



**AMERICAN
PSYCHOLOGICAL
ASSOCIATION**
SERVICES, INC.

March 7, 2025

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: **Proposed Revisions to the HIPAA Security Rule to Strengthen the Cybersecurity
of Electronic Protected Health Information (RIN 0945-AA22)**

To Whom it May Concern:

On behalf of American Psychological Association Services Inc. (APA Services), the companion organization of the American Psychological Association (APA), we are writing to provide comments to the Office of Civil Rights (OCR) for the US Department of Health and Human Services (HHS) in response to the proposed rulemaking to revise the Security Rule of the Health Information Portability and Accountability Act of 1996 (HIPAA), published in [90 Fed. Reg. 898](#) on January 6, 2025.

APA is the largest scientific and professional organization representing psychology in the United States, with a membership of over 173,000 clinicians, researchers, educators, consultants, and students. APA's mission is to promote the advancement, communication, and application of psychological science and knowledge to benefit society and improve lives.

We applaud OCR for taking steps to review and propose updates to the HIPAA Security Rule to reflect the changes in the use of technology in health care service delivery, health care claims processing, recordkeeping, and communications with patients, other providers and payers since HIPAA was first enacted nearly 30 years ago. With the growing adoption of technologies and tools in modern health care, there is a concurrent risk to the electronic health data that is generated, shared, and maintained across the health care ecosystem. That risk can be due to technological malfunctions, inadvertent human error, environmental events, or intentional bad acts such as theft, malware, or other kinds of cyberattacks. Hence, the need for more robust security measures and policies to protect against unauthorized access of sensitive patient data is critical as most recently evidenced by the 2024 Change Healthcare cyberattack, impacting now upwards of 190 million individuals and numerous health care practices and systems.¹

¹ [190 million people affected by Change Healthcare cyberattack, says UHG](#), Healthcare Finance News, Jan. 28, 2025.

APA.ORG
APASERVICES.ORG

Advocating for APA members and psychology

750 First Street, NE
Washington, DC 20002-4242

202.336.5800
202.336.6123 TDD

In response to this proposed rule, APA Services welcomes the opportunity to provide our perspective on some of the proposals to strengthen cybersecurity of patients' electronic protected health data especially information involving mental and behavioral health and substance use treatment (MH/BH), which may be entitled to heightened privacy protections given the sensitivity of the health data.

However, we would like to highlight the potential consequences for small and solo psychological practices (small practices), which are representative of many APA members, and make the following recommendations:

- **Exemption:** Provide an exemption for small practices from the additional security measures highlighted below as being particularly onerous for those practices.
- **Flexibility in Implementation:** Maintain most "addressable" implementation specifications for small practices to enable them to determine which are reasonable and appropriate for their practices.
- **Timeline Extensions:** In the alternative, grant an extended implementation timeline for small practices to better prepare for compliance as developers adapt their tools and products to empower providers to comply with additional Security Rule requirements.
- **Financial Support:** Develop financial assistance or grant programs to support small practices to acquire or upgrade their technology tools and cybersecurity measures.
- **Specific Resources and Guidance:** Develop specific resources and guidance tailored to small practices to help them navigate the new requirements and provide clear examples of how to scale various cybersecurity measures.

These recommendations, which are discussed in greater detail in Section C below, are important because small practices are disproportionately impacted by the significantly increased requirements of the proposed rule. This is because they have limited resources, both in terms of staffing and budget. They lack dedicated IT staff and often must manage technology-related tasks themselves. The proposed rule requires a level of technical expertise that many small practices simply do not possess. Hiring external consultants to fulfill these requirements would impose a significant financial burden, potentially jeopardizing the viability of many small practices at a time when demand for mental health services is extremely high.

These resource limitations are discussed further below.

A. Resource Challenges for Small Psychology Practices

Below are some of the challenges that many small practices already face in the current health ecosystem:

1. **Lack of Funding:** Non-physician health care providers often operate with limited financial resources. Unlike hospitals or larger physician groups (for which EHR adoption rates are

often cited as 97% and 78% respectively²), they did not have access to HITECH grant funding to invest in new technologies like certified electronic health records (EHRs).

- **High Initial Investment:** Implementing healthcare technologies like EHRs can require a substantial initial investment. Costs include purchasing hardware, software licenses, and potentially upgrading existing infrastructure.
 - **Ongoing Maintenance Costs:** Apart from the initial setup, there are ongoing costs for software updates, system maintenance, and potential security upgrades. Small practices may find it difficult to sustain these continual expenses.
2. **Limited IT Support:** Smaller practices are unlikely to have dedicated IT staff to facilitate the adoption, customization, and maintenance of EHR systems to ensure HIPAA Security Rule compliance.
 - Lack of in-house IT expertise can lead to challenges in customizing and optimizing health care technologies to meet the specific needs of the practice, leading to inefficiencies.
 - Without adequate IT support, small practices may find it difficult to keep up with evolving cybersecurity threats and compliance requirements. Furthermore, making all these stringent requirements mandatory under the premise of more security, the proposed rule removes the flexibility for organizations to prioritize their security efforts based on their specific needs and vulnerabilities. This could lead to a situation where they are forced to spread their limited resources thinly across all areas, potentially neglecting critical vulnerabilities, making them more susceptible to cyberattacks.
 3. **Training and Support:** Providers may lack access to comprehensive training programs for new technologies. This can make it more difficult to integrate these technologies into their workflows effectively. For those operating a small practice, they look for technological tools that are simple to install and use, relying largely on the product developers to ensure that the tools adhere to HIPAA Security Rule and related requirements.
 4. **Perceived Relevance:** There can be a perception that some health care technologies are more relevant to traditional medical practices than to non-physician providers like MH/BH providers, potentially reducing motivation to adopt these systems. In addition, the administrative and technical costs for many of the provisions in the proposed rulemaking outweigh the cybersecurity risks that small practices may pose. It is worth noting that the greater risks lie with larger organizations like the ransomware attack on Change Healthcare which resulted in an unprecedented breach of sensitive data.

² A Unified Approach to Health Data Exchange: A Report from the US DHHS, *JAMA*, published online Jan. 18, 2025, <https://doi.org/10.1001/jama.20250068>.

B. Specific Comments on Proposed Changes to the Security Rule

1. Administrative Safeguards – Section 164.308 (pp. 934-955)

Technology asset inventory and network map (pp. 936-938): The mandate for detailed technology asset inventory and network maps is particularly onerous. To start, the rapid pace of technological change makes it difficult to maintain up-to-date inventories and network maps, especially given the proposed requirement to update after *any change* affecting ePHI. Even seemingly minor changes, like software updates or the addition of a new connected device, would trigger a potentially time-consuming review and update process. The inclusion of IoT (Internet of Things) devices,³ which may indirectly affect ePHI security, adds another layer of complexity. Small practices may not even be fully aware of all such devices connected to their networks, making it difficult to account for them in the detailed inventory and network map.

Risk Analysis, Evaluation, Patch Management and Risk management Requirements (pp. 938-944): Elevating risk analysis from an addressable to a mandatory implementation specification with detailed requirements significantly increases the complexity and documentation burden. The requirement for a risk analysis to be performed at least every 12 months, with updates required whenever any change affecting ePHI occurs, adds a significant burden to small practices. This analysis must include: analyzing the technology asset inventory and network map; identifying and documenting all reasonably anticipated threats to ePHI; assessing vulnerabilities in electronic information systems; evaluating the effectiveness of existing security measures; determining the likelihood of threats exploiting vulnerabilities and the potential impact of such events; assigning risk levels to each identified threat and vulnerability; and, assessing risks associated with business associate agreements.

Small practices will struggle to dedicate the necessary time and resources to conduct a thorough risk analysis, evaluate changes, and implement patch management procedures based on these requirements, especially given the stringent timelines proposed for addressing vulnerabilities. The proposed rule outlines specific timeframes for applying patches based on the level of risk, requiring action within 15 days for critical risks and 30 days for high risks. It is not clear from a technical standpoint whether these timeframes are feasible. Furthermore, this rigid schedule can be challenging for small practices, who may need more flexibility to adequately test and implement patches without disrupting operations since small practices typically do not have dedicated IT staff. These requirements demand a high level of technical expertise to understand vulnerabilities, assess risks, and implement appropriate security measures. Many small practices lack in-house expertise and will find it financially prohibitive to acquire it externally. The need for ongoing monitoring, evaluation, and updates, especially in response to the ever-changing threat landscape, adds another layer of complexity that small practices may find difficult to manage.

³ The Internet of Things (IoT) can be defined in its simplest scenario as a network that connects uniquely identifiable devices (or *things*) to the internet, enabling them to collect, send, store, and receive data [4]. From a health care perspective, IoT can be considered as any device that can collect health-related data from individuals, including computing devices, mobile phones, smart bands and wearables, digital medications, implantable surgical devices, or other portable devices, which can measure health data and connect to the internet [5]. Kelly JT, Campbell KL, Gong E, Scuffham P. (2020). The Internet of Things: Impact and Implications for Health Care Delivery. *J Med Internet Res*, 22(11), e20135. <https://doi.org/10.2196/20135>.

Requirement for information system activity review (pp. 946-947): The proposed changes to information system activity review requirements create additional obstacles. The mandate for regular review of various logs and reports, including audit trails, event logs, and security incident tracking reports, is a significant undertaking for small practices, especially those without dedicated IT staff. This is further complicated by the fact that small practices often lack the resources to invest in automated tools for log aggregation and analysis. Manual review of these logs can be incredibly time-consuming and require technical expertise to identify suspicious activity, which small practices often do not have. Not only is establishing policies and procedures for retaining and reviewing records of activity complicated and time-consuming, but the maintenance of such policies is also an ongoing burden. The requirement to review and test these written policies and procedures at least once every 12 months further adds to the administrative workload of small practices.

Assigned Security Responsibility, Workforce Security, Information Access Management, and Security Awareness Training (pp. 947-953): The cumulative effect of these proposed changes necessitates significant operational adjustments for small practices. Developing, reviewing, testing, and auditing various policies and procedures related to risk analysis, risk management, information system activity review, sanction policies, workforce security, information access management, security incident procedures, and contingency planning will be incredibly challenging and resource intensive. Developing comprehensive and legally sound policies and procedures often requires specialized knowledge that many small practices do not possess. In addition, requirements such as formally designating a Security Official, establishing procedures for authorizing and terminating workforce access to ePHI, implementing timely notification protocols, managing role-based access controls, verifying user and technology asset identities, segmenting networks, and providing ongoing security awareness training, seems excessive for small practices with minimal, if any, staff and more appropriate for larger organizations.

Security Incident Procedures, Contingency Plan, Compliance Audit (pp. 953-955): Specifically, the proposed requirements for documenting all security incidents, including verbal reports, and maintaining such documentation for six years, creates a substantial administrative burden for small practices. Similarly, the mandate to establish and implement written procedures for creating and maintaining retrievable copies of ePHI and restoring critical systems and data within 72 hours of a loss presents significant operational challenges. As an initial matter, we are not confident that restoration of services within 72 hours is necessarily feasible for many systems. But meeting this 72-hour restoration requirement will be particularly difficult for small practices that lack dedicated IT staff and resources, potentially requiring significant financial investment in backup and recovery solutions. Additionally, the requirement to review and test contingency plans at least annually, document the results, and modify plans as needed further adds to the administrative burden faced by small practices. Overall, small practices, which constitute the majority of psychology businesses, lack the personnel and financial resources to dedicate to these tasks, diverting valuable time away from patient care. The added burden of all the requirements above, including conducting frequent contingency plan testing, further complicates their operations.

2. **Technical Safeguards** – Section 164.312 (pp. 962-980)

We have identified the following proposed changes to the technical safeguards that appear to be the most challenging:

- **Audit trail and system log control:** The proposal mandates the deployment of technology that records and identifies activity in all of the practice's relevant electronic information systems, not just those that directly handle ePHI. This requirement necessitates sophisticated technology that can monitor and analyze activity across various systems in real-time, which can be expensive and complex to implement. Additionally, the requirement to retain extensive audit logs and system activity records for a specified period adds to the storage burden and management complexity.
- **Vulnerability management:** This standard requires the implementation of technical controls to identify and address vulnerabilities in the practice's electronic information systems. This includes conducting automated vulnerability scans at least every six months and penetration testing at least every twelve months. While vulnerability scanning might be manageable with available tools, penetration testing often requires specialized expertise that many small practices lack in-house. Outsourcing this requirement to qualified security professionals would incur significant costs, straining the financial resources of small practices. Furthermore, the need to promptly install software patches and critical updates to remediate identified vulnerabilities demands dedicated time and effort, which can be challenging for small practices with limited staff and competing priorities. Since many small practices use third-party, cloud-based software, they would be unable to conduct vulnerability scans and penetration tests themselves. We ask for confirmation that small practices would be deemed as compliant so long as they use software that attests to conducting these vulnerability management practices regularly.
- **Data backup and recovery:** The proposal mandates the implementation of technical controls to create and maintain retrievable copies of ePHI, with backups being no more than 48 hours old and to test the effectiveness of backups at least monthly. This requirement would also impose excessive administrative and financial burdens on small practices.
- **Encryption:** The proposed rule's requirement for encryption of *all* PHI in all instances is overly broad and poses significant challenges and could significantly hinder routine communications with patients. For instance, the current proposal would prohibit common practices such as sending appointment reminders via text or unencrypted email, even if the patient prefers that method of communication. Even notifying a patient about a secure message could potentially be problematic, as the notification itself could be considered PHI if it identifies the individual as a patient. This leaves little room for practical communication and creates unnecessary obstacles, especially for small practices that rely on these communication methods to coordinate care and provide essential reminders. We recommend that OCR consider a more nuanced approach to encryption that balances the need for robust security with the practical realities of patient communication in diverse healthcare settings.

3. Eliminating "Addressable" Specifications – Section 164.306(c) (pp. 933-934)

Currently, the Security Rule allows covered entities flexibility in determining how to best meet “addressable” implementation specifications. The covered entity determines whether the specification is reasonable and appropriate for the entity’s risk environment; if not, whether there are one or more available alternative security measures that would accomplish the same purpose; or whether no available security measures are reasonable and appropriate. This flexibility is crucial for small psychology practices with limited staff and resources. It allows these smaller practices to tailor their security measures to their specific needs and risk assessments, effectively managing resources while ensuring compliance. The reality is that small practices do not pose the level of cybersecurity risk or scope of adverse impact that larger practices and systems do such as Change Healthcare, Kaiser Foundation Health Plan or UCLA Health.

The proposed rule would eliminate this flexibility, requiring all implementation specifications to be met, regardless of the size, complexity, or risk profile of the organization. This rigid approach disregards the unique risks and challenges faced by small practices and could lead to the adoption of less effective and targeted cybersecurity protocols. For example, some of the most burdensome requirements that would become mandatory include:

- Extensive documentation for risk analyses, security incidents, and contingency plans: This creates a significant administrative burden for small practices with limited staff.
- Strict timelines for implementing patches and notifying other entities: meeting these timelines can be operationally challenging for small practices with limited IT resources.
- Implementing and managing technical safeguards like access controls and network segmentation: These often require specialized expertise that small practices may not have in-house IT specialists leading to increased reliance on costly external consultants.
- Meeting physical safeguard requirements: Implementing facility access controls, workstation security measures, and technology asset controls can be challenging and expensive for small practices, especially those in shared office spaces or with limited control over their physical environment. Implementing all the required physical safeguards will also involve significant costs for equipment and infrastructure upgrades. In addition, the extensive documentation, review, and testing requirements for physical safeguards policies and procedures add to the administrative burden faced by small practices with limited staff.

Overall, doing away with the concept of “addressable” implementation specifications removes a major component of the discretion previously afforded to regulated entities to create cybersecurity programs tailored to their specific circumstances and their specific risk levels and vulnerabilities. For small psychology practices, this loss of flexibility could severely hinder their ability to effectively manage cybersecurity risks while maintaining compliance with the rigorous requirements of the proposed rule. The sheer number of new and onerous requirements proposed in this rule makes it even more critical to retain the flexibility of “addressable” specifications. This would allow small practices to prioritize the most critical security measures based on their individual risk assessments and resource constraints, ultimately ensuring the protection of ePHI without compromising patient care.

By eliminating this flexibility, the proposed rule could inadvertently create a situation where organizations are forced to adopt a rigid approach, leaving them more vulnerable in areas where they are most at risk. This unintended consequence would undermine the very goal of enhancing ePHI security.

4. **Additional Requirements relating to Business Associates** – Section 164.308(b)(1) & (2)(pp. 956-957)

The proposed changes regarding business associate agreements also pose challenges. Small practices often rely heavily on business associates for various functions to support practice operations, including IT services, cloud storage and professional services. The proposed new requirements regarding business associates that would be particularly challenging for small psychological practices are:

Verification requirement: The proposed rule would require covered entities to obtain written verification, at least every 12 months, from each business associate that the business associate has deployed the required technical safeguards, including a written analysis by a cybersecurity expert of the business associate's relevant electronic information systems, and written certification from the business associate that the analysis has been performed and is accurate. Even a small practice may have multiple business associates, meaning that just tracking whether those business associates have submitted updated verifications every 12 months would be an additional administrative burden, on top of reviewing and assessing what each business associate has submitted.

Moreover, most small practices do not have the technical expertise to meaningfully assess the verifications from their business associates. They would have no way of determining if the analysis really indicates that the business associate's cybersecurity analysis is valid. We are also concerned about the statement in the preamble indicating that this proposed provision would allow the covered entity and the business associate to determine how the person providing the assessment is compensated. [90 Fed Reg 953]. The concern is that when small practices are dealing with large business associates with greater bargaining power, the business associate may seek to impose the cost of the assessment – which the practice is required to obtain -- on the small practice, further adding to the burden of this requirement.

Risk Assessment Regarding Business Associates: APA Services also believes that the proposed new implementation specification for risk assessment regarding business associates will be challenging for small practices. It would require those practices to create a risk assessment regarding the risks of starting or continuing business associate agreements, based on the written verification from the current or prospective business associate. Given the limited technical capabilities of most small practices and their consequent limited capacity to meaningfully assess these verifications, we do not believe that many of those practices could effectively assess these risks. Thus, the significant burden this requirement would impose on small practices would likely outweigh any intended benefits from it.

On the other hand, APA Services believes that psychological practices would benefit from the proposed requirement that business associate agreements include a provision that the business associate must provide notice that it has activated its contingency plan without unreasonable delay, but no later than 24 hours later. That proposal would give all psychological practices an

earlier opportunity to react and protect their IT systems from security incidents occurring at the business associate.

We also believe that the opportunity to designate a business associate as the Security Official could be beneficial for many small practices with limited technical capabilities and/or insufficient bandwidth to keep up with security responsibilities. Where a practice does this, it would be important for the practice to be able to hold that business associate accountable through its business associate agreement for any negligence or willful misconduct that results in the practice being deemed noncompliant, regardless of the fact that the practice, as the covered entity, would be ultimately responsible for its own Security Rule compliance.

Recognizing that business associates often require that their own business associate agreements be used, we would suggest that business associates include in their own agreements an attestation that the agreement complies with Security Rule requirements.

C. Recommendations

Considering the limited resources that solo and small psychology practices have to implement the extensive proposed requirements that are proposed, we offer the following suggestions for your consideration:

- **Exemption:** Provide an exemption for solo/small practices from the additional security measures highlighted above as being particularly onerous for those practices
- **Flexibility in Implementation:** Maintain most "addressable" implementation specifications for solo/small practices to enable them to determine which of those provisions are reasonable and appropriate for their practices and consider alternative security measures. This flexibility is crucial for small providers with limited resources, allowing them to tailor their security measures to their specific needs and vulnerabilities. By maintaining the "addressable" provisions, solo and small practices can prioritize the most critical and appropriate security measures based on their individual risk assessments and resource constraints. This targeted approach would enable them to implement the most impactful safeguards while still ensuring the protection of ePHI, without compromising patient care or facing undue financial strain.
- **Timeline Extensions:** In the alternative, grant an extended implementation timeline for solo and small practices to better prepare for compliance as developers adapt their tools and products to empower providers to comply with additional Security Rule requirements.

Many of the proposed changes include aggressive timelines for implementation that seem unrealistic for small practices. The general expectation of implementing most requirements within 180 days of the final rule's effective date is simply not enough time to make the necessary system changes, operation adjustments, and financial investments. This compressed timeline would create significant challenges for many covered entities, but particularly small practices. We urge OCR to grant an extended implementation timeline specifically for solo and small practices to allow them more time to prepare for compliance, adapt operations, and make informed decisions about technology investments. It would also provide time for developers to adapt their tools and products to empower providers to comply with the additional requirements.

- **Financial Support:** Develop financial assistance or grant programs to support small and solo practices to acquire or upgrade their technology tools and cybersecurity measures.
- **Specific Resources and Guidance:** Develop specific resources and guidance tailored to small practices to help them navigate the new requirements and provide clear examples of how to scale various cybersecurity measures. This could include developing simplified risk assessment tools and templates; offering tailored educational materials and training programs with a focus on the unique challenges faced by small practices and providing practical guidance on implementing effective security measures; and/or creating a dedicated support help line for small practices seeking clarification and guidance on HIPAA compliance issues.

Thank you for your consideration of our response. APA Services appreciates OCR's efforts to ensure the security of patients' electronic health data with the increasing use of technological tools in modern health care while considering the limited resources that many solo and small health care practices face in trying to meet those cybersecurity requirements. If you have any questions or require any further resources, please contact Deborah C. Baker, Head of Professional Legal and Regulatory Affairs at dbaker@apa.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'Arthur C. Evans, Jr.', with a long horizontal flourish extending to the right.

Arthur C. Evans, Jr., PhD
Chief Executive Officer
American Psychological Association Services, Inc.