

Behavioral Health HIPAA Checklist

Practice Name: _____

Date: _____

Reviewer: _____

Privacy/Security Officer: _____

1. Privacy Policies & Staff Training

- ☐ HIPAA Privacy Officer designated in writing
- ☐ HIPAA Security Officer designated in writing
- ☐ Written privacy and security policies maintained and reviewed within the last 12 months
- ☐ Staff trained on HIPAA privacy and security requirements at hire and at least annually
- ☐ Staff training records maintained
- ☐ Sanctions policy for violations documented and applied
- ☐ Staff access updated promptly when roles change or employment ends
- ☐ HIPAA documentation (policies, logs, forms, risk analyses) retained for 6 years

2. Patient Privacy & Consent

- ☐ Notice of Privacy Practices provided at first visit, posted in the office, and on the website
- ☐ Acknowledgment of receipt documented
- ☐ Consent for treatment completed, when applicable
- ☐ Patient identity verified when appropriate
- ☐ Parent, guardian, or personal representative authority verified, when applicable
- ☐ State minor-consent laws for behavioral health reviewed and followed
- ☐ Patient communication preferences documented (phone, text, email, voicemail, who may receive information)
- ☐ Valid authorization obtained before disclosures that require one

- ☐ Minimum necessary standard applied to uses and disclosures other than treatment
- ☐ Record access requests fulfilled within 30 days (one 30-day extension allowed with written notice)
- ☐ Process in place for amendment requests, accounting of disclosures, restriction requests, and confidential communication requests

3. Behavioral Health Records

- ☐ Access to sensitive behavioral health information limited by role
- ☐ Psychotherapy notes kept separate when they meet HIPAA's definition of psychotherapy notes
- ☐ Separate authorization obtained for psychotherapy notes when required
- ☐ Information shared with family members or other third parties according to HIPAA and the patient's wishes
- ☐ State mental health confidentiality and duty-to-warn laws reviewed; stricter state rules followed

4. Electronic & Physical Security

- ☐ Unique user account for every staff member; no shared logins
- ☐ Access permissions assigned by job role and reviewed at least quarterly
- ☐ Multi-factor authentication enabled for EHR, email, and remote access
- ☐ Strong password requirements and automatic logoff set on all devices
- ☐ ePHI encrypted at rest and in transit (laptops, phones, backups, email)
- ☐ Audit logs enabled and reviewed on a set schedule
- ☐ Paper records stored in locked areas
- ☐ Paper records and devices disposed of securely; disposal logged
- ☐ Data backups tested; contingency and emergency-mode plan documented
- ☐ HIPAA Security Risk Analysis completed, documented, and updated at least annually or after major changes
- ☐ Risk management plan in place with assigned fixes

5. EHR, Vendors & Communication

- ☐ EHR and billing system safeguards reviewed
- ☐ Vendor inventory maintained (EHR, billing, telehealth, texting, cloud storage, shredding, IT)
- ☐ Business Associate Agreement signed with each vendor that handles PHI
- ☐ Only approved, secure communication methods used for patient information
- ☐ Recipients verified before sensitive information is sent
- ☐ Voicemails, texts, and appointment reminders limited to the minimum necessary (no diagnosis or treatment details)

6. Telehealth Privacy

- ☐ Telehealth platform security reviewed; Business Associate Agreement signed
- ☐ Telehealth consent obtained and documented
- ☐ Patient identity and location confirmed at the start of each session
- ☐ Provider uses a private space; patient asked to confirm theirs
- ☐ Emergency procedure established (patient location, local emergency contact, 988 information)
- ☐ Session recording done only with consent and according to policy and state law

7. Security Incidents & Breaches

- ☐ Staff know how to report suspected privacy or security incidents
- ☐ Procedure established for lost or stolen devices and unauthorized access
- ☐ Misdirected messages and suspected disclosures investigated
- ☐ Incidents documented, with a breach risk assessment completed for each
- ☐ Breach notice sent to affected individuals within 60 days of discovery; HHS and media notices made when thresholds are met
- ☐ State breach notification laws reviewed
- ☐ Corrective actions documented, assigned, and tracked to completion

8. Substance Use Disorder (SUD) Records (42 CFR Part 2)

- ☐ Determined whether the practice is a Part 2 program
- ☐ Part 2 privacy notice updated to the 2024 final rule (compliance date was February 16, 2026)
- ☐ Written consent forms meet Part 2 requirements (a single consent for future treatment, payment, and operations is permitted)
- ☐ Restrictions on disclosure and redisclosure followed; required notices attached to disclosures
- ☐ SUD records segregated or flagged in the EHR
- ☐ Staff trained on Part 2 confidentiality requirements
- ☐ Part 2 breach notification procedures maintained
- ☐ Part 2 records not used in legal proceedings against a patient without consent or a court order

9. Final Compliance Review

- ☐ Privacy and security policies reviewed
- ☐ Staff training documentation checked
- ☐ Required forms and authorizations reviewed
- ☐ Security risks and gaps documented
- ☐ Corrective actions assigned to responsible staff with due dates
- ☐ Follow-up review date scheduled (at least annually)
- ☐ Compliance documentation stored securely and retained for 6 years

Reviewer Signature: _____

Date: _____

Next Review Date: _____