Medical Practice HIPAA Security Readiness Checklist

Huntleigh Group

September 2025

Contents

Medical Practice HIPAA Security Readiness Checklist

Use this checklist to prioritize the 7 essentials auditors, insurers, and EHR vendors expect.

1. Risk Analysis & Governance

- Complete/update HIPAA Security Risk Analysis; document remediation plan.
- Assign security officer; set quarterly review cadence.
- Keep an asset inventory (workstations, mobile, cloud apps).

2. Policies, BAAs & Privacy Notices

- Current policies (InfoSec, Access, IRP, Backup/DR, AUP, Mobile).
- Signed BAAs for all vendors with PHI.
- Updated privacy notice and patient acknowledgement process.

3. Access Controls & MFA

- Unique IDs; role-based access; offboarding checklist.
- MFA on email/EHR/VPN; password manager or SSO if available.

4. Backup & Recovery

- Daily backups; offline/immutable copy; monthly restore test.
- Document RTO/RPO; screenshot evidence for insurers.

5. Device & Data Protection

- Full-disk encryption; auto-lock; patching on a schedule.
- EDR/AV on endpoints; allowlisting where feasible.
- Secure email (phishing defense, SPF/DKIM/DMARC).

6. Training & Awareness

- Annual HIPAA security training; phishing simulations quarterly.
- Track completion logs; include front desk and billing.
- Role-based refreshers for clinical vs. admin.

7. Incident Response & Breach Notification

- Written IRP; contact tree; regulator/state notification timelines.
- Tabletop-lite exercise; capture after-action items.
- Maintain insurer-ready artifact pack.

Optional: 42 CFR Part 2 (if applicable)

If you handle SUD records: consent forms, redisclosure notices, disclosure log; compliance by Feb 16, 2026.

Be audit-ready in 60 days: practical HIPAA and cybersecurity compliance for small practices."

Huntleigh delivers turnkey **vRC/vCISO services** tailored for medical practices with 5–20 staff, covering:

- **Policy & Consent Pack**: HIPAA and Privacy Rule updates, 42 CFR Part 2 alignment (if applicable).
- **Technical Safeguards**: MFA, encryption, application allowlisting (e.g., ThreatLocker), logging, validated backups.
- **Training & Awareness**: Role-based staff training modules, tracking logs, annual refreshers.
- **Incident Response & Breach Playbook**: HIPAA/HBNR notification templates, tested through tabletop exercises.
- **Evidence for Boards & Insurers**: Compliance dashboards, training logs, disclosure logs, and closure packages.

Delivered in **three tiers**:

1. **Guided** (oversight + templates)
2. **Hybrid** (shared execution + Huntleigh-led tabletop)
3. **Turnkey** (full implementation and delivery of all phases).

Get Started Now!

cs@huntleigh.com