PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

The Proposed HIPAA Security Rule May Not Be Final but the Signal It Sends Is

By Thomas DeMayo, Partner and Keith Solomon, Partner

The month of May is weeks away. That matters if you are in health care, touch health care as a covered entity or are a business associate or own businesses that do. The Office of Civil Rights (OCR) has had a proposed overhaul of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule on its regulatory agenda for that month, the most significant proposed change to the rule since 2013.

It has been on the agenda for over a year. It may never pass. The current administration inherited it, froze new rulemaking and faces significant industry pressure to withdraw it entirely. We don't know what happens next.

What we do know is this. The signal was sent the moment OCR published the proposal. It doesn't require a final rule to mean something. OCR looked at the health care sector, reviewed years of breach data and enforcement findings and concluded the current standard is no longer sufficient to protect patients. That conclusion stands whether the rule passes, gets modified or disappears entirely. And the enforcement environment around the current rule has never been more active.

What OCR Said and Why It Matters

OCR spent years reviewing breach data and watching the health care sector absorb attack after attack before concluding the current rule is no longer sufficient. The most significant change proposed is the elimination of the distinction between required and addressable safeguards. Under the current rule certain controls can be deferred if an organization documents why implementation isn't reasonable. The proposal removes that entirely. Everything becomes mandatory. Encryption of patient data at rest and in transit. Multifactor authentication across systems handling that data. Regular vulnerability scanning and annual penetration testing. The ability to recover critical systems when something goes wrong.

These are proposed, not law. Some may change before finalization. But they represent OCR's stated floor for what protecting patient data should now look like. If the rule publishes in May, organizations have approximately 180 days to comply. That puts the hard deadline around December 2026. It sounds like enough time. For most organizations it isn't.

Who Needs to Be Listening

HIPAA applies to covered entities, health plans, health care clearinghouses and providers that transmit protected health information electronically in connection with billing and claims. Also, nursing homes and assisted living providers; behavioral health organizations; home health agencies; nonprofits running Medicare- or Medicaid-funded programs. All of them typically meet that definition and carry the same proposed obligations as a hospital, regardless of margin or resources.

Business associates carry direct obligations as well, including proposed annual written verification of security controls and 24-hour notification to covered entities upon activating contingency plans. For private equity firms managing health care portfolio companies, the exposure runs through the businesses they operate, not just at acquisition. Under the proposed rule, HIPAA security posture becomes something a buyer can quantify and something that follows the deal after it closes.

The Enforcement Reality Right Now

OCR does not need a final rule to act. The third phase of HIPAA compliance audits is already underway with 50 covered entities and business associates under review. 2024 was one of the most active enforcement years in OCR's history, with over $6.6 million in fines and 22 enforcement actions. The violations were not sophisticated failures. Inadequate risk assessments. Unencrypted data; access controls that hadn't been reviewed in years; the enforcement posture; and the proposed rule are pointing in exactly the same direction. Organizations that understand that connection will not be caught off guard by either.

Start Now. But Start Right.

The most important thing you can do before the final rule arrives is understand where you actually stand. That starts with a proper security risk assessment, not a gap analysis. They are not the same thing and the difference matters.

A gap analysis measures your current practices against a checklist of requirements and tells you what you are missing. That has value. But a risk analysis goes further. It looks at your specific environment and identifies what could actually threaten the information you are responsible for protecting. When done correctly a risk analysis will inherently produce the gap analysis as part of its output and, frankly, will give you a far more complete and useful picture of your exposure than a standalone gap analysis ever could. One tells you what boxes aren't checked. The other tells you what could actually hurt you and why and gives you the foundation to prioritize the work that matters most. If a vendor is offering you a gap analysis and calling it a risk assessment, ask them to explain the difference. The answer will tell you a great deal about what you are actually buying.

We also want to say something about certificates of compliance because we care about the organizations we serve and want to make sure they are protected in ways that actually count. These certificates have become common in the market and we understand the appeal. Compliance is complicated and something that looks like an answer can feel like a relief. But a certificate of compliance is not recognized by OCR and carries no weight in an investigation or enforcement action. What OCR looks for is evidence that your program is real and operational. Documented analyses, implemented controls, tested procedures, maintained records. A certificate doesn't demonstrate any of that. We want our clients spending their limited resources on work that genuinely protects them, not on something that creates comfort without creating safety.

The Work Is Hard. The Direction Is Clear.

We understand the position many organizations in this space are in right now. Reimbursement rates that haven't kept pace with costs. Staffing pressures that never fully eased. A regulatory environment that keeps adding requirements to teams that are already stretched. The ask embedded in the proposed HIPAA Security Rule is not a small one, especially for organizations operating on thin margins with limited IT resources. We are not going to pretend otherwise.

But the patients these organizations serve deserve protection. Their records, their diagnoses, their histories are among the most sensitive things a person carries. The attacks targeting health care are real and they do not make exceptions for organizations that are under-resourced. Neither does OCR.

What we have seen, again and again, is that the organizations that come through difficult compliance moments are not always the best-funded or the most technically sophisticated. They are the ones that took an honest look at where they stood, understood what was coming and had someone in their corner helping them close the gaps before those gaps became findings.

May is approaching. When the final rule lands we will be here, ready to walk through it with you and help you figure out what it means for your organization specifically.

You don't have to navigate this alone. Darkness has a way of shrinking when someone turns the light on. That is what we are here for.

Contact Us

If you have questions or want a straight conversation about where your organization stands, please contact your PKF O'Connor Davies client service team or:

Thomas J. DeMayo, CISSP, CISA, CRISC, CIPP
Partner, Cybersecurity and Privacy Advisory
tdemayo@pkfod.com

Keith Solomon, CPA
Partner, Health Care Practice Lead
ksolomon@pkfod.com