

HIPAA & 42 CFR Part 2

Compliance Checklist for Therapy Practices

25-point technical safeguards audit covering HIPAA Security Rule (45 CFR §164.312) and 42 CFR Part 2 substance abuse record protections. Designed for solo practitioners, group practices, and counseling centers.

Access Controls (§164.312(a))

- 1 Every clinician and staff member has a unique login — no shared EHR accounts (SimplePractice, TherapyNotes, etc.).
- 2 Role-based access configured — billing staff cannot view session notes, admin cannot access clinical records.
- 3 Automatic screen lock activates after 5 minutes on all devices, including home office computers.
- 4 Multi-factor authentication (MFA) enabled on EHR, email, cloud storage, and telehealth platforms.

Session Notes & Clinical Records Security

- 5 Psychotherapy notes (as defined under HIPAA) are stored separately from the general medical record.
- 6 Session notes are never stored on local devices — only in encrypted, access-controlled cloud EHR.
- 7 Paper notes (if any) are secured in locked storage and shredded per retention policy.

Telehealth Compliance

- 8 Telehealth platform is HIPAA-compliant with a signed Business Associate Agreement (BAA) on file.
- 9 Session recordings (if permitted) are encrypted and stored per your retention policy.
- 10 Clients are informed about telehealth privacy limitations (shared spaces, screen visibility) in writing.
- 11 Home office telehealth setup uses a private network — not public Wi-Fi or shared household networks.

42 CFR Part 2 Requirements (Substance Abuse Records)

- 12 Substance abuse treatment records are segmented with stricter access controls than general health records.
- 13 Written patient consent is obtained before any disclosure of substance abuse records — even to other providers.
- 14 Audit trails specifically track access to 42 CFR Part 2 protected records.
- 15 Re-disclosure notices are included with any permitted sharing of substance abuse records.

Device & Endpoint Security

- 16 All devices (including personal laptops used for work) run endpoint detection and response (EDR).
- 17 Full-disk encryption (BitLocker/FileVault) is enabled on every device that accesses patient data.

- 18 Mobile devices with EHR access have remote wipe capability enabled.

Network & Home Office Security

- 19 Office or home network uses business-class firewall — not a consumer ISP-provided router.
- 20 Wi-Fi uses WPA3 or WPA2-Enterprise; clinical devices are on a separate network from personal devices.
- 21 VPN is used for any remote access to practice systems or shared drives.

Documentation & Training

- 22 Written HIPAA Security Risk Assessment completed within the last 12 months.
- 23 All staff (including solo practitioner) complete annual HIPAA + 42 CFR Part 2 security training.
- 24 Business Associate Agreements (BAAs) are on file for every vendor with access to PHI.
- 25 Incident response plan documented and tested — you know what to do if a breach occurs.

Red Flags — Get Professional Help Immediately

If any of these apply to your practice, contact a security professional before your next audit:

- Session notes stored on a personal laptop without encryption or EDR
- Using Zoom, FaceTime, or Google Meet without a signed BAA for telehealth sessions
- No written risk assessment — the #1 finding in HIPAA audits and malpractice claims
- Substance abuse records accessible to all staff without segmented access controls
- Sharing patient information via text message or regular (unencrypted) email
- Home Wi-Fi network shared with family members and smart home devices with no segmentation
- No BAAs on file for EHR, cloud storage, or telehealth vendors

Ready to Secure Your Practice?

Get a free security assessment — no obligation, no sales pitch.

(469) 306-9520 | pdgeek.com/contact

This checklist is for informational purposes only and does not constitute legal advice. HIPAA and 42 CFR Part 2 compliance require formal risk assessments conducted by a qualified professional. © 2026 Pleasant Digital LLC (PD Geek). All rights reserved.