☑ CFR PART 2 — RISK HEAT MAP

Risk Severity Across Compliance Domains
Color coding:

High Risk (Red) – regulatory violation likely, severe penalties

Medium Risk (Orange) – operational weakness, fix required

Low Risk (Green) – compliant or controlled

💧 1. Consent & Authorization Risks

RISK AREA	DESCRIPTION	RISK LEVEL
Missing written patient consent	AI/system uses Part 2 data without explicit consent	▩ High
Consent form lacks required elements	No specification of purpose, recipient, or description	▩ High
No revocation workflow	Patient cannot withdraw consent effectively	▨ Medium

💧 2. Redisclosure Risks

RISK AREA	DESCRIPTION	RISK LEVEL
Part 2 data shared with unauthorized entities	Redisclosure without permission	▩ High
APIs not blocking outbound SUD data	Technical redisclosure vulnerability	▩ High
Clinical dashboards revealing SUD data	Unauthorized SUD exposure	▩ High

💧 3. Data Segregation & Storage Risks

RISK AREA	DESCRIPTION	RISK LEVEL
SUD data stored with general PHI	No logical/physical separation	▨ High
Mixed AI training datasets	SUD data contaminates general models	▨ High
Lack of labeling/tagging SUD data	Misclassification leads to accidental disclosure	▧ Medium

💧 4. Access Control Risks

RISK AREA	DESCRIPTION	RISK LEVEL
Too broad access permissions	Non-authorized staff can view SUD records	▨ High
No MFA for SUD access	Weak user verification	▧ Medium
Lack of quarterly access review	Permissions remain outdated	▧ Medium

💧 5. AI-Specific Risks

RISK AREA	DESCRIPTION	RISK LEVEL
AI models inferring SUD status	Output indirectly reveals protected data	▨ High
SUD indicators used in predictions without consent	Violates Part 2 restrictions	▨ High
Model drift exposing patterns	Over time, AI exposes sensitive trends	▧ Medium

6. Telehealth & Messaging Risks

RISK AREA	DESCRIPTION	RISK LEVEL
Telehealth sessions unencrypted	High exposure event	▨ High
Staff using SMS/email for SUD data	High redisclosure risk	▨ High
Local device storage of sessions	Uncontrolled PHI spread	▧ Medium

7. Logging & Monitoring Risks

RISK AREA	DESCRIPTION	RISK LEVEL
No dedicated logs for SUD access	Cannot prove compliance	▨ High
Incomplete audit trails	Breach investigations impossible	▨ High
Insufficient anomaly detection	Hidden unauthorized access	▧ Medium