March 7, 2025

Anthony Archeval
Acting Director, Office for Civil Rights
Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W., Room 515F
Washington, D.C. 20201

SUBJECT: RIN 0945–AA22, HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, Proposed Rule, Federal Register (Vol. 90, No. 3), January 6, 2025

Dear Acting Director Archeval:

On behalf of more than 400 hospitals and health systems, the California Hospital Association (CHA) appreciates the opportunity to comment on the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) proposed rule modifying 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).

California's hospitals and health systems are committed to protecting patients' health information and strengthening cybersecurity practices to safeguard clinical technologies and information systems. As the health care sector has become an increasing target of cybercriminals, hospitals have dedicated significant resources to defending networks, securing patient data, preserving the efficient delivery of health care services and, most importantly, protecting patient safety. **However, the proposed rule — while well intentioned — would divert hospital resources away from the most effective strategies to prevent and mitigate cyberattacks by shifting these resources toward compliance with overly burdensome documentation requirements and unrealistic technical standards and timeframes.**

CHA urges OCR to rescind the proposed rule. As HHS contemplates deregulatory actions to comply with President Donald Trump's Executive Order 14192, *Unleashing Prosperity Through Deregulation*, it should not finalize policies that are estimated by the department to cost the health care sector $9 billion in the first year of compliance and $6.8 billion for regulated entities annually thereafter. Indeed, these

cost estimations are likely a significant underestimation of the true costs to comply with the proposed rules, which would apply to all HIPAA covered entities and business associates — whether they be a large multibillion dollar health plan, multistate health system, rural community hospital, or independent physician office. **The proposed rule would significantly increase health care costs and could threaten access to care in the most underserved communities.**

The proposed rule is overly focused on documentation at the expense of proven cybersecurity protections.

As stated in the proposed rule, the HIPAA Security Rule sets a national floor for the security measures covered entities are required to implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). While OCR proposes certain specific minimum cybersecurity hygiene requirements that it says are reflective of modern industry best practices, **many of the proposed policies would establish excessive documentation requirements that will strain hospital resources.**

For example, current regulations require HIPAA-covered entities to conduct security risk analyses. OCR reduces flexibility and significantly increases documentation requirements under its proposal to establish eight new implementation specifications for the security risk analysis standard. Many HIPAA-covered entities will not have the in-house expertise to comply with initial and annual updates required under the proposed rule and will have to dedicate significant resources to outsourced regulatory compliance. This will be especially challenging for small and rural hospitals that are already facing financial challenges.

The proposed rule would also require covered entities to annually obtain written verifications from business associates and subcontractors that have implemented all required technical safeguards. OCR severely underestimates the burdens associated with such a proposal. A large health system could have more than 10,000 business associates, and the resources that would be required to separately verify every business associate's technical security infrastructure are immeasurable. Even smaller entities may have hundreds or thousands of business associates and would lack the resources to comply with such requirements without resorting to costly outsourcing, further limiting resources available to adopt high-impact cybersecurity protections.

CHA urges OCR to work with its federal and industry partners to consider alternative policies that will incentivize broader sector-wide adoption of wide guidelines, best practices, and strategies to prevent and mitigate impacts of cyberattacks. This could include strategies to assist HIPAA-covered entities in adopting the voluntary consensus-based guidelines included in the HHS Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs). The department developed this set of essential and enhanced goals in close collaboration with hospitals and other health care industry leaders to address common attack vectors against U.S. domestic hospitals and help health care organizations prioritize implementation of high-impact cybersecurity practices.

Hospitals have significant concerns with the feasibility of implementing the proposed requirements. OCR proposes several specific requirements that demonstrate a lack of understanding of the operational and technical environment hospitals operate in. For example, the proposed rule would require covered entities to develop disaster recovery plans that establish written procedures to restore loss of the covered entity's or business associate's critical relevant electronic information systems and data within 72 hours of the loss. While a laudable goal, restoration of electronic health records and other clinical systems on this timeline is not realistic and often impossible. It can take weeks or even months just to determine the source of a breach and obtain the necessary third-party attestations to bring systems back online. Hospitals already comply with HIPAA regulations to maintain robust backup procedures to protect the confidentiality, integrity, and availability of patient health information, including regular backups, offsite storage, and disaster recovery plans that are activated in the event of a cyberattack. An arbitrary 72-hour restoration requirement could subject hospitals and other HIPAA-covered entities to penalties that would further exacerbate the impact of criminal cyberattacks.

The proposed rule includes several similar examples of requirements that are not informed by technological and operational realities. For example, increased encryption of ePHI and expanded deployment of multi-factor authentication (MFA) are viewed as common-sense strategies to prevent data breaches. However, encrypting all ePHI — as proposed — would require significant increases in processing power, resulting in workflow slowdowns and reduced system performance. Encrypting certain imaging files could degrade image quality after decryption, which could impact diagnostic accuracy and harm patients. Universal MFA requirements for all technology assets in relevant electronic information systems would be extremely costly to deploy and introduce significant operational slowdowns that could impact patient care. While hospitals are increasing the use of MFA in their systems, a more flexible approach is necessary to limit potential impacts on workflow.

Improving cybersecurity in the health care sector requires coordinated federal support. Under the existing regulatory framework, hospitals have demonstrated a commitment to protecting ePHI and safeguarding clinical technology against cyberattacks. Hospitals also understand that more can be done to keep up with the evolving threat of cyberattacks and remain committed to furthering investments in cybersecurity. However, hospitals alone cannot control cyber risks for the entire sector — a fact that was made clear when the attack on Change Healthcare, a UnitedHealth Group subsidiary and the predominant source of more than 100 functions critical to U.S. health care system operations, was attacked in February 2024. While the significant impacts of this attack were felt broadly among patients, payers, and providers, hospitals deployed backup plans and operational workarounds that allowed them to continue performing their primary function of providing safe and timely patient care.

In fact, an American Hospital Association review of top data breaches in 2023 showed that more than 95% of the most significant health care sector data breaches, defined as those where more than 1 million records were exposed, were related to business associates and other non-hospital health care entities. There is also significant risk in health apps and other technology platforms that are not HIPAA-covered

entities and are not subject to the proposed rule but are also targets of cybercriminals. **CHA again urges OCR to rescind the proposed rule and instead focus policymaking on coordinated federal efforts — including law enforcement — to prevent and deter cyberattacks in the broader health care sector.**

If you have any questions, please contact me at mhoward@calhospital.org or (202) 488-3742.

Sincerely,

/s/
Megan Howard
Vice President, Federal Policy