

PROTECTING PATIENT PRIVACY. SECURING TRUST.

HEALTHCARE CYBERSECURITY READINESS

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

Ransomware and cyberattacks on healthcare continue to rise, raising operational, financial, and patient-safety risks. To comply with OCR enforcement of the HIPAA Security Rule, organizations must prioritize actionable, legally defensible cybersecurity.

HHS proposes major Security Rule updates, but finalization is delayed. Waiting is unwise. Key controls like MFA, encryption, identity governance, network segmentation, penetration testing, and disaster recovery reduce risk and align with current rules; NIST guidance will now require implementation. Addressable will no longer be acceptable.

For Microsoft 365 users, security functionality to meet HIPAA already exists but must be configured, enforced, and documented. This guide explains strong healthcare security today, its impact on M365, and a phased roadmap to act on now, regardless of rule finalization.

ENFORCED TODAY

The current HIPAA Security Rule is fully in effect and actively enforced by OCR.

EXPECTED NOW

MFA, encryption, and segmentation are baseline expectations from insurers, boards, and NIST.

72-HOUR TARGET

A defensible recovery objective for critical ePHI systems.

Why These Controls Matter Now

"Historically, HIPAA implementation specifications fell into two buckets: 'required' and 'addressable.' Addressable never meant optional, but in practice many organizations treated it that way, documenting a rationale for non-implementation and moving on. HHS's proposed update would remove that distinction and make every safeguard mandatory. That rule is currently delayed, but the direction is unmistakable: MFA, network segmentation, and annual penetration testing are no longer 'nice to have.' Regulators, insurers, and attackers already treat them as baseline. Organizations that wait for a final deadline to act are accepting an unnecessary risk they don't need to carry.

THE CONTROLS THAT MATTER MOST

01

No More "Addressable" Specifications

The proposed rule would end the addressable vs. required distinction and make every safeguard mandatory. Even today, treating these controls as optional leaves clear, exploitable gaps, and won't satisfy insurers or OCR.

02

Multi-Factor Authentication (MFA)

MFA should be enforced 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 belongs on ePHI both in transit and at rest. Systems without it are a top-tier risk and are a common finding in OCR enforcement and insurance reviews.

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.

Cybersecurity Readiness Checklist

Use this to assess your current state against each core control.

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

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. That is a direct security gap today, and exactly what insurers and OCR flag. 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 to strengthen your HIPAA security posture maps 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.

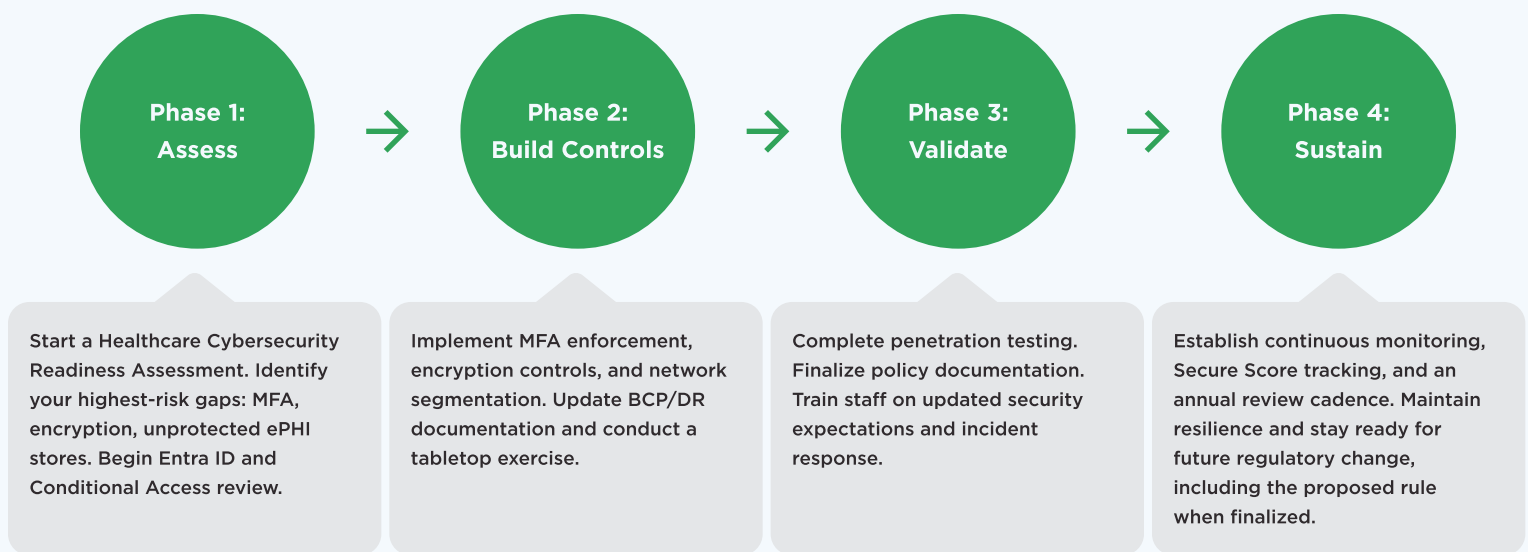
How Koniag Cyber Can Help

As a Microsoft Cloud Solution Provider with deep healthcare cybersecurity experience, Koniag Cyber is positioned to help you close cybersecurity and HIPAA 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 today's HIPAA Security Rule and cybersecurity best practices, 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.

Cybersecurity Maturity Roadmap



Ready to Get Started?

The threats are real, and they aren't waiting for a regulatory deadline. Strengthening your security posture now, while the proposed rule is still in flux, is the difference between a controlled, methodical program and a scramble later. Koniag Cyber offers a complimentary 30-minute Healthcare Cybersecurity Readiness Briefing for healthcare organizations using Microsoft 365. We'll 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