documentation, auditing, and compliance reporting—all important elements of security oversight—but these do not necessarily translate into improved protection against cyber threats.

The AADA does not support the proposed rule in its current form. As the agency evaluates potential changes to the HIPAA Security Rule, we urge HHS to consider the financial and operational challenges physicians will face in meeting new and expanded security requirements. Any updates must ensure that compliance expectations are practical, scalable, and structured in a way that supports security goals without creating unnecessary administrative strain on physicians.

II. Technical Standards and Compliance Challenges

If finalized, the proposed rule would introduce highly technical security obligations that would require substantial adjustments for regulated entities, including physician practices. While many

practices already engage IT personnel or external cybersecurity vendors to meet existing security requirements, gaining compliance with these expanded technical standards would increase costs, administrative burdens, and oversight at the practice level. Even when security functions are outsourced, physician practices remain responsible for ensuring compliance and integrating security protocols into their operations, which may strain already limited resources, particularly in small or independent practices.

The proposed rule includes new and revised security measures, such as mandatory encryption of all ePHI at rest and in transit, implementation of multi-factor authentication, and stricter patch management policies requiring remediation of critical vulnerabilities within 15 calendar days. While some of these measures can be addressed through automated software, other proposed measures would require physician practices to conduct manual, resource-intensive processes, such as maintaining a comprehensive inventory of technology assets, conducting formalized compliance audits, and ensuring annual risk assessments are thoroughly documented. The rule also mandates contingency planning measures, requiring data backup and recovery protocols capable of restoring ePHI within 72 hours of a breach.

Additionally, the proposal removes the distinction between "addressable" and "required" standards in most cases, reducing flexibility for physicians to implement security measures based on their specific needs and technical capabilities. For smaller practices with limited IT resources, this change could impose rigid, prescriptive requirements without significantly improving security protections.

HHS must ensure that any new or revised technical requirements are practical, scalable, and achievable for physicians. As written, the proposed rule introduces highly technical and complex security mandates that may be unmanageable for small and independent practices, which the AADA does not support. As HHS evaluates future updates to the HIPAA Security Rule, we encourage the agency to consider financial and technical support mechanisms that help small and independent practices meet security requirements without diverting critical resources from patient care.

III. Financial Strain of Compliance Mandates

The AADA supports efforts to strengthen cybersecurity and protect ePHI but does not support the proposed rule in its current form due to the significant financial burden it would impose, as well as broader concerns about its feasibility and impact on physician practices Compliance costs extend beyond initial technology upgrades to include ongoing expenses such as cybersecurity monitoring, staff training, and third-party security assessments—placing additional strain on practice resources, whether IT services are managed internally or outsourced.

Small practices, which often have fewer financial reserves than larger healthcare systems, would face disproportionate challenges in absorbing these costs. Security investments—such as multi-factor authentication, real-time cybersecurity monitoring, and meeting strict patch management timelines—require both financial and operational resources that may divert funding away from patient care, staffing, and other essential practice operations.

If finalized as proposed, the rule would require substantial investments in technology, security infrastructure, and workforce training, with most measures needing to be implemented within 180 days of the final rule's effective date—a significant challenge for many physicians and physician practices.

The AADA is concerned that the compliance burden and associated costs in the rule's current form are too significant. At the same time, physicians continue to face year-after-year Medicare cuts that do not keep up with the cost of medical practice, unlike other providers, such as hospitals, that receive annual payment updates based on inflation. These ongoing financial challenges only heighten the difficulty of meeting the rule's extensive compliance requirements. As written, the proposed rule would exacerbate these financial pressures, making compliance even more challenging, particularly for small and independent practices.

As HHS evaluates potential changes to the HIPAA Security Rule, we strongly urge the agency to consider strategies that mitigate financial strain on physicians. This includes phased implementation timelines, technical assistance programs, and financial support mechanisms to help practices comply without causing undue disruptions to patient care.

IV. Increased Burden of Vendor Oversight

Business associates, including IT vendors and cybersecurity firms, play an important role in supporting security and compliance efforts. While we support strengthening ePHI protections, the rule in its current form would significantly shift oversight responsibilities onto physicians. If finalized as written, it will require physicians to take on expanded roles in vendor compliance, renegotiating agreements, and verifying security assurances.

These changes could disrupt vendor relationships, making it harder for physicians—especially those in small practices—to secure services that meet their needs. Additionally, increased oversight requirements may have unintended consequences, such as discouraging physician participation in clinical data registries.

Clinical data registries play a vital role in improving patient care by collecting and analyzing data to support quality improvement, research, and evidence-based decision-making. However, added compliance obligations and administrative burdens may deter participation, particularly

for smaller practices with limited resources. A decline in registry participation could, in turn, hinder advancements in patient care and outcomes, undermining broader public health goals.

While the AADA supports efforts to strengthen ePHI protections and cybersecurity, we do not believe the proposed rule appropriately accounts for its impact on physician-business associate relationships. We encourage HHS to assess how the proposed changes may affect physicians' ability to coordinate with business associates while ensuring compliance.

The proposed rule requires clarification of oversight responsibilities, and any future updates to the HIPAA Security Rule should include clear, practical implementation strategies to prevent unnecessary disruptions to vendor relationships.

V. Cybersecurity Gaps in Non HIPAA-covered Entities

HIPAA establishes security and privacy requirements for covered entities and their business associates, but it does not extend to many other entities that handle patient data. Likewise, the proposed rule does not address cybersecurity risks associated with these non-covered entities, raising concerns about data security gaps and regulatory inconsistencies.

Currently, the HIPAA Security Rule applies only to covered entities such as healthcare providers, health plans, and clearinghouses, as well as their business associates. Non-covered entities, including health apps, direct-to-consumer platforms, and other technology companies, are not subject to the same security and privacy requirements. With the expanding role of these entities in healthcare—especially with the rise of artificial intelligence, telehealth, and patient-generated health data—there is a growing need to assess and address cybersecurity vulnerabilities that fall outside of HIPAA's current scope.

Without uniform security requirements that apply across all entities handling patient data, physician practices may still face indirect risks when engaging with non-HIPAA-covered entities. Data shared through these technologies may be more vulnerable to breaches, creating liability concerns, regulatory uncertainty, and risks to patient trust. Additionally, if a non-HIPAA-covered entity experiences a data breach, physician practices could still be impacted—even when the breach occurs outside their direct control.

To ensure a more comprehensive approach to cybersecurity, we strongly encourage HHS to explore broader protections beyond HIPAA's current framework. A coordinated, multi-agency effort involving relevant industry stakeholders could help establish appropriate security safeguards for physician practices interacting with non-covered entities. However, we reiterate that efforts to expand security protections should prioritize effectiveness while avoiding unnecessary compliance burdens on physician practices.

VI. Supporting Small Practices in Meeting Compliance

To reiterate, the AADA does not support the proposed rule as written. We believe it does not adequately consider the challenges physicians, particularly small and independent practices, face in implementing new and revised regulatory requirements. As HHS evaluates potential changes to the HIPAA Security Rule, it is critical to ensure that any future updates account for the varying resources and capacities of physician practices.

Small and independent practices are generally subject to the same compliance requirements as larger healthcare organizations, even though they often lack the administrative and financial resources to manage complex regulatory requirements. **If HHS decides to move forward with the proposed changes, at a minimum, the agency must incorporate practical and adaptable solutions into any future updates, such as standardized resources, role-based training, and regulatory flexibility tailored to the needs of small practices.**

Tailored Resources and Training

Providing small practices with accessible compliance tools and training options can support their ability to meet security requirements without undue administrative burden. As HHS considers future updates, it should:

- Develop a simplified risk assessment template specifically designed for small practices to streamline compliance while maintaining security integrity.
- Provide a standardized business associate compliance verification tool, reducing the need for individual practices to develop their own oversight frameworks.
- Offer training alternatives, such as role-specific programs, that scale based on ePHI access levels. A flexible approach to training requirements can help reduce administrative burdens while maintaining strong security protections. Allowing adjustments in training frequency for lower-risk roles could further support small practices in managing compliance without unnecessary burden or added financial strain.

Regulatory Flexibilities

Recognizing the resource constraints of small practices, we urge HHS also to consider targeted regulatory flexibilities to support physician compliance. Such flexibilities may include:

- Exempting small practices below a certain size or revenue threshold from annual compliance audits to allow resources to remain focused on patient care while maintaining security standards.
- Providing extended implementation timelines to give small practices sufficient time to adopt new security measures without disrupting operations.
- Tailoring compliance requirements based on practice size and capabilities, building on HHS's previous efforts to provide regulatory flexibility for small practices. For example, under the Quality Payment Program (QPP), HHS established hardship exemptions and

alternative reporting pathways to ease compliance burdens for small practices. A similar approach to HIPAA Security Rule compliance could help ensure security measures are both effective and feasible across all practice settings.

Providing targeted support for small practices, including practical resources and regulatory flexibilities, would help facilitate physician compliance with any new or updated security requirements while minimizing disruptions to physician operations.

VII. New and Emerging Technologies Request for Information

HHS has requested input on how artificial intelligence (AI) and other emerging technologies can be leveraged to strengthen cybersecurity protections for ePHI. AI-driven security tools offer potential benefits, such as enhanced threat detection, automated security monitoring, and predictive risk assessments, all of which could improve data protection for physician practices. At the same time, AI introduces unique risks, particularly regarding data privacy, cyber threats, and compliance with HIPAA security requirements. AI-driven cybersecurity models must be transparent, explainable, and validated to ensure they do not inadvertently expose ePHI, create unintended vulnerabilities, or introduce new complexities in risk management. Additionally, AI-powered cyber threats—such as automated phishing attacks and adaptive malware—may present greater challenges for physician practices, particularly those with limited IT resources.

As AI security tools continue to evolve, physician practices may need greater clarity on how these technologies intersect with HIPAA compliance obligations, including risk assessments, data governance, and incident response expectations. AI-generated cybersecurity recommendations should be aligned with existing regulatory frameworks to prevent unintended security gaps, and clear oversight mechanisms should be in place to ensure compliance. However, as AI-driven cybersecurity advances, small practices risk being left behind due to cost barriers. Unlike large health systems, they may lack the resources to implement these tools. We urge HHS to ensure equitable access through subsidies, grants, or cost-sharing programs, preventing undue financial burden.

Additionally, the potential for AI bias in cybersecurity threat detection models should be carefully evaluated. Unintended biases could lead to false positives or missed vulnerabilities, potentially increasing security risks for physician practices. Regulatory safeguards should ensure AI tools used in cybersecurity are rigorously tested, regularly updated, and do not introduce new compliance challenges.

We encourage HHS to consider how advancements in AI-driven security tools may impact physician practices' ability to comply with both current and any future HIPAA requirements. Additionally, HHS should consider whether additional guidance is needed to help practices assess and mitigate AI-related risks to ePHI.

VIII. Conclusion

The AADA opposes the proposed rule as written and urges HHS to reevaluate its approach to ensure the feasibility of any updated security requirements for physicians. While we recognize the importance of strengthening ePHI protections and safeguarding patient data against evolving cyber threats, any changes to the HIPAA Security Rule must be practical and achievable across all practice settings—particularly for small and independent physician practices that may face significant financial and operational challenges.

As HHS considers future modifications to the HIPAA Security Rule, it is critical that compliance expectations remain flexible, scalable, and practical to account for the varying capabilities of physician practices. Implementing security requirements in a way that balances strong protections with feasible compliance pathways will help maintain cybersecurity standards without placing unnecessary strain on physician practices. A balanced approach that allows for flexibility in implementation will support physician practices in meeting security requirements effectively while continuing to provide high-quality patient care.

The AADA appreciates the opportunity to provide input and urge HHS to consider these factors to support both strong security protections and sustainable compliance for physicians. If you have any questions regarding this letter, please contact Cameron Huff, Manager, Payment Policy at chuff@aad.org or 847-240-1958.

Sincerely,

Seemal R. Desai, MD, FAAD
President, American Academy of Dermatology Association