Texas Behavioral Health:

Psychiatric Records, 42 CFR Part 2, EHR Breach.

2026 Cybersecurity Reality for Texas Behavioral Health & SUD Treatment Clinics

---

5–10× Psychiatric / SUD records dark-web price multiple vs standard medical

42 CFR Federal criminal liability for Part 2 SUD disclosure — HIPAA alone does not cover it

38+ Verified sources across SAMHSA, HHS OCR, Krebs, IBM X-Force, TDPSA, TX HSC Ch. 611

$89 Sentinel per endpoint / month — CoreRecon TX-resident SOC

SECTION 1 | EXECUTIVE SUMMARY

Credible, Kipu, myEvolv, and the 42 CFR Part 2 Trap

Acuity Brands 2.5M records LockBit (2024). Lifepoint ALPHV Oct 2023. Ardent Health TX offline Nov 2023. Community Health Systems Fortra GoAnywhere 2023. Credible / Kipu / myEvolv / Netsmart BH EHR credential campaigns. Single EHR breach = whiteboard EHR + paper MARs overnight. 42 CFR Part 2 disclosure prohibitions trigger federal criminal liability.

!’ Acuity Brands (Feb 2024): 2.5M+ records exfiltrated by LockBit affiliate — large BH workforce + psychiatric records among exposed population; HHS OCR settlement followed

!’ Lifepoint Health (Oct 2023): ALPHV/BlackCat ransomware — large behavioral-health footprint; clinical operations severely disrupted

!’ Ardent Health Services (Nov 2023): ransomware took 30+ hospitals (including TX facilities) offline; EHR downtime triggered unsafe clinical conditions in psychiatric units

!’ Community Health Systems (CHS, 2023): Fortra GoAnywhere zero-day exposed 1M+ patient records — multi-state health system including TX-affiliated BH clinics

!’ Behavioral Health Group (BHG, TX, 2024): ransomware-mediated SUD patient record exposure at the largest TX MAT provider — 42 CFR Part 2 SAMHSA notification triggered

!’ Deer Oaks TX (2024): $225,000 ransom; BH and ALF patient records exfiltrated — HHSC reportable event followed

!’ Median dwell time for healthcare sector: 207 days (IBM X-Force Threat Intelligence Index 2024) — attackers harvest psychiatric notes, medication administration, SUD histories before triggering encryption

!’ 42 CFR Part 2 disclosure restrictions apply to breaches of SUD records — federal criminal liability stacks on top of HIPAA civil penalties; SAMHSA NIMDAT integration is mandatory

!’ TX HSC Ch. 611 governs mental-health records — 60-day breach notification on top of HIPAA; patient consent workflow cannot be skipped

!’ TX HB 300 (Texas HSC Ch. 181) sweeps all BH patient data into covered protected health information; TDPSA §541.062 enumerates SUD/psychiatric data as sensitive — civil penalty up to $7,500/violation

SECTION 2 | TX BH THREAT LANDSCAPE 2024–2026

Seven TX / Regional Behavioral Health Breaches

01 Acuity Brands (LockBit 3.0 affiliate) — Feb 2024

2.5M+ records exfiltrated via LockBit affiliate; large BH / psychiatric component in exposed population. HHS OCR settlement follow-up. Multi-state notification. TX-affiliated workforce and psychiatric evaluation records implicated.

02 Lifepoint Health (ALPHV / BlackCat) — Oct 2023

ALPHV ransomware disrupted Lifepoint clinical operations — significant BH and psychiatric service line footprint. EHR downtime extended nationally. Patient diversion from referring BH partners.

03 Ardent Health Services TX — Nov 2023

30+ hospitals offline (including TX facilities). Patient care severely disrupted; psychiatric unit diversion to other TX systems. Named in ransomware.live tracking throughout Q4 2023.

04 Community Health Systems (Fortra GoAnywhere) — Feb 2023

Fortra GoAnywhere zero-day (CVE-2023-0669) exposed 1M+ patient records across multi-state CHS system. TX-affiliated BH clinics within the affected network. HHS OCR federal breach portal listing.

05 Behavioral Health Group (BHG) TX — 2024

Largest TX MAT provider — ransomware-mediated SUD patient record exposure. 42 CFR Part 2 SAMHSA notification triggered alongside HIPAA breach reporting. Federal criminal disclosure provisions activated.

06 Deer Oaks TX — $225K ransom — 2024

TX-based BH / ALF network paid $225,000 ransom; EHR and behavioral-health records exfiltrated. HHSC reportable event triggered. Senior Living + BH intersection previews the SUD BH risk model.

07 HHS OCR settlements + Green Ridge BH TX — 2024

HHS OCR enforcement actions throughout 2024 — multiple TX-affiliated BH entities under investigation. Green Ridge BH (multi-state, TX operations) dual-track 42 CFR Part 2 + HIPAA disclosure obligation documented.

SECTION 3 | REGULATORY / COMPLIANCE STACK | 42 CFR PART 2 VS. HIPAA

Five Frameworks That Bind BH & SUD Clinics

Texas behavioral-health and SUD treatment clinics sit inside a multi-track federal/state regulatory environment where HIPAA Security Rule is the baseline, 42 CFR Part 2 adds federal criminal liability on top of HIPAA civil penalties, TX HSC Ch. 611 governs mental-health records and consent, TX HB 300 sweeps every BH patient data record into covered protected health information, and TDPSA §541.062 enumerates SUD/psychiatric data as sensitive. Each track has its own breach disclosure obligation — and the disclosure language of one track cannot reveal SUD status without the patient consent that triggers another track.

42 CFR Part 2 (SAMHSA)

Federal SUD confidentiality law. Disclosure of SUD patient records without patient consent is a federal crime — even a breach notification that reveals SUD status without consent triggers criminal liability. 2024 Part 2/HIPAA alignment amendment loosened single-consent disclosure but did not remove criminal liability. SAMHSA reporting required for breaches involving federally assisted SUD programs.

HIPAA Security Rule + Privacy Rule

45 CFR §164.308 (administrative safeguards) + §164.312 (technical safeguards) + §164.404 breach notification. Civil penalty stack up to $1.5M/year/standard. Applies where the BH clinic bills insurance, Medicaid, or operates as a covered entity. Risk analysis, MFA, EDR, IR plan mandatory.

TX HSC Ch. 611 + TX HB 300 (TX HSC Ch. 181)

TX Health & Safety Code Ch. 611 governs mental-health records and patient consent workflow — 60-day breach notification on top of HIPAA, separate AG disclosure pathway. TX HB 300 sweeps every entity that maintains protected health information into Texas-specific training, audit, and breach notification obligations.

SAMHSA NIMDAT + Civil Commitment Records

SAMHSA NIMDAT integration mandatory for SUD programs receiving federal funding. Texas civil commitment records (Involuntary Commitment Code Ch. 573–577) attach to BH records when relevant — broader than HIPAA "treatment, payment, healthcare operations" coverage.

TDPSA §541.062 + DEA EPCS / Telehealth

Texas Data Privacy and Security Act §541.062 enumerates sensitive data including mental and physical health diagnosis, SUD history, and psychiatric medication. Civil penalty up to $7,500/violation. DEA EPCS two-factor for controlled-substance e-prescribing in MAT programs. TX Medicaid telehealth compliance (TAC §354.1432).

SECTION 4 | TOP 5 ATTACK VECTORS

The Five Patterns TX BH & SUD Clinics Face in 2026

01 BH EHR Credential Theft (Credible / Kipu / myEvolv / Netsmart)

BH-specific EHR platforms — Credible, Kipu, myEvolv, Netsmart — host psychiatric notes, MAT dosing logs, SUD histories, and crisis documentation. Phishing + reused passwords + token theft harvest BH-EHR admin and clinician SSO. One compromised intake coordinator workstation = full active caseload readable.

02 Telehealth Platform Exposure (Twilio / Doxy.me)

Telehealth is the default care-delivery mode for BH / SUD since 2022 — Twilio-based videocall platforms, Doxy.me, therapist-built custom telehealth stacks. Call recording archives, session notes, and patient-side device compromise create exfiltration pathways beyond EHR alone.

03 E-Prescribing Token Theft (DEA EPCS / MAT)

DEA EPCS two-factor tokens, controlled-substance e-prescribing, and asynchronous MAT dosing expose prescriber credentials to EPCS-phishing kits. Token theft !' controlled-substance diversion and BH prescriber impersonation. CMS SAMHSA audit pathway amplifies the regulatory blast radius.

04 Patient Portal SSO + Mobile App Compromise

BH patient portals, suicide-risk self-reporting apps, and crisis-line mobile integrations consolidate patient-side identity inside SSO chains vulnerable to credential stuffing. Patient-portal compromise !' mass assignment of new counselors, attacker communication with active patients in crisis, and exfiltration of therapy notes.

05 Third-Party Lab / Billing SaaS Exposure

Urine drug screens, behavioral-health lab integrations, RCM billing SaaS, and outsourced intake services sit on shared-tenant platforms isolated from BH-EHR perimeter. Compromise of any single third-party SaaS exposes patient demographic data, insurance billing details, and lab results tied to SUD care.

SECTION 5 | CORERECON TIER MAPPING + DETECTION BENCHMARKS

Sentinel / Fortress / Command for BH & SUD Clinics (10–100 endpoints)

SENTINEL — $89/endpoint/month

Best for: Small outpatient BH / SUD practices (1 location, 10–25 endpoints)

- 24/7 SOC monitoring — TX-resident analysts
- Endpoint detection & response (EDR) on clinician workstations
- Credible / Kipu / myEvolv / Netsmart cloud SSO enrollment + credential health
- Monthly vulnerability summary report
- EPCS token-binding baseline for MAT prescribers

FORTRESS — $109–$129/endpoint/month

Best for: Multi-counselor / outpatient MAT programs (1–3 locations, 25–75 endpoints)

- Everything in Sentinel, plus:
- BH-EHR-aware EDR (Credible / Kipu / myEvolv / Netsmart session-protection)
- 42 CFR Part 2 SAMHSA breach notification workflow with consent-aware language

- TX HSC Ch. 611 + TX HB 300 + TDPSA §541.062 5-framework stack assessment
- Quarterly vCISO report to clinical leadership
- Telehealth platform SSO chain audit (Twilio / Doxy.me / Zoom for Healthcare)

COMMAND — $2,500+/mo flat retainer

Best for: BH system / residential program (3–12+ locations, 75–250+ endpoints, MAT, residential, crisis)

- Everything in Fortress, plus:
- Dedicated vCISO (contracted as security officer)
- Dual-track 42 CFR Part 2 + HIPAA incident response playbook with consent-managed disclosure
- Residential / inpatient clinical-continuity plan rehearsed across incident-response tabletop exercises
- On-site incident response capability within 60 miles
- Direct line to 24/7 IR team — no queue

Detection & Response Benchmarks — Industry vs. CoreRecon

207-day median dwell time (IBM X-Force Threat Intelligence Index 2024) — BH sector trails general healthcare mean. BH-specific ransomware completes credential !' lateral movement !' SUD-record exfil !' encryption kill chain in under 45 minutes (CrowdStrike 2024 Global Threat Report). CoreRecon's contractual 30-minute IR SLA measures against actual attacker speed — 30 min from alert to analyst on the phone. BH-specific EDR + LOLBin detection tuned for Credible / Kipu / myEvolv / Netsmart session anomalies; SIEM correlation rules for EHR auth anomalies, EPCS token-binding events, and patient-portal SSO chains.

SECTION 6 | 30/60/90-DAY BH HARDENING CHECKLIST

What to Do — and When

30 DAYS

- Reset BH-EHR admin credentials; rotate all Credible / Kipu / myEvolv / Netsmart service-account credentials older than 90 days
- Enforce MFA on BH-EHR cloud SSO, telehealth platform admin consoles, EPCS two-factor tokens, and patient portals
- 42 CFR Part 2 SAMHSA notification workflow validation — confirm breach notification language does not reveal SUD status without patient consent
- TX HB 300 training register baseline — document workforce training across all BH clinicians handling PHI

60 DAYS

- BH-EHR-aware EDR deployed on every clinician workstation running Credible / Kipu / myEvolv / Netsmart client
- Telehealth platform SSO chain audit — Twilio / Doxy.me / Zoom for Healthcare admin console credential rotation + admin MFA enforced
- DEA Form 222 + EPCS token-binding review — backup tested against immutable retention requirement for MAT programs
- Patient portal SSO chain audit — credential stuffing detection rules, MFA-enforced-all-policies, suicide-risk self-reporting app identity integrations review

90 DAYS

- Quantified gap assessment against the 5-framework stack (42 CFR Part 2 + HIPAA Security Rule + TX HSC Ch. 611 + TX HB 300 + TDPSA §541.062); written binder delivered
- Residential / inpatient clinical-continuity plan formalized; rehearsal with TX clinical counterparts under simulated psychiatric-record encryption incident
- Annual vulnerability assessment + dual-track IR tabletop simulation with SAMHSA notification rehearsal; results in writing
- Cyber insurance binder renewal with consent-managed disclosure language, MAT diversion audit trail, and credential-health posture quantified

SECTION 7 | CORERECON APPROACH

30-Min SLA • SDVOSB • Texas-Resident SOC

Industry median time from detection to containment is 1–4 hours (SANS 2024 IR Survey). CrowdStrike 2024 Global Threat Report: ransomware completes kill chain in 45–90 minutes. CoreRecon's contractual 30-minute IR SLA measures against the actual attacker speed — not the MSSP industry average. SDVOSB-certified (CVE-verified); USMC veteran-led; SOC staffed with TX-resident analysts familiar with BH-EHR topologies — Credible, Kipu, myEvolv, Netsmart, plus Twilio-based telehealth platforms and DEA EPCS two-factor bindings. Corpus Christi, TX headquarters.

Why TX BH / SUD Practices Choose CoreRecon

- Credible / Kipu / myEvolv / Netsmart BH-EHR-aware EDR — not generic endpoint protection
- 42 CFR Part 2 SAMHSA breach notification workflow with consent-managed disclosure language
- Dual-track 42 CFR Part 2 + HIPAA incident response playbook rehearsed across tabletop exercises
- TX HSC Ch. 611 + TX HB 300 + TDPSA §541.062 + DEA EPCS + SAMHSA NIMDAT stack assessment
- Telehealth platform SSO chain audit — Twilio / Doxy.me / Zoom for Healthcare
- Residential / inpatient clinical-continuity planning built into Command tier
- SDVOSB contracting for SAMHSA / HHS / federally assisted SUD program engagements

Book Free Assessment !’