rhinogram

Healthcare Communication & Compliance Solutions

HIPAA 2026 MFA Compliance Readiness Checklist

Overview

The healthcare regulatory landscape is evolving. With **HIPAA 2026 MFA changes** approaching, multi-factor authentication (MFA) is becoming an expected safeguard for protecting electronic protected health information (ePHI).

This checklist is designed to help healthcare organizations—including **medical, dental, and orthodontic practices**—evaluate their readiness for evolving HIPAA MFA expectations and enforcement trends.

This document is intended as a **practical compliance aid** and should be used alongside a formal HIPAA Security Risk Assessment.

🔐 Multi-Factor Authentication (MFA) Implementation

☐ MFA is enabled for all systems that access ePHI
☐ MFA is required for all remote access methods (VPN, RDP, cloud portals)
☐ MFA is enforced for administrative and privileged user accounts
☐ MFA applies to employees, contractors, and third-party vendors
☐ MFA policies are formally documented and approved

🧠 Risk Assessment & Documentation

☐ A current HIPAA Security Risk Assessment has been completed and documented
☐ MFA risks and safeguards are explicitly addressed
☐ Systems without MFA have documented compensating controls
☐ Risk decisions are reviewed annually or after system changes
☐ Documentation is centrally stored and audit-ready

💻 Healthcare IT Systems Review

☐ EHR / EMR platforms support MFA
☐ Cloud email systems use MFA
☐ Practice management and billing platforms use MFA
☐ Third-party integrations are reviewed for MFA support
☐ Legacy systems have documented mitigation plans
☐ Communication Partners have MFA enabled

👥 Workforce Training & Access Control

☐ Workforce members are trained on MFA usage
☐ MFA onboarding is part of new-hire procedures
☐ MFA access is revoked immediately upon termination
☐ Role-based access limits unnecessary ePHI exposure
☐ Shared logins are prohibited

📊 Monitoring, Logging & Enforcement

☐ MFA login activity is logged
☐ Failed login attempts are monitored
☐ Credential-related incidents are documented
☐ MFA policies are enforced consistently
☐ Logs are retained per organizational policy

📋 Policies & Compliance Alignment

☐ Access control policies reference MFA
☐ Incident response plans address credential compromise
☐ Business Associate Agreements address access security
☐ Policies align with HIPAA Security Rule guidance
☐ Leadership reviews MFA readiness regularly

✅ Final Readiness Review

☐ MFA aligns with organizational risk profile
☐ Leadership understands 2026 enforcement expectations
☐ No critical systems rely on passwords alone
☐ Compliance posture can be explained to an auditor
☐ A continuous improvement plan is in place

Important Notice

This checklist is provided for **informational purposes only** and does not constitute legal or compliance advice. Organizations should consult qualified professionals to address specific compliance requirements.
