corsica technologies

IT COMPLIANCE SERVICES

HIPAA Compliance Checklist

The 2026 HIPAA updates are here. Are you ready?

The 2026 HIPAA compliance landscape is changing. With a mandatory Notice of Privacy Practices (NPP) update due by **February 16, 2026**, and significant modernizations to the Security Rule on the horizon, ensuring your organization is prepared is more critical than ever.

Use this checklist to assess your readiness for these new, more stringent requirements.

Audits and Assessments

Has your organization conducted a comprehensive **Asset and Device Audit,** including all network-connected medical, IoT, and personal devices?

- [ ] Security Risk Assessment
- [ ] HITECH Subtitle D Privacy Audit
- [ ] Physical Security Audit
- [ ] Asset and Device Audit
- [ ] Security Standards Audit
- [ ] Privacy Standards Audit

Remediation Plans

- [ ] For the above required audits, has your organization identified and documented all gaps in compliance?
- [ ] Has your organization created a remediation plan to address identified gaps?
- [ ] Does your organization review this remediation plan annually, and if so, can you provide supporting documentation to an auditor?

corsica technologies

Training

- [ ] Have all staff members undergone required annual HIPAA training?
- [ ] Have all training records been documented, and if so, can you provide them to an auditor?
- [ ] Has a staff member been officially designated as the HIPAA Compliance, Privacy, and/or Security Officer?

Incident Response

- [ ] Has your organization **tested its incident response plan** within the last 12 months with defined recovery time objectives?
- [ ] Can your organization fulfill its reporting obligations for security incidents and breaches?
- [ ] Does your organization provide its staff members with a way to anonymously report a security incident or breach?

Policies and Procedures

- [ ] Has your organization updated its **Notice of Privacy Practices (NPP)** to meet the February 16, 2026 deadline?
- [ ] Have all staff read and attested to their understanding of these policies and procedures, and if so, can you provide supporting documentation to an auditor?
- [ ] Does your organization annually review these policies and procedures, and if so, can you provide supporting evidence to an auditor?

Vendors and Business Associates

- [ ] Has your organization established Business Associate Agreements with all relevant business associates?
- [ ] Does your organization review these agreements annually, and if so, can you provide supporting evidence to an auditor?
- [ ] Does your organization have a **documented vendor risk management program** that includes initial due diligence and ongoing monitoring?
- [ ] Does your organization have Confidentiality Agreements in place with vendors that do not qualify as Business Associates?

Technical Safeguards & Security Controls

- [ ] **Multi-Factor Authentication (MFA):** Is multi-factor authentication required for all users (clinical and administrative) to access systems containing ePHI?
- [ ] **Data Encryption:** Is all ePHI encrypted both at rest (on servers, laptops) and in transit (over email, web)?
- [ ] **Vulnerability Management:** Does your organization have a documented process for identifying, prioritizing, and patching system vulnerabilities in a timely manner?
- [ ] **24/7 Security Monitoring:** Are your systems monitored 24/7 by a Security Operations Center (SOC) to detect and respond to threats in real-time?
- [ ] **Backup and Recovery:** Have you tested your data backup and recovery capabilities within the last 6 months to ensure data integrity and availability?

Governance and Strategy

- [ ] **Recognized Security Practices:** Has your organization adopted a recognized security framework (e.g., NIST Cybersecurity Framework, HITRUST) to guide its security program?

Confidently Meet the 2026 Requirements with a HIPAA Readiness Assessment

Our team of compliance experts has deep expertise helping healthcare organizations reach and maintain full compliance in accordance with strict industry regulations.

Every compliance gap review includes:

- A comprehensive analysis of your technology and cybersecurity environment.
- A review of your potential cybersecurity gaps and compliance risks.
- A plan customized for your organization with actionable steps to help mitigate risks and protect client data.

Schedule Your Free Assessment