New HIPAA Security Rule Requirements

What Independent Rheumatology Practices Need to Know

⚠ **EFFECTIVE Late 2026: Penetration Testing Now REQUIRED Every 12 Months**

What Changed in the HIPAA Security Rule?

The U.S. Department of Health and Human Services (HHS) published a Notice of Proposed Rulemaking on January 6, 2025, that fundamentally changes HIPAA cybersecurity requirements for all covered entities, including independent rheumatology practices. The new rule eliminates the 'addressable' classification for critical security controls, making them **mandatory** for practices of all sizes.

Security Requirement	Required Frequency	First Deadline
Penetration Testing	Every 12 months	January 2027
Vulnerability Scanning	Every 6 months	November 2026
Compliance Window	240 days post-May 2026	January 2027

Why This Matters to Your Independent Practice

- **OCR Enforcement is Escalating:** In 2025, OCR imposed $6.6M in HIPAA penalties across multiple healthcare entities. Recent settlements include $112,500 against Concentra (urgent care clinics) for inadequate risk analysis and $2.15M against Jackson Health System—demonstrating that independent practices are not exempt from enforcement.
- **Penalties Are Significant:** HIPAA violation penalties in 2026 range from $145 to $2,190,294 per violation category. Willful neglect can result in penalties exceeding $2M annually per violation type.
- **State Privacy Laws Add Complexity:** Washington's My Health My Data Act, Nevada's SB 370, and Connecticut's health data privacy law now regulate consumer health data beyond HIPAA. These laws apply to practices collecting patient data in those states—even if your practice is located elsewhere.
- **Multi-Location Practices Face Higher Risk:** Practices with multiple locations, telehealth services, patient portals, or third-party vendors (billing, EHR, imaging) have expanded attack surfaces that require documented security testing.
- **Ransomware Targeting Healthcare:** Independent practices are increasingly targeted due to perceived weaker defenses compared to hospital systems. The average healthcare data breach now costs $10.93M to remediate.

What You Need to Do Now

- **Assess Current State:** Determine when your last formal penetration test was completed (if ever) and review your current risk analysis documentation.
- **Understand the Gap:** Identify the difference between internal security policies and third-party validated testing required under the new rule.
- **Plan Your Timeline:** Schedule your first mandatory penetration test before the January 2027 deadline and establish a recurring annual testing schedule.
- **Address State Compliance:** If you serve patients in Washington, Nevada, or Connecticut, review your data collection and consent practices for state-specific requirements.
- **Budget Appropriately:** Plan for annual penetration testing and semi-annual vulnerability scanning as ongoing compliance costs (typically $3,500-$8,500 annually for small-to-mid-sized practices).

How We Can Help

We are facilitating a **complimentary Healthcare IT & Compliance Workshop** specifically for independent rheumatology practices preparing for the new HIPAA Security Rule. The workshop provides a Cyber Risk Assessment, HIPAA compliance gap analysis, state privacy law review, and a clear penetration testing roadmap—all at no cost. We also offer flat-rate annual penetration testing and vulnerability scanning designed specifically for HIPAA-covered entities.