Authsignal

Your HIPAA MFA Readiness Checklist

The proposed HIPAA Security Rule removes the "addressable" loophole for MFA. Once the final rule publishes, every covered entity and business associate will have roughly 240 days to comply. This checklist helps you start now.

Note: As of June 2026, the final rule has not been published. The direction is clear however, use the runway to prepare, not to wait.

Step 1

Inventory every system that touches ePHI

How many systems in your organisation touch ePHI? If the answer is 'we're not sure,' that's the first finding. Map every system that creates, receives, maintains, or transmits electronic protected health information. Include EHRs, patient portals, billing and revenue cycle systems, analytics and reporting tools, remote access portals (VPN, Citrix, RDP), admin consoles, clinical applications, and vendor-managed systems.

Do not forget: medical devices with network access, telehealth platforms, third-party integrations, and any system accessible via shared or service accounts.

- [ ] ePHI system inventory complete

Step 2

Record the current authentication state

For each system in the inventory, document what authentication is in place today. Capture: SSO or local credentials, whether MFA is enforced or optional, which MFA method is used (SMS, TOTP, push, passkeys, none), whether shared accounts or service accounts exist, and whether the system is vendor-managed or internally controlled.

This becomes your gap analysis. The proposed rule expects evidence of deployed controls, not just a policy that says MFA should exist.

- [ ] Authentication state documented for all ePHI systems

Step 3

Sort access by risk tier

Not all ePHI access carries the same risk. Prioritize:

- Tier 1 (highest risk): Privileged access (admin, DBA, system config), remote access (VPN, Citrix, cloud consoles), vendor and business associate access
- Tier 2 (high risk): Clinician and practitioner access to patient records, bulk data export or reporting, contact centre agent access to ePHI
- Tier 3 (standard): Routine workforce access to clinical applications, scheduling systems, internal portals with limited ePHI exposure

- [ ] Risk tiers defined and systems assigned

Step 4

Move Tier 1 access toward phishing-resistant MFA first

Start with the highest-risk access. Modern authentication layers can be dropped in on top of existing identity providers, without needing to replace your IdP. The proposed rule favours phishing-resistant methods, such as passkeys (FIDO2/WebAuthn) and hardware security keys, aligned with NIST SP 800-63B. These methods are bound to the legitimate domain and cannot be phished, intercepted, or replayed.

Priority targets: Admin accounts, remote access portals, vendor access, and any system that was the entry point for a previous incident (the Change Healthcare breach entered through a Citrix portal with no MFA).

- [ ] Phishing-resistant MFA deployed or in pilot for Tier 1 systems

Step 5

Use adaptive step-up for clinical and patient-facing workflows

Blanket MFA prompts in clinical environments create friction, and friction often leads to workarounds. Use risk-based step-up authentication to apply the strong check where it matters:

- New or unrecognised device
- Remote or unusual location
- Privilege escalation or role change
- High-volume data export
- Sensitive record access outside normal patterns

Routine access on a recognised device at a known workstation should be fast. The high-risk moments get scrutiny.

- [ ] Adaptive step-up rules defined for clinical and patient-facing workflows

Step 6

Document systems that genuinely cannot support MFA

Some legacy clinical applications, medical devices, and older systems cannot integrate with modern authentication protocols. For each one, document:

- The specific technical constraint preventing MFA
- Compensating controls in place (network segmentation, access restrictions, enhanced monitoring, restricted access windows)
- A migration or replacement timeline

The proposed rule includes provisions for documented exceptions on genuinely constrained systems. The key word is "documented" — an undocumented exception is a finding.

- [ ] Exception documentation complete with compensating controls and migration plans

Step 7

Start vendor and BAA conversations now

Every business associate with ePHI access will need to demonstrate MFA controls. Updated business associate agreements will need to reflect the new requirements. Vendor security reviews, procurement, and legal negotiation take time — typically 3 to 6 months for enterprise healthcare.

Do not wait for the final rule to start these conversations. The 240-day compliance window after publication does not include time for vendor discovery and procurement.

- [ ] Vendor inventory reviewed and BAA update timeline established

Step 8

Build the audit trail as you go

The proposed rule expects evidence that MFA controls are deployed and operating. Capture authentication events from day one:

- Who authenticated
- With which method
- Against which policy
- At what time, from what device and location
- What happened on high-risk events (step-up triggered, blocked, allowed)

Reconstructing this evidence under a deadline is far harder than logging it as it happens. Start capturing now, even on the systems you are migrating first.

- [ ] Authentication event logging active on priority systems

The final rule will start the deadline. It should not start the work.

Get the full HIPAA MFA regulatory breakdown, method comparison, and preparation guide: →

Ready to talk through what HIPAA-ready MFA looks like for your environment? →