AMERICAN PSYCHIATRIC ASSOCIATION

800 Maine Avenue, S.W.
Suite 900
Washington, D.C. 20024



March 4, 2025

Anthony Archeval
Acting Director for Office for Civil Rights (OCR)
U.S. Department of Health and Human Services
Office for Civil Rights
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 (RIN 0945-AA22)

Dear Mr. Archeval:

The American Psychiatric Association (APA), the national medical society representing more than 39,200 psychiatric physicians and their patients, appreciates the opportunity to comment on the proposed Health Insurance Portability and Accountability Act (HIPAA) Security rule. APA supports regulated entities to implement reasonable technical, physical, and administrative safeguards intended to mitigate the potential impermissible use or disclosure of Protected Health Information (PHI). The proposed requirements for multifactor authentication, network segmentation, and data encryption are viewed as essential steps to safeguard patient data. However, the proposed rule takes a generalized approach that does not consider the vast differences in resources, infrastructure and the level of risk for a data breach between small psychiatric practices and large healthcare systems. Below are areas that APA believes are important in order to make the proposed rule more effective in protecting healthcare data.

**Concerns Over Applying the Same Standards to All Practice Types**

Cybersecurity threats, while serious, do not pose the same level of risk to small practices as they do to major health systems, which store vast amounts of patient data and are more attractive targets for cybercriminals. Applying the same stringent cybersecurity mandates across all healthcare providers may unnecessarily burden small practices without a proportional benefit for patient security. A psychiatric practice in a rural community and in other areas with a shortage in mental health professionals, will also face disproportionate challenges in implementing many of these changes. These types of practices have fewer administrative and financial resources and limited access to technical and regulatory expertise. We urge the Office of Civil Rights (OCR) to develop tiered compliance measures that recognize these differences.

**Concerns Over Implementation Costs and Feasibility**

The estimated cost of implementing these measures is projected to be $9 billion in the first year and $6 billion annually over the subsequent four years. Many healthcare practices will face hurdles in meeting these requirements without substantial financial strain. **APA encourages the DEA to develop programs, technical assistance, and financial resources, which can help small and under-resourced entities that**

**need assistance in implementing cybersecurity best practices**. For instance, the Regional Extension Center (REC) program can serve as a model and would help address the shortage of available health IT and cybersecurity professionals and the lack of cybersecurity expertise in many physician practices.

The proposed rule also suggests a compliance date of 180 days after the final rule's effective date. This is an aggressive timeline and will not be feasible for many practices to meet. We urge OCR to consider extending this timeframe to at least a year or providing financial and technical assistance to ensure compliance is achievable.

Documentation requirements will be an additional burden. For example, the proposed rule mandates that covered entities obtain written verification from business associates, at least annually, confirming the implementation of required technical safeguards. This requirement will likely increase administrative burdens and introduce challenges in ensuring compliance with annual reporting across all business associates. The new requirement of documenting an annual compliance audit will increase costs and administrative burdens and will be especially challenging for small practices.

**Contingency Planning and Data Recovery**

We concur with OCR on the importance of contingency planning, including plans for data recovery, given the increasing risk of cyberattacks and the reliance of the healthcare system on electronically accessible information for patient care. The inclusion of criticality analysis in any contingency planning is an important aspect of being able to prioritize crucial actions that should be taken in the event of a cyberattack or other disaster. However, we are concerned with the inclusion of a 72-hour deadline for restoration of critical relevant electronic information systems and data.

Implementing rapid data recovery systems is costly and technically challenging. Large organizations have greater access to security and technical resources whiles mall practices are likely to need costly expert consultation to address contingency plans, criticality analyses, and technical modifications in addition to the greater costs of products that support rapid data restoration. Furthermore, even with robust planning, the hallmark of a disaster is its unpredictability. As such, it is preferable for practices and organizations to be able to show evidence of a good faith effort to restore critical systems rapidly rather than having a specified 72-hour deadline.

**Lack of Detailed Guidance**

The proposed rule does not provide specific guidance on securing emerging technologies, such as cloud computing, artificial intelligence, and Internet of Things (IoT) devices. More detailed instructions are needed to address the unique security challenges posed by these technologies. The proposed rule also introduces several new definitions and compliance expectations that require further clarification from OCR such as on effective technical policies, as small practices often lack automated tools to uniformly apply technical policies across their enterprise. **APA encourages OCR to create educational resources on cybersecurity best practices for the health care community to reference.**

**Interoperability with Other Standards**

There is a need for clearer guidance on how the proposed HIPAA Security Rule amendments align with other federal and state regulations, as well as international standards. This alignment is crucial for providers such as psychiatrists who must comply with multiple regulatory frameworks. Specifically, we

urge OCR to provide specific compliance recommendations for navigating the interplay between HIPAA and 42 CFR Part 2 (regulation protecting substance use disorder patient data), ensuring that psychiatric providers do not face conflicting obligations.

**HIPAA and health technology platforms**

HIPAA regulates covered entities, such as healthcare clearinghouses, health plans, and healthcare providers who submit HIPAA transactions, such as claims, electronically. Because non-covered entities do not need to comply with HIPAA requirements, they will be vulnerable to data breaches and cyber-attacks. However, most patients assume that HIPAA applies to all health-related information and do not understand the differences between covered and non-covered entities. While not the focus of this regulation, health applications and other technology platforms, in particular, present substantial risks to health information and warrant greater attention in the regulations.

APA appreciates HHS and OCR's commitment to HIPAA protections. APA encourages the agency to take into consideration differences between small practices compared to larger entities in the healthcare sector, where a breach can lead to major disruptions in care delivery and severely restrict patient access to care. Thank you for your review and consideration of these comments. If you have any questions or would like to discuss any of these comments further, please contact Zuhal Haidari (zhaidari@psych.org), Deputy Director, Digital Health.


Marketa Wills, MD, MBA
CEO and Medical Director