American College of Radiology™

March 7, 2025

Submitted via Regulations.gov

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: (RIN: 0945-AA22; Docket ID: HHS-OCR-0945-AA22) HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information; Comments of the American College of Radiology

The American College of Radiology (ACR)—a professional association representing more than 40,000 diagnostic radiologists, interventional radiologists, radiation oncologists, nuclear medicine physicians, and medical physicists—appreciates the opportunity to file comments with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) regarding the agency's Notice of Proposed Rulemaking (NPRM), "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information," published in the January 6, 2025, *Federal Register* (RIN: 0945-AA22; Docket ID: HHS-OCR-0945-AA22).

While the ACR strongly supports the overarching goal of enhancing cybersecurity within the healthcare sector, we are deeply concerned the proposed revisions of the HIPAA Security Rule will impose substantial burdens, including significant and unrecoverable costs to already stretched providers facing reimbursement cuts and practice expense increases. These proposed changes would necessitate coordination among multiple stakeholders and integration of various legacy medical devices/technologies, some of which may have unsupported software components. These modifications would be particularly challenging for smaller hospitals, critical access hospitals, imaging centers, and rural facilities, and could compromise their ability to deliver essential healthcare services.

The ACR recommends that OCR rescind or rework the current NPRM and develop a new framework following extensive engagement of the physician community. The new rulemaking should undergo rigorous review by the Office of Management and Budget and include a clear, realistic implementation plan and timeline carefully considering the logistical and financial constraints faced by diverse healthcare providers, including a review of the responsibility and financial contributions of each stakeholder. Any new cybersecurity mandates should consider the roles, available resources, and good faith compliance efforts of disparate covered entities (CEs) and business associates (BAs) and take their reliance on vendors and other third parties for software updates into account. OCR should consider publishing educational resources and establishing a network of help centers to offer cybersecurity guidance and other practical assistance to providers and small entities. Moreover, rules should prioritize the largest actors within the health care sector, including health plans and clearinghouses, due to the severe nationwide effects on patients and providers of security incidents targeting those organizations and their systems.

ACR Comments on Specific OCR Proposals

45 CFR 160.103 – Definitions

The ACR supports the proposed technical update to the "electronic media" definition to modernize this terminology to include media on which data is maintained or processed. We agree the definition update would reflect the modern understanding.

§ 164.312(b)(1) – Standard: Encryption and Decryption

The ACR recommends reconsideration of the proposed new requirement for encryption that meets prevailing cryptographic standards for all electronic protected health information (ePHI) at rest and in transit. We also believe the exception defined at § 164.312(b)(3)(i) for "*a technology asset currently used by a regulated entity that does not support encryption according to prevailing cryptographic standards*" should be made more flexible to accommodate scenarios where the encryption is supported but not currently mandated for the asset(s) in question.

The encryption criteria described in the NPRM is generally viewed as a best practice; for example, whole-disk encryption is common for mobile devices, workstations, and servers. However, because Digital Imaging and Communications in Medicine (DICOM) supports but does not mandate encryption, many endpoints in hospitals are still unencrypted. Additionally, DICOM-QR is typically an unencrypted transfer that relies on the network's intrinsic security for protection, and the transfer itself does not apply additional encryption. Newer standards via DICOMweb (like QIDO/WADO) support—but do not mandate—the use of Hypertext Transfer Protocol Secure (HTTPS) for encryption at transit. Therefore, the proposed § 164.312(b)(1) should have a flexible and realistic transition period to accommodate collaboration between radiology practices, vendors, and other parties involved in these transfers.

§ 164.308(a)(10)(ii)(E) – Network Segmentation

The ACR recommends OCR implement a more flexible transition period for radiology practices to implement segmentation of relevant systems to limit access to ePHI to authorized workstations. Health systems will likely benefit from enhanced network segmentation; for example, segmenting traffic for imaging modalities and PACS workstations would improve protection. However, OCR's proposed mandates are anticipated to be costly and disruptive for providers.

§ 164.308(a)(12)(i) / (a)(13)(ii)(D) – Standard: Security Incident Procedures

The ACR opposes the proposed clarification that a regulated entity would be required to restore its critical relevant electronic information systems and data within 72 hours of loss via a security incident. This 72-hour deadline is arbitrary and assumes that all CEs/BAs have comprehensive control over all systems/data impacted by any security incident. However, radiology private practices with interpretive equipment and digital assets also typically rely on multiple contracted services, including hospitals and other third parties, to supply and support—and therefore restore and recover—impacted systems/data. OCR's regulations should instead eliminate arbitrary deadlines for provider stakeholders and differentiate between systematic abusers and good faith attempts by others to resolve problems expeditiously.

§ 164.308(b)(1) and (2) – Standard: BA Contracts and Other Arrangements
The ACR is concerned the proposal for BA verification of the deployment of technical safeguards at least once every 12 months will be arduous for contracted radiology practices that have adopted clinical algorithms, including AI-enabled software as a medical device (SaMD) and non-device AI solutions, individually. Practices that adopt platform approaches with a single vendor point-of-contact would be less affected. So, these extra administrative burdens may influence technological investments in unintended ways. We recommend situationally appropriate flexibility to allow for good faith efforts by smaller providers and others who rely on information from, or compliance activities by, multiple third parties.

§ 164.314 – Organizational Requirements
OCR proposed to require BA agreements to include a provision for BAs to report to CEs activation of the contingency plan required under § 164.308(a)(13) no later than 24 hours after activation (but without unnecessary delay). This proposal would not change breach notification rules. The ACR believes this requirement should differentiate planned from unplanned activations. Planned events (e.g., scheduled downtimes) should also use advance notifications.

Additionally, administrative safeguards should focus on operational needs at the time of activation. If a BA must notify hundreds of CEs upon activation of an unplanned contingency plan without unnecessary delay, the BA's leadership may be unintentionally incentivized to delay activation. Such delays would conflict with the intent of the contingency plan (i.e., to facilitate rapid response). The ACR recommends OCR explore alternatives, such as allowing a grace period during which BA resolution of the issue would not trigger the proposed requirement.

Thank you for your consideration of these comments. The ACR welcomes continued communication with OCR staff to help advance cybersecurity objectives. Please contact Michael Peters, Senior Director, Government Affairs, at mpeters@acr.org, with questions.

Sincerely,

D Smetherman

Dana H. Smetherman, MD, MPH, MBA, FACR
Chief Executive Officer
American College of Radiology