☑ CFR PART 2 COMPLIANCE CHECKLIST

Confidentiality of Substance Use Disorder (SUD) Patient Records
System Base Labs — Ethical AI Governance

SECTION 1 — SUD DATA IDENTIFICATION & CLASSIFICATION

Identify All Part 2 Data Sources
☐ SUD diagnosis records
☐ SUD treatment notes
☐ Medication-Assisted Treatment (MAT) data
☐ Opioid Treatment Program (OTP) data
☐ Counseling and psychotherapy notes
☐ Referrals to SUD programs
☐ Telehealth SUD sessions
☐ Predictive analytics containing SUD indicators
☐ Any data revealing a patient has a SUD condition

Classify Data Risk Level
☐ Part 2-Protected SUD Records
☐ SUD-Adjacent Behavioral Health Records
☐ Non-SUD Health Records
☐ De-identified or anonymized SUD data

SECTION 2 — CONSENT MANAGEMENT

Written Patient Consent Requirements
☐ Consent form includes "To Whom," "For What Purpose," "What Information"
☐ Consent specifies AI/system use if applicable
☐ Consent revocation workflow implemented
☐ Consent expiration timelines adhered to
☐ Consent logs stored securely
☐ No access to SUD data without valid consent

System Base Labs

A Carbon-Neutral Company 🌿

SBL

Today's AI Startup. Engineering the Intelligence of Tomorrow

Redisclosure Prohibition Compliance
□ No sharing of Part 2 data beyond named recipient
□ Redisclosure warnings auto-attached to all records
□ APIs block outbound redisclosure
□ Audit logs track all disclosures

SECTION 3 — DATA SEGREGATION & ACCESS CONTROL

Segregation Controls
□ SUD data stored separately from general PHI
□ Separate database collections / access labels
□ AI training pipelines prevent SUD data mixing
□ Logging streams separated

Access Controls
□ Role-based access (RBAC) with SUD-specific roles
□ Attribute-based access control (ABAC) for SUD tags
□ MFA required for SUD-data access
□ Access reviewed quarterly
□ Emergency access ("break-glass") rules defined

SECTION 4 — TECHNICAL SAFEGUARDS

Encryption
□ Encryption at rest (AES-256)
□ Encryption in transit (TLS 1.2+)
□ Key vault management implemented

Monitoring & Auditing
□ Real-time monitoring of SUD access
□ Audit logs immutable
□ Alerts for unauthorized access

AI-First Technology   Ethical AI   GPU Farms   Shankar AI   Blockchain + Biomedical   Education

System Base Labs

A Carbon-Neutral Company 🌿

SBL

Today's AI Startup. Engineering the Intelligence of Tomorrow

☐ Monthly audit reports generated

Integrity & Security Controls
☐ Hashing applied to stored records
☐ Backups encrypted
☐ Zero-trust network policies applied

SECTION 5 — AI-SPECIFIC PART 2 CONTROLS

AI Model Training
☐ SUD data not used unless explicitly consented
☐ De-identified data validated by expert
☐ Synthetic data documented
☐ Bias & feature-importance analysis for SUD indicators

AI Predictions & Outputs
☐ AI cannot reveal SUD status without consent
☐ Clinical dashboards hide SUD-related model outputs unless authorized
☐ Explainability tools do not expose SUD data
☐ Drift monitoring for SUD-sensitive models

AI Deployment Controls
☐ SUD-restricted inference endpoints
☐ Layered authorization before inference
☐ API tokens segmented for SUD workflows
☐ Logging per-prediction access

SECTION 6 — ORGANIZATIONAL & ADMINISTRATIVE SAFEGUARDS
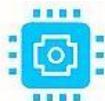
Policies & Procedures
☐ Written Part 2 compliance policy
☐ Redisclosure prohibition policy
☐ SUD-specific access control policy

AI-First Technology   Ethical AI   GPU Farms   Shankar AI   Blockchain + Biomedical   Education

System Base Labs

A Carbon-Neutral Company 🍃

SBL

Today's AI Startup. Engineering the Intelligence of Tomorrow

☐ Consent & revocation SOPs

☐ Emergency disclosure policy

Training & Workforce Management

☐ Annual staff training on Part 2

☐ Role-specific training for clinicians, developers, data staff

☐ Signed acknowledgment of obligations

Business Associate Agreements (BAAs)

☐ BAAs updated to include Part 2 obligations

☐ Vendors evaluated for SUD data protection

☐ Redisclosure restrictions spelled out

SECTION 7 — TELEHEALTH & DIGITAL COMMUNICATIONS

Telehealth Compliance

☐ Encrypted video sessions

☐ No unapproved recording

☐ Secure patient authentication

☐ No SUD notes stored on provider devices

Messaging & Communication

☐ Secure messaging channels (end-to-end encrypted)

☐ No SMS/email sharing of SUD info

☐ Access logs for all communications

SECTION 8 — INCIDENT RESPONSE & BREACH NOTIFICATION

Incident Handling

☐ Defined process for SUD-related breaches

☐ Rapid isolation rules

☐ Forensic audit procedure

AI-First Technology   Ethical AI   GPU Farms   Shankar AI   Blockchain + Biomedical   Education

Notification Requirements
□ Notify patient if unauthorized disclosure occurs
□ Document breach details
□ Maintain records for required duration

SECTION 9 — DOCUMENTATION & RETENTION

Required Records
□ Consent forms
□ Disclosure logs
□ Redisclosure restriction statements
□ Training logs
□ Access logs
□ Technical audit trails
□ De-identification certifications

Data retained according to federal requirements.

SECTION 10 — CONTINUOUS COMPLIANCE

Ongoing Actions
□ Quarterly access reviews
□ Annual Part 2 risk assessment
□ Model drift review (if AI is involved)
□ Vendor re-evaluation
□ Governance committee review