



HIPAA Compliance Checklist

For Behavioral Health & Small Private Practice Offices

Administrative Safeguards

- Privacy Officer assigned
- Security Officer assigned
- HIPAA policies and procedures documented
- Workforce HIPAA training completed
- New staff HIPAA orientation completed
- Sanctions policy in place for violations
- Business Associate Agreements signed and current
- Risk assessment completed and documented
- Risk management plan in place
- Access to PHI limited by role

Privacy Requirements

- Notice of Privacy Practices available to patients
- Patient authorization process in place
- Minimum necessary standard followed
- Release of information procedures documented
- Patient right to access records process in place
- Patient amendment request process in place
- Patient restriction request process in place
- Confidential communication request process in place

Security Safeguards

- Unique user logins assigned
- Password policy in place
- Automatic screen lock enabled
- Antivirus and system updates current
- Secure email procedures in place
- Encryption used where appropriate
- Backup system active and tested
- Secure storage for paper records
- Secure disposal/shredding process in place
- Facility access controls in place

Behavioral Health Considerations

- Psychotherapy notes stored separately when applicable
- Sensitive behavioral health records access limited appropriately
- Staff trained on extra confidentiality considerations
- Telehealth privacy procedures in place
- Private areas used for counseling and patient calls
- Substance use disorder record protections reviewed when applicable

Incident Response

- Breach reporting procedure documented
- Security incident response process in place
- Suspected unauthorized access reviewed promptly
- Patient notification workflow established when required
- Documentation of incidents maintained

Ongoing Compliance Review

- Annual HIPAA training scheduled
- Periodic policy review scheduled
- Periodic access review completed
- Vendor/business associate review completed
- Compliance checklist reviewed and updated regularly

Office Notes / Follow-Up Actions

This checklist is for general educational and operational support purposes only and is not legal advice. Requirements may vary based on setting, services, and applicable federal or state rules.