Mentalyc

Free Therapist Source

2026 HIPAA Psychotherapy Notes Compliance Checklist

A pdf reference for solo and group private practices. Tape it inside your notes folder

By Dr. Salwa Zeineddine · Clinically reviewed by Brittainy Lindsey, LMHC, LPC · Updated June 2026

1. Psychotherapy notes vs progress notes

Psychotherapy notes

Your private reflections, hypotheses, supervision prompts. Stored separately. Written authorization needed for almost all disclosures. Client has no HIPAA access right

Progress notes

The official treatment record: interventions, response, diagnosis, plan. Part of the medical record.Disclosable for treatment, payment, operations.

- [ ] Keep psychotherapy notes physically/electronically separate
  — mixing them into the chart strips HIPAA protection (45 CFR 164.501).
- [ ] Keep treatment content out of psychotherapy notes
  — meds, test results, diagnosis, plan, start/stop times belong in the progress note

2. 2026 encryption & MFA requirements

- [ ] Encrypt all ePHI at rest and in transit
  — NIST-level, 256-bit minimum. "Addressable" is no longer a defense
- [ ] Enable MFA on every account that touches PHI
  — EHR, email, cloud storage, AI tools.
- [ ] No PHI on personal devices or consumer cloud
  — no standard Gmail/Outlook, Dropbox, Google Drive, or iCloud without a BAA.

3. Access control

- [ ] Restrict psychotherapy notes to the originating therapist
  — role-based access in the EHR, not discretionary.
- [ ] No routine access for admin, billing, other clinicians, or supervisors
  — narrow exceptions only (same-client treatment, limited supervision, legal defense).
- [ ] Lock the screen when you step away; keep audit logs on
  — your EMR must track every view, edit, and delete

Mentalyc

Free Therapist Source

2026 HIPAA Psychotherapy Notes Compliance Checklist

A pdf reference for solo and group private practices. Tape it inside your notes folder

By Dr. Salwa Zeineddine · Clinically reviewed by Brittainy Lindsey, LMHC, LPC · Updated June 2026

4. Retention rules

- [ ] Keep records at least 6 years under HIPAA
  — from creation or date last in effect
- [ ] Follow the stricter state rule (often 7–10 years)
  — minors' records often until they reach 18 or 21 plus the standard period.
- [ ] Destroy properly and document it
  — shred paper, permanently delete digital, record the destruction.

5. Annual review prompts

- [ ] Run a documented Security Risk Analysis + remediation plan
  — OCR's 2026 priority now includes risk management, not just the assessment.
- [ ] Re-run the SRA after any material change
  — new EHR, new staff with PHI access, new vendor, or a breach
- [ ] Confirm your revised Notice of Privacy Practices is posted
  — deadline was February 16, 2026 (SUD + redisclosure language).
- [ ] Train everyone with PHI access annually; document attendance
  — training records are reviewed in OCR audits.

6. BAA verification checklist for AI tools

- [ ] Signed BAA in place before the first transcription
  — not just "claims HIPAA-compliant" on the website
- [ ] Explicit ban on training models on your patient data
  — generic vendor BAAs often miss this.
- [ ] Annual SOC 2 Type II report available
  — plus encryption at rest and in transit.
- [ ] Accessible audit logs and subcontractor BAA chain
  — if audio goes to a third party, that party needs its own BAA
- [ ] Defined data destruction with certification on cancellation
  — negotiate breach notice down to 24–72 hours from discovery.