U.S. Department of Health and Human Services Delays HIPAA Security Rule Changes

July 16, 2026

INSIGHTS

- The U.S. Department of Health and Human Services has delayed the anticipated final action on the HIPAA Security Rule from May 2026 to July 2027, giving covered entities and business associates additional time to prepare for significant regulatory changes.
- The proposed amendments would represent the first major overhaul of the HIPAA Security Rule since 2013 and are intended to strengthen cybersecurity protections for electronic protected health information (ePHI) in response to increasing cyber threats targeting the healthcare sector.
- Among the most significant proposed changes are mandatory encryption of ePHI both at rest and in transit and mandatory multi-factor authentication (MFA) for all systems accessing ePHI, replacing the current more flexible and less prescriptive requirements.
- Healthcare organizations are encouraged to use the extra time proactively by evaluating encryption capabilities, implementing MFA, and updating incident response plans.

OVERVIEW

According to reginfo.gov, the U.S. Department of Health and Human Services (HHS) has pushed back the anticipated final action on the HIPAA Security Rule from May 2026 to July 2027. The delay gives covered entities and business associates additional time to prepare for the sweeping changes to the HIPAA Security Rule that HHS's Office for Civil Rights (OCR) first proposed in its notice of proposed rulemaking on January 6, 2025 (NPR). If finalized, it would become the first material overhaul of the HIPAA Security Rule since 2013. The revised timeline appears in the updated 2026 federal regulatory agenda, which now lists July 2027 as the target date for final action on the NPR. The official entry for this rulemaking (RIN 0945-AA22) can be reviewed on the government's regulatory agenda portal here.

The new deadline, like the prior one, is not set in stone—regulatory timeframes published by federal agencies are not legally binding, so the July 2027 date could be delayed again or, alternatively, OCR could finalize the rule ahead of schedule. Notably, the proposed rule itself has not changed, and the government has not publicly explained the reason(s) for the delay. Publication of the final rule was likely delayed due to OCR's focus on other priorities, such as patients' right of access, and the thousands of comments OCR received in response to the NPR.

The NPR was designed to strengthen cybersecurity protections for ePHI in response to the escalating volume and sophistication of cyberattacks against the healthcare sector. The substance of the proposed rule signals that the government intends to move the Security Rule's requirements in a more prescriptive direction. Among its most notable proposed changes, the rule would make encryption of ePHI mandatory—both at rest and in transit—with only limited exceptions, eliminating the current framework under which encryption is treated as an "addressable" specification subject to a reasonableness analysis. It would also require multi-factor authentication (MFA) for all systems that access ePHI, moving beyond the existing rule's general "person or entity authentication" requirement, which does not specify MFA. Read more about the proposed rule here.

Although the extended timeline eases immediate deadline pressure, organizations that handle ePHI would be well served to use the additional time to prepare, including by assessing encryption posture, ensuring MFA implementation, and updating incident response plans rather than deferring preparation. If finalized as proposed, covered entities and business associates would have 240 days from publication of the final rule to comply.

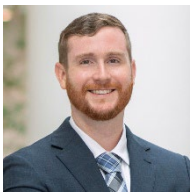
Please note that the information provided in this release is general in nature and not intended as legal advice. Specific circumstances may vary, and we encourage clients to contact us directly for personalized assistance and further information.

AUTHORS

If you have any questions regarding this client alert, please contact one of the authors below.

Jonathan R. Granade

Partner
Atlanta
404.420.1148
jgranade@phrd.com



Travis C. Williams

Associate
Atlanta
404.880.4751
twilliams@phrd.com