FREE COMPLIANCE CHECKLIST

HIPAA IT Compliance Checklist for Medical Practices

42 actionable items to secure patient data, pass audits, and avoid penalties up to $2.1M per violation category.

Joe Crist
CEO & Founder, Transform 42 Inc.
Service-Disabled Veteran-Owned Small Business
Miami & South Florida

Administrative Safeguards

HIPAA Security Rule §164.308 — Policies, procedures, and workforce management

Risk Analysis & Management

- [ ] **Conduct annual SRA (Security Risk Assessment)** covering all systems that create, receive, maintain, or transmit ePHI §164.308(a)(1)(ii)(A)
- [ ] **Document all identified risks** with likelihood ratings, impact severity, and remediation plans with deadlines §164.308(a)(1)(ii)(B)
- [ ] **Maintain a current asset inventory** of all devices and systems storing ePHI (servers, workstations, mobile devices, cloud services, medical devices)
- [ ] **Review and update risk assessment** after any significant change (new EHR deployment, office move, merger, breach)

Workforce Security

- [ ] **Implement role-based access controls** — front desk, clinical staff, billing, and admin each get minimum necessary access to EHR (Epic, athenahealth, eClinicalWorks) §164.308(a)(3)
- [ ] **Enforce MFA on all systems with ePHI** (EHR, email, cloud storage, VPN, patient portal admin) §164.312(d)
- [ ] **Conduct background checks** on all workforce members with ePHI access before granting credentials
- [ ] **Terminate access within 24 hours** for any departing employee — disable AD/Entra account, EHR login, email, VPN, badge access §164.308(a)(3)(ii)(C)
- [ ] **Conduct annual HIPAA security awareness training** for all workforce members, with phishing simulation exercises quarterly §164.308(a)(5)

Incident Response

- [ ] **Maintain a written Incident Response Plan** with named response team, contact tree, and 60-day HHS breach notification timeline §164.308(a)(6)

- [ ] **Test the IR plan annually** via tabletop exercise (ransomware scenario, stolen laptop, insider threat)
- [ ] **Document all security incidents** including near-misses, with root cause analysis and corrective actions

Pro tip: HHS OCR auditors look at your SRA first. If you can't produce a current, thorough risk assessment, nothing else matters. Use the NIST Cybersecurity Framework (CSF 2.0) as your SRA template — it maps directly to HIPAA requirements.

Technical Safeguards

HIPAA Security Rule §164.312 — Technology controls protecting ePHI

Access Controls & Authentication

- [ ] **Unique user identification** for every person accessing ePHI — no shared logins, ever §164.312(a)(2)(i)
- [ ] **Automatic session timeout** after 15 minutes of inactivity on all workstations and EHR sessions §164.312(a)(2)(iii)
- [ ] **Emergency access procedures** documented for break-glass scenarios (system failure during patient emergency) §164.312(a)(2)(ii)
- [ ] **Password policy: 14+ characters**, complexity requirements, 90-day rotation (or NIST 800-63B passphrase model), account lockout after 5 failed attempts

Encryption & Data Protection

- [ ] **Encrypt ePHI at rest** on all devices: BitLocker (Windows), FileVault (Mac), LUKS (Linux), SQL TDE for databases §164.312(a)(2)(iv)
- [ ] **Encrypt ePHI in transit** via TLS 1.2+ for all network communications, VPN for remote access, encrypted email (Microsoft Purview or Virtru) §164.312(e)(1)
- [ ] **Encrypt all backups** including cloud backups (AES-256), and store encryption keys separately from backup data
- [ ] **Implement DLP policies** in Microsoft 365 / Google Workspace to prevent ePHI from being emailed or shared to unauthorized recipients

Audit Controls & Monitoring

- [ ] **Enable audit logging** on all systems with ePHI: EHR access logs, Windows Event Logs, firewall logs, email access logs §164.312(b)
- [ ] **Centralize logs in SIEM** (Microsoft Sentinel, Splunk, or managed SOC) with 6-year retention per HIPAA

- [ ] **Review audit logs monthly** for anomalies: off-hours access, bulk record views, failed login spikes, privilege escalation
- [ ] **Deploy EDR/MDR** (Microsoft Defender for Endpoint, SentinelOne, or CrowdStrike) on all endpoints accessing ePHI

Network Security

- [ ] **Segment clinical network** from guest WiFi, IoT/medical devices, and administrative network via VLANs
- [ ] **Next-gen firewall** with IDS/IPS, geo-blocking, and content filtering (Fortinet, Palo Alto, or Meraki MX)
- [ ] **Patch all systems within 30 days** of critical CVE release — 14 days for internet-facing systems

Physical Safeguards & BAAs

HIPAA Security Rule §164.310 + Business Associate requirements

Physical Security

- [ ] **Server room/MDF locked** with badge access, visitor log, and environmental monitoring (temperature, humidity) §164.310(a)(1)
- [ ] **Workstation use policy** — screens face away from patient areas, privacy screens on check-in terminals, clean desk policy §164.310(b)
- [ ] **Mobile device management (MDM)** on all phones/tablets accessing ePHI with remote wipe capability (Intune, Jamf) §164.310(d)(1)
- [ ] **Secure media disposal** — NIST 800-88 compliant wiping or physical destruction of drives, with certificates of destruction

Business Associate Agreements

- [ ] **Execute BAAs with ALL vendors** that access, store, or transmit ePHI: EHR vendor, cloud provider, IT MSP, billing service, shredding company, email host §164.308(b)(1)
- [ ] **Verify BAA coverage** for: Microsoft 365 (HIPAA BAA available), Google Workspace (BAA), AWS/Azure (BAA), your phone system (VoIP BAA often missed)
- [ ] **Review BAAs annually** and re-execute when vendor relationships change or new services are added
- [ ] **Maintain a BAA inventory spreadsheet** with vendor name, service description, BAA execution date, renewal date, and responsible party

Backup & Disaster Recovery

- [ ] **3-2-1 backup strategy**: 3 copies, 2 different media, 1 offsite (encrypted cloud) — test restores quarterly §164.308(a)(7)
- [ ] **RPO < 4 hours, RTO < 8 hours** for EHR and critical clinical systems
- [ ]

Documented disaster recovery plan covering natural disaster, ransomware, hardware failure, and pandemic scenarios

- [ ] **Air-gapped or immutable backups** to prevent ransomware from encrypting backup data (Veeam immutability, AWS S3 Object Lock)

Common audit finding: Practices sign a BAA with their EHR vendor but forget about email (Microsoft 365 BAA must be explicitly activated), their answering service, cloud fax, and medical device reps who remote into equipment. Every access point needs a BAA.

Need Help Getting HIPAA Compliant?

Transform 42 specializes in IT compliance for medical practices in Miami and South Florida.
We handle the SRA, deploy the technical controls, manage your BAAs, and keep you audit-ready year-round.

Book a Free HIPAA IT Assessment

Joe Crist — CEO & Founder
joe.crist@transform42inc.com | (424) 955-6238
transform42inc.com
Service-Disabled Veteran-Owned Small Business

LinkedIn **Facebook** **Instagram**