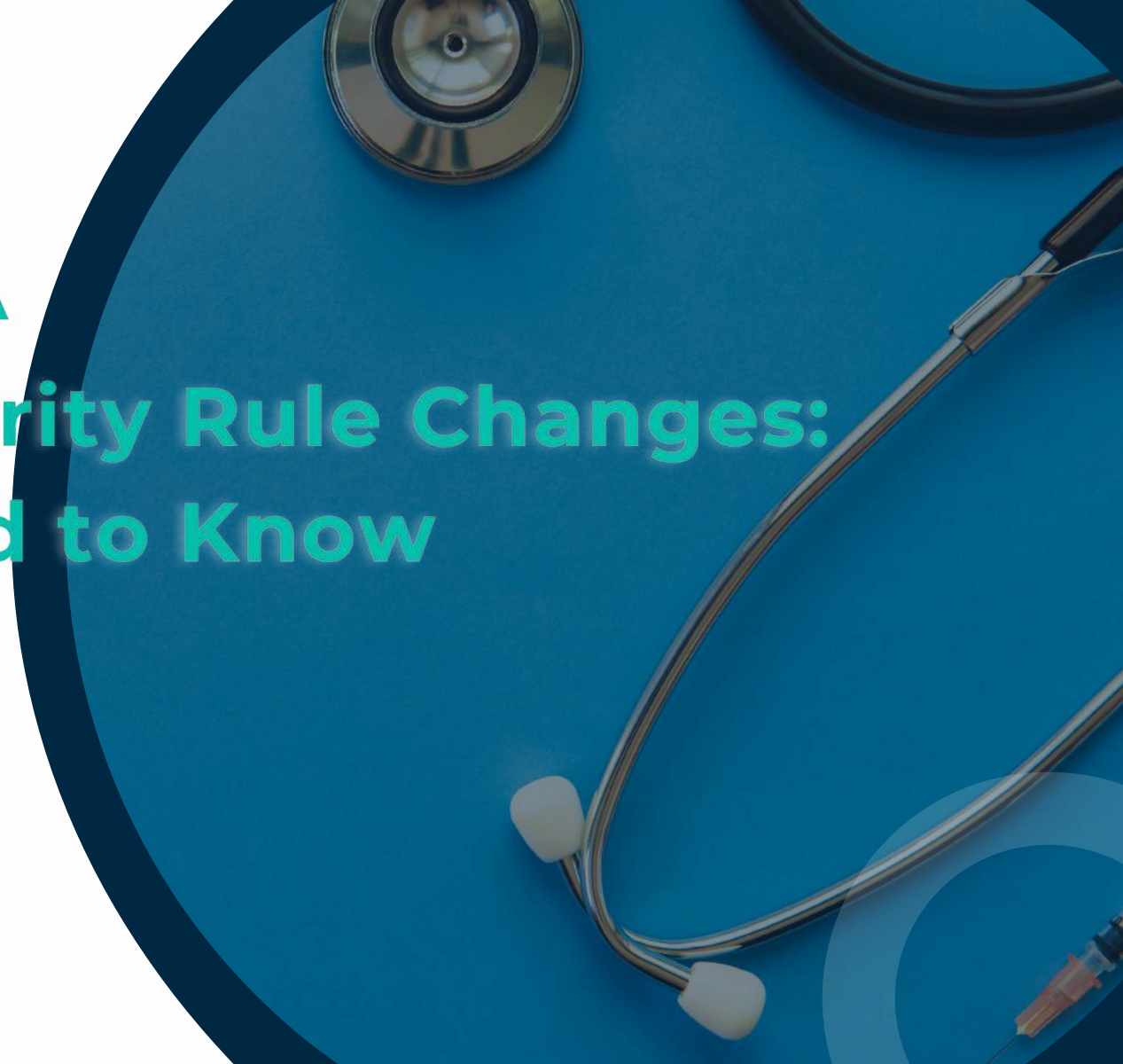
eBook

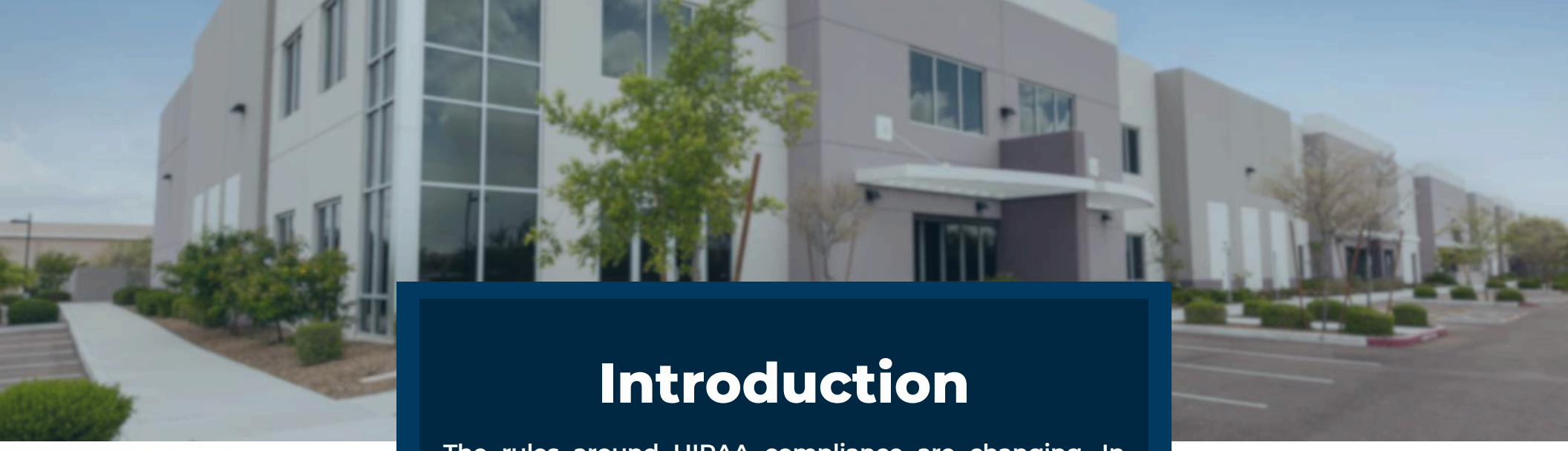
2025 HIPAA Proposed Security Rule Changes: What You Need to Know



Pillar Technology
PARTNERS

Table of Contents

Pillar Technology
PARTNERS



Introduction

The rules around HIPAA compliance are changing. In 2025, the new HIPAA Security Rule is closing loopholes and raising the bar on security. Access management, multi-factor authentication (MFA), and encryption aren't optional anymore—they're required. This means security leaders have more responsibility than ever.

This eBook cuts through the complexity to help you understand exactly what's changing, how it impacts your business, and what you need to do to stay ahead. These regulations are moving fast—don't get caught off guard.

What's Driving These Changes?

On December 27, 2024, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking (NPRM) to update the HIPAA Security Rule. This overhaul aims to combat growing cyber threats targeting healthcare and aligns with the 2023 National Cybersecurity Strategy.

These are the first major updates to HIPAA's Security Rule in over a decade. The key takeaways?

- The distinction between "required" and "addressable" safeguards is gone—everything is required now.
- New documentation requirements will hold organizations accountable for their security policies and actions.
- Cyber resilience is front and center, with mandates for rapid incident response and recovery.

Real-World Context: Why This Matters Now

Cyberattacks on healthcare systems are escalating, with breaches exposing millions of patient records. Here are **two recent incidents** that highlight the urgency of stronger security regulations:

Example 1: The 2023 HCA Healthcare Breach

- One of the largest U.S. health systems, HCA Healthcare, suffered a cyberattack that leaked **11 million** patient records.
- Stolen data included names, locations, and appointment details.
- **Lesson:** Stricter encryption and multi-factor authentication could have mitigated the risk.

Example 2: The CommonSpirit Health Ransomware Attack (2022)

- A cyberattack on **CommonSpirit Health** disrupted **hospitals in 21 states**, delaying critical patient care.
- The attack was linked to a **lack of network segmentation** and **slow response time**.
- **Lesson:** Incident response planning and network segmentation are now required under the new HIPAA changes.

Key Changes in the HIPAA Security Rule

Cybersecurity Takes Center Stage

- **Multi-Factor Authentication (MFA):** Now required for all systems handling ePHI.
- **Encryption:** Mandatory for data at rest and in transit—no more ambiguity.
- **Vulnerability Scanning & Penetration Testing:** Regular scans every six months and annual penetration tests to identify weaknesses before attackers do.

More Responsibility for Covered Entities & Business Associates

- Healthcare providers, health plans, and business associates must implement stronger security measures across the board.
- Significant investments in cybersecurity will be needed to meet compliance.

Pillar Technology PARTNERS

HIPAA Compliance Action Plan

Phase 1

Immediate Actions (0-30 Days)

- ✓ Conduct a **gap analysis** to assess current security controls.
- ✓ Implement **multi-factor authentication (MFA)** for all ePHI access points.
- ✓ Encrypt all ePHI at **rest and in transit**.
- ✓ Develop a **business associate compliance strategy** for oversight.

Phase 2

Strengthening Security (30-60 Days)

- ✓ Conduct **vulnerability scans** and **penetration testing**.
- ✓ Implement **network segmentation** to limit ePHI access risks.
- ✓ Update **incident response plans** to meet new HIPAA requirements.
- ✓ Train **workforce members** on updated security policies.

Phase 3

Full Compliance Readiness (60-90 Days)

- ✓ Conduct a **full-scale compliance audit** to verify adherence to new HIPAA rules.
- ✓ Ensure **backup systems** meet the new 48-hour ePHI recovery standard.
- ✓ Review and revise **vendor security contracts** with business associates.
- ✓ Establish an **annual compliance review process** moving forward.

What's Changing?

	Current HIPAA Rules	2025 HIPAA Updates
1 Multi-Factor Authentication	Recommended but not required	**Mandatory for all ePHI access**
2 Encryption	Addressable	**Required for ePHI at rest & in transit**
3 Incident Response	Vague guidance	**Must restore data within 72 hours**
4 Compliance Audits	Self-regulated	**Annual compliance audit required**
5 Vulnerability Testing	No clear timeline	**Vulnerability scans every 6 months, pen testing annually**

Pillar Technology
PARTNERS

What This Means for Your Organization

While some of these requirements reflect best practices that security-conscious organizations already follow, many businesses will need to make substantial changes. Proactive compliance will not only help you avoid penalties but also strengthen your organization's overall cyber resilience.

Now is the time to:

- ✓ Conduct a gap analysis to see where your security measures align—or fall short.
- ✓ Invest in critical security infrastructure like MFA, encryption, and continuous monitoring.
- ✓ Review and update incident response plans and backup strategies.
- ✓ Ensure business associates meet heightened security requirements.

Insights from Industry Experts

"Healthcare is under siege by cybercriminals. The new HIPAA rule changes are a much-needed wake-up call to prioritize cybersecurity before it's too late."
— John Smith, CISO, Leading Healthcare System

"Organizations that fail to take action now will face both regulatory penalties and increased risk of data breaches. Compliance is just the starting point—true security requires continuous improvement."
— Jane Doe, Cybersecurity Attorney

Final Thoughts

The new HIPAA Security Rule is a clear message: **cybersecurity is no longer negotiable.** Healthcare organizations must act now to stay compliant, protect patient data, and safeguard their operations.

Are you ready? Now's the time to assess your security posture and make the necessary updates before these changes become mandatory. **The clock is ticking—don't wait until it's too late.**

Contact Us

For more information to stay HIPAA compliant, protect patient data, and safeguard your organization, contact us at:

678-304-9099

info@ptechcyber.com

www.ptechcyber.com

YOUR TRUSTED PARTNER IN CYBERSECURITY

Pillar Technology
PARTNERS