Koniag CYBER

Microsoft Solutions Partner

PROTECTING PATIENT PRIVACY. SECURING TRUST.

UPDATED HIPAA SECURITY RULE

Safeguarding ePHI through administrative, physical, and technical safeguards.

Administrative

Policies, Procedures, and Workforce Training

Physical

Facility Access Controls, Workstation Security & Protection

Technical

Access Control, Audit Controls, Encryption & Integrity

The HIPAA Security Rule has been around since 2003. For most of that time, "compliance" meant checking boxes and documenting your reasoning for skipping the hard parts. That era is over.

The Department of Health and Human Services finalized the most significant update to the HIPAA Security Rule in over two decades. The compliance clock is running. For healthcare organizations using Microsoft 365, that is actually good news — most of the tools you need are already in your environment. The harder question is whether they are configured, enforced, and documented to meet the new requirements.

This guide cuts through the noise. It lays out what changed, what it means for your M365 environment specifically, and a clear timeline for what you should be doing right now.

~240 DAYS
to comply once the final rule is effective

100% MANDATORY
all safeguards required — no more "addressable" exceptions

72 HOURS
maximum recovery time for critical ePHI systems

What Changed: The End of "Addressable"

Under the old rule, HIPAA implementation specifications fell into two buckets: "required" and "addressable." Addressable did not mean optional — but in practice, many organizations treated it that way, documenting a rationale for non-implementation and moving on.

The final rule eliminates that distinction. Every safeguard is now mandatory. You can no longer document a reason for skipping MFA, skipping network segmentation, or skipping annual penetration testing. If you have been waiting to act, that window has closed.

THE MAJOR NEW REQUIREMENTS

01 No More "Addressable" Specifications

The addressable vs. required distinction is gone. Every safeguard is mandatory. Documentation of a reason for non-implementation no longer satisfies the rule.

02 Multi-Factor Authentication (MFA)

MFA is required for all systems accessing electronic Protected Health Information (ePHI). Every user, every system, every access point — including service accounts and legacy integrations.

03 Encryption of ePHI

Encryption is mandatory both in transit and at rest. Systems without encryption are out of compliance, full stop.

04 Network Segmentation

Healthcare data environments must be isolated from general network traffic. Your ePHI environment needs dedicated segmentation — it cannot share a flat network with general office systems.

05 Annual Penetration Testing

Pen testing moves from a risk-based judgment call to an annual mandatory requirement, with results documented and available for audit.

06 72-Hour Recovery Capability

Business Continuity and Disaster Recovery plans must demonstrate a tested, documented ability to restore critical ePHI systems within 72 hours.

Compliance Readiness Checklist

Use this to assess your current state against each new requirement.

NEW REQUIREMENT	YOUR CURRENT STATUS
MFA enforced on ALL accounts, including service accounts	☐ In place ☐ Partial ☐ Gap
ePHI encrypted at rest AND in transit	☐ In place ☐ Partial ☐ Gap
Network segmentation isolating ePHI environments	☐ In place ☐ Partial ☐ Gap
Annual penetration testing scheduled and completed	☐ In place ☐ Partial ☐ Gap
72-hour recovery capability tested and documented	☐ In place ☐ Partial ☐ Gap
BCP/DR plan current and validated	☐ In place ☐ Partial ☐ Gap

YOUR MICROSOFT 365 ENVIRONMENT

The Gap Is Configuration, Not Tooling

As a healthcare organization running Microsoft 365, many of the tools needed to satisfy these requirements are already in your licensing. The gap is almost never the tooling — it's the configuration, enforcement, and documentation.

Microsoft Entra ID

MFA & Identity

Microsoft Entra ID (formerly Azure Active Directory) is your primary identity platform. Many organizations have MFA turned on for most staff but not enforced across all users and applications — particularly legacy integrations and shared service accounts.

IN PRACTICE:

A physician group has MFA enabled for most staff, but their EHR integration runs on a service account with a static password and no MFA. Under the new rule, that is a direct compliance gap. A thorough Entra ID review identifies all service accounts, enforces Conditional Access Policies, and implements phishing-resistant MFA (FIDO2 keys or Microsoft Authenticator) across every access point to ePHI.

Microsoft Purview & BitLocker

Encryption

Microsoft 365 provides native encryption through Microsoft Purview (data at rest and in transit) and BitLocker for endpoints. These must be actively configured — they are not in a compliance-ready state by default.

IN PRACTICE:

A behavioral health network stores patient notes in SharePoint Online and sends clinical summaries via Outlook. Microsoft encrypts data in transit by default, but their on-premises billing file share has no encryption, and staff laptops lack BitLocker enforcement. A data-flow mapping exercise identifies all ePHI locations, enables Purview sensitivity labels for automatic ePHI classification, enforces BitLocker via Intune, and documents the encryption posture for audit purposes.

Azure & Microsoft Defender

Network Segmentation

For organizations leveraging Azure, network segmentation means Virtual Network (VNet) segmentation, Network Security Groups (NSGs), and micro-segmentation between ePHI systems and general IT infrastructure.

IN PRACTICE:

A home health agency runs its patient management system and general office tools on the same flat network. A ransomware infection in the office environment can spread directly to ePHI systems. A segmented Azure network architecture, NSGs to restrict ePHI traffic, and Microsoft Defender for Cloud providing continuous monitoring changes that exposure entirely.

Annual Penetration Testing

Penetration testing must occur annually, cover all systems that store, process, or transmit ePHI, and be documented in a format that satisfies OCR requirements. That means your M365 tenant, your Azure environment, and any on-premises integrations are all in scope.

IN PRACTICE:

A federally qualified health center (FQHC) has never conducted a formal penetration test. Monthly patching happens, but whether those vulnerabilities are actually exploitable has never been validated. A HIPAA-scoped penetration test targeting the M365 tenant, Azure-hosted workloads, and network perimeter — with a full report formatted for OCR documentation requirements — closes that gap.

Azure Backup & Business Continuity

72-Hour Recovery Capability

Azure Backup and Azure Site Recovery give organizations robust tools for meeting the 72-hour requirement. But configured tools and compliant tools are not the same thing. Backups must be tested, recovery must be documented, and the DR plan must reflect your actual current environment — not the one from three years ago.

IN PRACTICE:

A radiology practice has M365 backups configured through their CSP but has never tested a restore. Their DR plan references systems that no longer exist. Reviewing and updating BCP/DR documentation, validating Azure Backup configurations, running a tabletop recovery exercise, and producing a tested-and-documented recovery runbook demonstrating sub-72-hour RTO for all ePHI systems turns a paper plan into a real one.

If your organization supports VA healthcare programs, DoD medical services, or other federal health IT contracts, you face compliance requirements on two fronts: HIPAA and CMMC (Cybersecurity Maturity Model Certification).
The good news: there is significant overlap. MFA, network segmentation, incident response, and audit logging appear in both frameworks. Work done toward the HIPAA Security Rule update can be mapped directly to your CMMC posture — and vice versa. An integrated gap assessment covering both frameworks simultaneously reduces cost, eliminates duplicated effort, and accelerates compliance on both tracks.

How Koniag Cyber Can Help

As a Microsoft Cloud Solution Provider with deep healthcare cybersecurity experience, Koniag Cyber is positioned to help you close HIPAA compliance gaps within your existing M365 and Azure environment — without adding third-party tooling in most cases.

SERVICE	DESCRIPTION
HIPAA Gap Assessment	Comprehensive review of your current security posture against the final rule requirements, with a prioritized remediation roadmap.
Microsoft 365 HIPAA Configuration Review	Detailed assessment of your M365 tenant — Entra ID, Defender, Purview, Intune, SharePoint, Teams — against HIPAA technical safeguard requirements.

SERVICE (CONTINUED)	DESCRIPTION (CONTINUED)
MFA & Conditional Access Deployment	Design and implementation of phishing-resistant MFA and Conditional Access Policies across your environment.
Encryption & Data Classification	Purview sensitivity labeling, BitLocker enforcement, and data-flow mapping to ensure ePHI is encrypted at rest and in transit.
Network Segmentation Design	Azure VNet and NSG architecture review and implementation for ePHI environment isolation.
Annual Penetration Testing	HIPAA-scoped penetration testing of M365 tenant, Azure workloads, and network perimeter with OCR-ready reporting.
BCP/DR Assessment & Tabletop Exercise	Recovery capability validation, documentation update, and tested runbook development to meet the 72-hour requirement.
Ongoing vCISO & Compliance Monitoring	Fractional CISO services and continuous Microsoft Secure Score monitoring to maintain compliance posture year-over-year.

Recommended Action Timeline

Now through June 2026

Request a HIPAA Gap Assessment. Identify your highest-risk gaps: MFA, encryption, unprotected ePHI stores. Begin Entra ID and Conditional Access review.

July through Sept 2026

Implement MFA enforcement, encryption controls, and network segmentation. Update BCP/DR documentation and conduct tabletop exercise.

Oct through Nov 2026

Complete annual penetration test. Finalize policy documentation. Begin staff training on updated requirements.

Dec 2026 / Jan 2027

Target compliance-ready posture before the effective date. Establish continuous monitoring and annual review cadence.

Ready to Get Started?

The compliance window is real, and it is shorter than most organizations realize. Starting now — before the effective date — is the difference between a controlled, methodical process and a scramble.

Koniag Cyber offers a complimentary 30-minute HIPAA Security Rule Readiness Briefing for healthcare organizations using Microsoft 365. We will review your current environment, identify your most critical gaps, and give you a clear picture of where you stand and what comes next.

Email: info@koniagcyber.com
Website: koniagcyber.com
Phone: (907) 261-4001