PBMares SM
CPAs and Consultants

Navigating the 2026 HIPAA Security Rule Changes: What You Need to Prepare

Safeguarding patient information has long been a top priority for healthcare organizations. The Health Insurance Portability and Accountability Act (HIPAA), in place since 1996, has been the cornerstone of these efforts. Now, a major update to the HIPAA Security Rule is on the horizon, bringing stricter cybersecurity requirements and new obligations for everyone handling patient data.

Expected to be finalized in early to mid-2026 based on the HHS Unified Agenda, these changes represent a significant shift in how organizations must protect electronic protected health information (ePHI). This guide breaks down the major updates and the steps you can take now to ensure you're ready when the new rules take effect.

Timeline and Key Dates

Based on the proposed rule from the Department of Health & Human Services (HHS), the clock is ticking. After a public comment period in early 2025, the changes are anticipated to be finalized in early to mid-2026, based on the HHS Unified Agenda. Once published, the effective date for the new rules are anticipated approximately 60 days after final publication, followed by an estimated 180-day compliance period (timing subject to change). This gives most organizations about eight months from final publication to meet all new requirements, likely putting the deadline in mid-2026.

While that might seem like plenty of time, the changes are substantial. Organizations that handle ePHI should start planning now. Making the necessary improvements to technology, updating vendor agreements, developing new training, and budgeting for security enhancements will require a thoughtful, proactive approach.

As with all federal rulemaking, timelines remain subject to change until the final rule is published in the Federal Register. While timing may evolve, the direction of the proposed requirements is unlikely to materially change, making early preparation advisable

The 8 Biggest Changes to the HIPAA Security Rule

1. **Annual Compliance Audits Organizations** are expected to be required under the proposed rule to conduct formal security audits every 12 months. An important addition is that business associates must share their audit results with the covered entities they work with. This change promotes consistent oversight and greater transparency between partners.

2. **Enhanced Business Associate Agreements** (BAAs) will need to go beyond standard legal language. The new rules are expected to require these businesses to specify security controls like multi-factor authentication (MFA), strict encryption standards, and faster incident reporting deadlines—often within 24 hours. They must also confirm that the business associate follows recognized cybersecurity best practices, like the NIST Cybersecurity Framework.

3. **More Detailed Risk Assessments Risk** assessments have always been a part of HIPAA, but the expectations are now much higher.

You will need to maintain up-to-date network maps, a full inventory of all devices and systems, and a clear process for identifying and addressing security risks.

4. **Mandatory Network Mapping** Healthcare organizations must create and maintain clear data flow diagrams that show where ePHI is stored and how it moves through their systems. These maps are essential for ensuring no data is left unprotected in overlooked corners of your network. The maps must be reviewed at least once a year or whenever significant system changes occur.

5. **Tighter Incident Reporting and Response** The new rule broadens the definition of a "security incident" to include smaller events that disrupt system operations, even if no data is breached. Covered entities must develop written incident response plans, test them regularly, and coordinate with business associates. Business associates will be required to notify covered entities within 24 hours if they activate their own incident response plan.

6. **Required Multi-Factor Authentication (MFA)** The days of MFA being an optional or "addressable" measure are over. The proposed changes make MFA mandatory for any person or system accessing ePHI. Exceptions will be rare and must be justified with a robust, documented risk analysis.

7. **Increased Encryption Standards** Organizations should plan to use strong encryption for ePHI both when it's stored (at rest) and when it's being sent (in transit). Additionally, organizations must use widely accepted, government-approved encryption methods. This could be a significant challenge for those still using older systems.

8. **Stricter Workforce Training Requirements** Generalized annual training will no longer be sufficient. The rule calls for ongoing, role-specific security awareness education for anyone who handles ePHI. The effectiveness of this training must be tested, and new training should be triggered by events like the implementation of new systems or policy updates.

How to Prepare for Compliance

Organizations should start preparing now as these updates demand careful planning.

First, perform a gap analysis. Review your current HIPAA compliance program against the proposed requirements to identify missing procedures, weak policies, or outdated technologies.

Next, document your ePHI flows. Create clear network diagrams and identify all third parties and cloud services that handle sensitive data. If your current risk assessment is more of a checklist, it's time to upgrade it to a more detailed analysis using a framework like NIST or CIS (Center for Internet Security).

Rolling out MFA and stronger encryption can be complex, especially if you have legacy devices or custom applications. Work closely with your IT team and vendors to plan for necessary upgrades.

Finally, revisit your business associate agreements. Add clauses that specify annual audits, timely incident notifications, and stricter security measures to ensure every partner is aligned with the new rules.

Potential Challenges Ahead

Many healthcare organizations, particularly smaller clinics, will face challenges with legacy infrastructure. Older devices may not support advanced encryption or MFA, and budget constraints can make upgrades difficult.

Vendor management adds another layer of complexity. Every business associate, from billing services to cloud providers, must adhere to the same new rules. This will likely involve lengthy contract renegotiations and more frequent audits of your partners.

Finally, don't underestimate the importance of workforce training and cultural change. Moving from simple check-the-box training to meaningful, continuous education requires a concerted effort. However, fostering this level of engagement is one of the most effective ways to reduce the risk of human error leading to a security incident. By starting now, you can build a proactive, audit-ready compliance program that not only meets regulations but also protects your patients and your organization.

How PBMares Can Help

At PBMares, our Cyber & Risk Advisory services center on helping organizations meet the HIPAA Security Rule's existing mandatory HIPAA risk assessment requirements, which the proposed rule is expected to clarify and strengthen through more prescriptive standards. If your organization stores or processes electronic protected health information (ePHI), whether you're in healthcare, insurance, technology, research, or another industry) HIPAA applies to you. We work with you to complete a thorough, documented risk assessment and to schedule and execute vulnerability scans, penetration tests, and security awareness training so no compliance deadlines are missed.

We specialize in building and refining incident response processes that not only help you react swiftly when trouble occurs but also enable you to confidently meet the new 24-hour incident reporting window. Our team can craft tailored workforce training programs that reflect the nuanced needs of each role within your organization, ensuring that security awareness is embedded into daily operations.

Our experts also provide consulting support to refresh security policies and procedures, update and strengthen Business Associate Agreements (BAAs), and align your program with recognized cybersecurity frameworks such as NIST and other industry best practices. Whether you need to develop robust network maps, strategize encryption controls, or streamline a system-wide MFA rollout, we believe in a proactive, customized approach to security and compliance—one that helps you meet regulations and, more importantly, protects your patients, your reputation, and your bottom line. The result is a proactive, audit-ready compliance posture that reduces risk and demonstrates a strong commitment to protecting ePHI.

About PBMares

As one of the largest accounting and consulting firms in the United States and a top 100 Accounting Firm as named by *Accounting Today,* PBMares brings a comprehensive approach to client engagements by providing a high level of expertise and experience in tax strategy, audit services, consulting, cybersecurity, and wealth management.

VA | MD | DC | NC

PBMares SM
CPAs and Consultants

Contributing Experts

Antonina K. McAvoy, CISA, CISM, QSA, PCIP
Partner, Cybersecurity & Risk Advisory Services

757-355-6011
amcavoy@pbmares.com

www.pbmares.com

Antonina brings 14 years of experience performing cybersecurity reviews, compliance audits, data mapping, and IT internal control assessments. Her expertise includes guiding organizations toward secure, sustainable, and compliant technology environments, with a focus on modernizing approaches to protecting sensitive data.

Reid Peterson, CPA
Assurance Manager, Healthcare Services

757-627-4644
rpeterson@pbmares.com

www.pbmares.com

Reid brings 11 years of experience leading financial statement audits, reviews, compilations, and consulting engagements. His expertise includes helping healthcare and not-for-profit organizations strengthen financial reporting, improve internal controls, and navigate complex accounting and regulatory requirements.

Sources:

https://www.cyera.com/blog/new-hipaa-rules-mandate-mfa-and-encryption-for-ephi--is-your-organization-ready?utm_source=chatgpt.com

https://www.reuters.com/legal/litigation/top-10-takeaways-new-hipaa-security-rule-nprm-2025-03-14/?utm_source=chatgpt.com

https://www.linkedin.com/pulse/hipaa-compliance-changing-8-security-rule-updates-coming-2026-ac25e