COLLEGE of AMERICAN PATHOLOGISTS

March 7, 2025

The Honorable Anthony Archeval
Acting Director for Office for Civil Rights (OCR)
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201

Subject: RIN 0945-AA22 – HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

Submitted via Electronic Submission to www.regulations.gov

Dear Acting Director Archeval:

The College of American Pathologists (CAP) appreciates the opportunity to comment on the Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) draft proposed rule *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information* (proposed rule). As the world's largest organization of board-certified pathologists and leading provider of laboratory accreditation and proficiency testing programs, the CAP serves patients, pathologists, and the public by fostering and advocating excellence in the practice of pathology and laboratory medicine worldwide. Pathologists are physicians whose timely and accurate diagnoses drive care decisions made by patients, primary care physicians, and surgeons. When other physicians need more information about a patient's disease, they often turn to pathologists who provide specific diagnoses for each patient. The pathologist's diagnosis and value are recognized throughout the care continuum and many patient encounters.

The nation's health care system—which cybersecurity consultants and government officials have consistently identified as the sector of the U.S. economy most susceptible to attacks—is insufficiently prepared to meet the cybersecurity challenges of an increasingly digital system. Pathologists understand the reality that our information systems exchange more electronically stored patient information, both medical and financial, than ever before. Ensuring laboratories are protected from cybersecurity attacks will allow pathologists to efficiently fulfill their duties as directors of the laboratory and promote quality in laboratory care so that patients receive the right test, at the right time, and with the right result.

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100

Cybersecurity attacks on health care entities have been increasing. **The CAP supports the OCR's overarching objective of the proposed rule: to protect patients' electronic protected health information (ePHI) to address significant changes in technology and changes in breach trends and cyberattacks.** Cybersecurity is a patient safety issue. Cyberattacks have delayed or disrupted patient care and threatened patient safety by locking physicians out of treatment tools, preventing physicians from accessing past medical history and communicating with colleagues, shutting down hospital equipment used for care, and by creating backlogs that further delay treatment. Indeed, in-hospital mortality rises in the aftermath of a cyberattack. Moreover, cyberattacks can compromise sensitive patient health and financial data. The magnitude of the challenge in coordinating stakeholders across the entire health care industry and in ensuring patient safety and access to care in aftermath of a cybersecurity incident necessitates federal leadership, guidance, and financial support.

The CAP has focused our comments on our desired elements for federal cybersecurity policy. We believe that HHS and OCR can avoid unintended, burdensome consequences by standardizing federal cybersecurity enforcement and helping to establish an environment where health care providers can proactively and transparently implement protections for the sensitive data of for patient care.

Specific Comments

1. **Risk-Based Approach to Enforcement – The CAP encourages OCR to enforce the HIPAA Security Rule based on levels of risk.**

Federal government enforcement of the cybersecurity responsibilities and expectations established in the HIPAA Security Rule should be based on the levels of risk posed by entities. We view risk as defined not only in terms of an entity's size and the number of patients that entity affects, but also the risk they pose to the entire health system. For example, if a small rural private practice gets hacked, the effects of that hack do not impact the entire U.S. health system unlike what could happen if a large corporate entity were hacked. Consequentially, the federal government's cybersecurity enforcement should be lighter on a small rural private practice than on a large corporate entity because the effect of a successful attack on a large corporate entity is more devastating.

The CAP appreciates the acknowledgement in the proposed rule that an entity's cybersecurity risk management responsibilities would be calibrated to its specific circumstances, including but not limited to its size, needs and capabilities, risk profile, the ability of security measures to reduce or eliminate a particular identified risk or vulnerability, and the ubiquity of such security measures.

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100

2. **Standardized, Consistent, and Uniform Approach to Cybersecurity that Minimizes Regulatory Burdens.**

As part of this risk-based cybersecurity policy, we believe that the Trump Administration should employ a standardized, consistent, and uniform cybersecurity approach across the entire federal government to avoid burdensome requirements. Thus, the CAP urges HHS to ensure that the cybersecurity requirements in OCR's final rule are consistent across all federal agencies and departments. Fortifying consistency and transparency in the federal approach will help save federal funds and make it easier for health care providers to meet the least burdensome requirements.

3. **Incentives to Assist with Adoption and Implementation of Cybersecurity Protection by Covered Entities – The CAP emphasizes that remaining current with cybersecurity protections requires considerable financial resources and requests federal assistance.**

The federal government should incentivize adoption and implementation of cybersecurity protection by health care entities. Incentives should include financial assistance from federal agencies (such as grants and increased federal health care program payments) for steps taken to improve cyberattack prevention and response. As the Trump Administration is aware, smaller hospitals and doctors' practices often do not have the money to pay for enhanced cybersecurity measures or the expertise to examine serious threats – particularly those in rural and less-populated areas. Consequently, the CAP encourages HHS to provide financial assistance to health care entities to adopt enhanced cybersecurity protections. While health care providers would certainly aim to employ technical updates and remain current with available protections, keeping technology **updated** often comes with significant expenses to implement. Sufficient financial assistance is vital for regulated entities to adopt these cybersecurity standards and help avoid unfunded mandates.

4. **Educational Approach to Cybersecurity Protection – The CAP urges OCR to employ an educational approach to its proposed rule to help entities comply, rather than a punitive approach.**

Federal oversight agencies should provide educational resources and guidance to enable entities to demonstrate that they are following optimal approaches to address an evolving landscape of cybersecurity. As the infrastructure for cybersecurity protection is being built and constantly changing, the federal government's adoption and implementation approach should not be punitive; rather, it should enable providers to demonstrate that they are meeting recommended standards.

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100

* * * * *

Thank you for the opportunity to submit these comments. The CAP looks forward to working with the OCR and always stands willing to collaborate with government agencies, industry, pathologists, and other stakeholders to support high quality laboratory operations and medical care. Please direct questions on these comments to Han Tran at htran@cap.org.

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100