TRANSFORM 42 · HEALTHCARE IT COMPLIANCE

HIPAA IT Compliance Self-Assessment

Evaluate your practice against HIPAA Security Rule requirements. Identify gaps before auditors do — and build a remediation plan that protects patients and your practice.

Why HIPAA IT Compliance Can't Wait

The HHS Office for Civil Rights (OCR) has increased enforcement actions by 300% since 2022. Small and mid-size practices are no longer "too small to audit" — they're the primary targets for both regulators and attackers.

$2.1M
AVG. HIPAA BREACH SETTLEMENT

89%
OF HEALTHCARE ORGS BREACHED

$500
MIN. FINE PER RECORD (TIER 2)

How This Assessment Works

This self-assessment covers the 7 domains of the HIPAA Security Rule's technical, administrative, and physical safeguards. For each requirement, rate your practice:

SCORE	MEANING	ACTION
1 — Not Implemented	No controls in place	Immediate priority
2 — Partially Implemented	Some controls, not documented	Address within 90 days
3 — Implemented	Controls in place and documented	Annual review
4 — Managed & Monitored	Controls active, monitored, tested	Maintain

> **Important: This Is Not Legal Advice**
>
> This assessment helps identify IT compliance gaps. For a formal HIPAA compliance determination, consult a qualified healthcare compliance attorney. Transform 42 provides IT controls implementation — not legal compliance certification.

01 Access Controls (§ 164.312(a))

REQUIREMENT	1	2	3	4
Unique user identification for all EHR/system access	☐	☐	☐	☐
Emergency access procedure documented and tested	☐	☐	☐	☐
Automatic session timeout/logoff configured	☐	☐	☐	☐
PHI access restricted to minimum necessary	☐	☐	☐	☐
Multi-factor authentication on all PHI systems	☐	☐	☐	☐
Role-based access aligned with job responsibilities	☐	☐	☐	☐

02 Audit Controls (§ 164.312(b))

REQUIREMENT	1	2	3	4
Audit logs enabled on all systems containing PHI	☐	☐	☐	☐
Logs reviewed regularly (weekly minimum)	☐	☐	☐	☐
Log retention for minimum 6 years	☐	☐	☐	☐
Alerts configured for suspicious access patterns	☐	☐	☐	☐
Audit trail tamper-proof (centralized SIEM)	☐	☐	☐	☐

03 Transmission Security (§ 164.312(e))

REQUIREMENT	1	2	3	4
PHI encrypted in transit (TLS 1.2+ minimum)	☐	☐	☐	☐
Encrypted email for patient communications	☐	☐	☐	☐
Secure patient portal for document exchange	☐	☐	☐	☐
VPN required for all remote access to PHI	☐	☐	☐	☐
Wireless networks encrypted (WPA3)	☐	☐	☐	☐

04 Data Integrity & Encryption (§ 164.312(c)(d))

REQUIREMENT	1	2	3	4
PHI encrypted at rest (AES-256)	☐	☐	☐	☐
Full-disk encryption on all workstations/laptops	☐	☐	☐	☐
Mobile device encryption enforced via MDM	☐	☐	☐	☐
Backup encryption (data at rest in backups)	☐	☐	☐	☐
Data integrity mechanisms (checksums/hashing)	☐	☐	☐	☐
Media disposal procedures (NIST 800-88)	☐	☐	☐	☐

05 Physical Safeguards (§ 164.310)

REQUIREMENT	1	2	3	4
Server room/closet access restricted and logged	☐	☐	☐	☐
Workstation use policy (screen lock, positioning)	☐	☐	☐	☐
Device inventory maintained and current	☐	☐	☐	☐
Remote wipe capability for lost/stolen devices	☐	☐	☐	☐
Visitor access controls and escort policy	☐	☐	☐	☐

06 Administrative Safeguards (§ 164.308)

REQUIREMENT	1	2	3	4
Designated HIPAA Security Officer	☐	☐	☐	☐
Annual risk assessment completed and documented	☐	☐	☐	☐
Workforce security training (annual + new hire)	☐	☐	☐	☐
Incident response plan documented and tested	☐	☐	☐	☐
Business Associate Agreements (BAAs) current	☐	☐	☐	☐
Contingency plan (backup, DR, emergency mode)	☐	☐	☐	☐
Sanctions policy for HIPAA violations	☐	☐	☐	☐

07 Backup, DR & Vendor Management

REQUIREMENT	1	2	3	4
Daily encrypted backups of all PHI	☐	☐	☐	☐
Backup stored offsite/cloud (geographically separate)	☐	☐	☐	☐
Quarterly restore tests documented	☐	☐	☐	☐
Recovery Time Objective (RTO) defined and achievable	☐	☐	☐	☐
Vendor risk assessments for all PHI handlers	☐	☐	☐	☐
BAAs signed with all vendors who access PHI	☐	☐	☐	☐
Cloud service providers HITRUST/SOC 2 certified	☐	☐	☐	☐

Your Compliance Score

Add up your ratings across all 46 items. Maximum possible score: 184.

SCORE RANGE	COMPLIANCE LEVEL	RECOMMENDED ACTION
156–184	**Strong** — well-positioned for audit	Annual maintenance, penetration testing
120–155	**Moderate** — gaps exist	90-day remediation plan, prioritize score-1 items
80–119	**Concerning** — significant exposure	Engage HIPAA-specialized MSP immediately
Below 80	**Critical** — breach and penalty risk high	Emergency assessment and remediation

Your Total Score: _____ / 184

Record the date of this assessment: _____. HIPAA requires annual risk assessments at minimum. Transform 42 specializes in helping healthcare practices in the Miami area achieve and maintain HIPAA compliance — from technical controls to documentation.

2026 HIPAA Update: NPRM Changes Coming

The HHS proposed new rules in 2024 that would require: mandatory encryption (no longer "addressable"), 72-hour incident reporting, annual penetration testing, and technology asset inventories. Practices that prepare now will avoid the compliance scramble.

Ready to Secure Your Practice?

Schedule a free 30-minute IT compliance assessment with Transform 42's team. We'll review your score and build a prioritized action plan.

(305) 709-0050

info@transform42inc.com

TRANSFORM42INC.COM