HIPAA Compliance Checklist

For Mental Health Therapists | January 2026

DOCUMENTATION & POLICIES

- ■ Written HIPAA Privacy Policies and Procedures
- ■ Written HIPAA Security Policies and Procedures
- ■ Notice of Privacy Practices (NPP)
  - ■ NPP document created
  - ■ NPP provided to all clients
  - ■ Signed acknowledgment on file
- ■ Risk Assessment completed and documented
- ■ Breach Notification Procedures documented
- ■ Records Retention Policy (minimum 6 years; check state law)
- ■ Sanction Policy for workforce violations

Note: Risk assessment should be repeated annually or when significant changes occur.

BUSINESS ASSOCIATE AGREEMENTS (BAAs)

- ■ EHR / Practice Management Software
- ■ Telehealth Platform
- ■ Billing Service or Clearinghouse
- ■ Cloud Storage (if storing PHI)
- ■ Email Service (if sending PHI)
- ■ Answering Service
- ■ IT Support (if they access PHI)
- ■ Shredding / Document Destruction Service
- ■ BAA copies saved and accessible

Note: No BAA = HIPAA violation, even without a breach. Verify BAA before using any vendor.

TECHNOLOGY SAFEGUARDS

- ■ HIPAA-compliant EHR system with signed BAA
- ■ HIPAA-compliant telehealth platform
  - ■ Platform provides BAA
  - ■ End-to-end encryption confirmed
  - ■ NOT using: standard Zoom, FaceTime, Skype
- ■ All devices encrypted (laptops, tablets, phones)
- ■ Strong, unique passwords on all systems
- ■ Two-factor authentication (2FA) enabled where available
- ■ Automatic screen lock (15 minutes or less)
- ■ Automatic logoff from EHR after inactivity
- ■ Secure WiFi (not public) or VPN for remote work
- ■ Antivirus / security software installed and updated
- ■ Regular data backups (encrypted)

PHYSICAL SAFEGUARDS

- ■ Private office space for sessions (door closes/locks)
- ■ Computer screens not visible to unauthorized persons

- ■ Paper records in locked storage (if applicable)
- ■ Secure disposal of paper PHI (shredding)
- ■ Workstation in secure location
- ■ Visitor access controlled

WORKFORCE TRAINING

- ■ Initial HIPAA Training completed
  - ■ Privacy Rule training
  - ■ Security Rule training
  - ■ Practice-specific policies reviewed
- ■ Training completion documented with date and signature
- ■ Annual refresher training scheduled
- ■ Training records retained (6+ years)
- ■ All staff trained (including part-time, contractors, interns)

Note: Even solo practitioners must document self-training.

CLIENT COMMUNICATION

- ■ Secure messaging system in place OR
  - ■ Policy prohibits sending PHI via standard email/text
  - ■ Policy documented and communicated to clients
- ■ Client communication preferences documented
- ■ Informed consent for electronic communication obtained
- ■ Telehealth consent form (if providing telehealth)

CLIENT RIGHTS PROCEDURES

- ■ Process for clients to access their records (within 30 days)
- ■ Process for clients to request amendments
- ■ Process for accounting of disclosures
- ■ Process for restricting certain disclosures
- ■ Complaint process communicated to clients