Texas Behavioral Health & Mental Health Clinics: HIPAA, 42 CFR

2026 Cybersecurity Reality for TX BH Outpatient, IOP/PHP, Psychiatry Practices & MSO Networks

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

42 CFR Federal criminal liability on unauthorized SUD record disclosure

$7,500 Per-violation civil penalty — TX HB300 + TDPSA §541.062

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

SECTION 1 | HIPAA PAIN POINTS — TX CLINICS & MSO NETWORKS

BH-EHR Credential Hygiene, Telehealth Recording, Multi-County MSO

HIPAA Security Rule (45 CFR §164.308 administrative safeguards plus §164.312 technical safeguards) requires documented risk analysis, MFA, audit logging, encryption-in-transit, and encryption-at-rest — and Texas behavioral-health and mental-health clinics run multi-clinic MSO networks, BH-EHR credential sprawl, telehealth session recording footprints, intake-paper residual PHI, and patient-portal MFA bypasses at scale. The Acuity Brands (Feb 2024, LockBit 3.0 affiliate, 2.5M+ records including psychiatric/SUD data on affiliated behavioral-health populations), Lifepoint Health (Oct 2023 ALPHV/BlackCat, large BH service-line footprint, NIH-affiliated research), Ardent Health Services TX (Nov 2023, 30+ hospitals offline including TX facilities, psychiatric-unit diversion documented), Community Health Systems Fortra GoAnywhere (Feb 2023, CVE-2023-0669 zero-day, 1M+ patient records across multi-state BH network), Acuity (Feb 2024 BH workforce slice of LockBit exfil), CHS Fortra GoAnywhere, and HHS OCR enforcement confirm what Texas BH executive directors and compliance officers already know: the BH-EHR admin SSO sprawl (Credible, Kipu, myEvolv, Netsmart) is now the perimeter and the credential-stuffing campaigns around these vendors are HHS-reportable under §164.408 breach notification within 60 days of discovery.

!’ Acuity Brands (Feb 2024) — LockBit 3.0 affiliate; 2.5M+ records exfiltrated; BH-affiliated workforce slice; HHS OCR enforcement action pending; HIPAA Security Rule §164.308 risk-analysis gap

!’ Lifepoint Health (Oct 2023) — ALPHV/BlackCat; clinical operations disrupted; large BH service-line footprint; NIH-affiliated patient data exposed on the affiliate leak site

!’ Ardent Health Services TX (Nov 2023) — 30+ hospitals offline including TX facilities; psychiatric-unit diversion to non-affiliated BH facilities documented; ransomware kill chain entered through third-party vendor

!’ Community Health Systems Fortra GoAnywhere (Feb 2023) — CVE-2023-0669 zero-day; 1M+ patient records exfiltrated; multi-state BH hospital network affected; OCR settlement in 2024

!’ Credible (BH-EHR) credential-stuffing campaigns — vendor advisory in 2024 exposed admin-side brute-force against clinic deployments; tx-bh-clinic SSO sprawl across multi-county deployments

!’ Kipu EMR (SUD/EHR) admin credential hygiene — Kipu markets to MAT providers; the Kipu admin console is now perimeter; SOC-side EDR on Kipu operator workstations is the minimum floor

!’ Netsmart myEvolv (BH-EHR for behavioral-health human-services) hosted deployment — 30+ state hosted instance; a single credential compromise exposes hundreds of clinics; BH-specific intake-data sprawl

!’ Multi-county MSO cross-county credential anomaly surface — SSO tokens issued in County A reused in County B; BH-MSO cyber-insurance underwriting now scores cross-county token reuse

!’ Telehealth session recording storage (TX Medicaid TAC §354.1432) — recorded sessions containing patient statements; cloud-stored recording bucket misconfiguration exposes millions of telehealth encounters

!’ Patient-portal MFA bypass — BH patient populations show low MFA opt-in; clinician-initiated portal bypass creates audit-log blind spots under §164.312(b) audit controls

!’ Intake-paper residual PHI — clinic intake desks accumulate physical paperwork with SUD/psychiatric disclosure; paper shredding process gaps + disposal vendor risk

!’ 30-min IR SLA — industry median 1–4 hour containment (SANS 2024 IR Survey); ransomware kill chain completes in 45–90 minutes (CrowdStrike 2024 Global Threat Report)

SECTION 2 | 42 CFR PART 2 — THE FEDERAL CRIMINAL-LIABILITY TRAP

Re-Disclosure Trap & Consent-Managed Breach Notification

42 CFR Part 2 — the SAMHSA Confidentiality of Substance Use Disorder Patient Records rule — imposes federal criminal liability (not just civil HIPAA penalties) on the unauthorized disclosure of any record that reveals a patient is in a federally assisted SUD program. The 2024 Part 2/HIPAA single-consent alignment amendment did NOT remove criminal liability: a breach notification letter that "reveals SUD status without patient consent" remains a federal crime. SAMHSA NIMDAT integration (now finalized) means federally assisted SUD programs must run SAMHSA-issued notification workflow on disclosure events. Court-ordered disclosure exceptions under Texas Ch. 573–577 (mental-health court-ordered treatment) require careful separation from Part 2 consent-managed disclosure. Written-consent language is now regulatory — not optional. The dual-track 42 CFR Part 2 + HIPAA breach notification (Part 2 SAMHSA pathway plus HIPAA 60-day HHS OCR clock) runs in parallel with materially different timelines.

!’ 42 CFR §2.13 — written patient consent required for any disclosure that reveals SUD status; breach notification language that names the SUD program is itself a Part 2 disclosure

!’ Federal criminal liability under 42 USC §290dd-2 — misdemeanor for first violation, felony for pattern; fines up to $500 per first offense, $5,000 per subsequent for knowing violations

!’ 2024 Part 2/HIPAA single-consent amendment (HHS Final Rule, Feb 2024) — aligned Part 2 consent requirements with HIPAA for treatment, payment, and healthcare operations — but criminal liability remained intact

!’ SAMHSA NIMDAT (National Inventory of Mental Health and Substance Abuse Treatment) integration — federally assisted SUD programs must register and run SAMHSA-issued notification workflow on Part 2 disclosure events

!’ Texas Civil Practice & Remedies Code Ch. 573–577 — court-ordered mental-health treatment disclosure exceptions are SEPARATE from Part 2 consent-managed disclosure for SUD; dual-track review is mandatory

!’ Written-consent language requirements — patient must sign a specific PART 2 consent naming the recipient program; the consent cannot be open-ended or "blanket"

!’ Breach-disclosure language that names the SUD program = federal crime — the disclosure letter itself becomes a Part 2 disclosure; consent-managed outbreak-notice templates required

!’ Dual-track breach notification calendar — Part 2 SAMHSA pathway (immediate, no defined clock — "as soon as practicable") + HIPAA 60-day HHS OCR clock (45 CFR §164.408) + TX HB300 60-day AG clock + TX HB300 30-day notice-to-individuals

!’ BH-EHR (Credible/Kipu/myEvolv/Netsmart) disclosure-log tools — modern BH-EHRs keep consent-managed disclosure-log entries; breach-notification automation must read consent log before sending notice

!’ Court-ordered disclosure exception (42 CFR §2.65) — usable only with specific court order; not a "blanket" exception; counsel must be involved before any Part 2 disclosure under court order

!’ Medical-emergency disclosure (42 CFR §2.51) — narrow exception; documentation of the emergency required; not a cover for routine breach notification

!’ Audit-research disclosure (42 CFR §2.52) — requires IRB approval + patient consent; not a cover for disclosure during an incident IR

!’ Deer Oaks Behavioral Health TX (2024) — $225K ransom; BH/ALF patient records exfiltrated; the breach notification required Part 2 dual-track because Deer Oaks operates an SUD treatment arm

SECTION 3 | SAMHSA / M&A VENDOR-RISK EXPOSURE

BH Roll-Up M&A Due Diligence, Hosted BH-EHR Concentration

Texas behavioral-health market saw a 2024–2026 acquisition wave across MSO roll-ups: federally assisted SUD program vendor flow-down under SAMHSA 42 CFR Part 2, M&A cyber-due-diligence gaps at the BH-roll-up stage, hosted BH-EHR (Kipu EMR, Netsmart myEvolv) vendor concentration risk, MSO acquisition cyber-liability representations and warranties gaps, and third-party BH-EHR BAA enforcement gaps. Behavioral Health Group TX (largest TX MAT provider), Green Ridge Behavioral Health TX, and Deer Oaks Behavioral Health TX APC are representative of the consolidation pattern. The cyber-liability stack at acquisition — including Part 2 disclosure history, prior OCR enforcement, BAA enforcement record, and BH-EHR vendor cyber posture — is now a deal-killer at TX BH MSO roll-up diligence.

!’ Federally assisted SUD program vendor flow-down — under 42 CFR Part 2, vendor flow-down contracts require Part 2-compliant confidentiality language; many 2018–2022 BH-EHR BAAs lack this clause

!’ M&A cyber-due-diligence gap (TX BH MSO roll-up acquisitions 2024–2026) — buyers conduct financial and clinical diligence; cyber/posture/Part 2 disclosure history diligence is frequently skipped or shallow

!’ BH Group TX — largest TX MAT provider; multi-county footprint; SUD program flow-down to local clinics; SAMHSA-registered; Part 2 disclosure history now part of M&A data room

!’ Green Ridge Behavioral Health TX — multi-clinic BH services operator; M&A in 2025; cyber-due-diligence became a board-level control under acquired-entity risk profile

!’ Netsmart myEvolv hosted concentration risk — single compromise exposes hundreds of TX BH clinics on one deployment; multi-tenant hosted risk now underwritten by cyber insurance markets

!’ Kipu EMR hosted deployment — Kipu for SUD treatment programs is a hosted multi-tenant; Kipu admin credential compromise = entire client base exposure

!’ BH-EHR BAA enforcement gaps — older 2018–2021 BH-EHR BAAs lack 42 CFR Part 2 vendor-flow-down language; enforcement gap becomes acquired-entity cyber-liability on M&A

!’ M&A representations & warranties — cyber-liability R&W insurance market now excludes BH/EHR/PHI carve-outs unless Part 2 disclosure history + OCR enforcement history is shared at diligence

!’ Hosted BH-EHR BAA enforcement under M&A — the buyer acquires the BAA liability; the seller's prior enforcement gaps become a buyer problem within first 12 months post-close

!’ Third-party BH-EHR SOC 2 / HITRUST certifications — many 2018–2022 deployments lacked renewed SOC 2 Type II; cyber-due-diligence should reject without current SOC 2 + HITRUST CSF

!’ M&A TX HSC Ch. 611 mental-health records custodian transfer — records custodian transfer requires HHSC-aligned notice to patients; cyber-incident-during-transition risk is the deal-killer

!’ Cybersecurity insurance underwriting for TX BH MSO roll-ups — carriers now require Part 2 disclosure history, OCR enforcement history, BH-EHR vendor cyber posture, and cyber-incident-response runbook readiness

SECTION 4 | TX HB300 + FTC HBNR NOTIFICATION CLOCK

60-Day AG Disclosure (HB300) + 30-Day FTC HBNR (Non-Covered Apps)

Texas Health & Safety Code Chapter 181 (TX HB300) imposes a 60-day Texas Attorney General breach notification clock (with concurrent 30-day individual notice) on covered entities that handle protected health information, with civil penalty up to $7,500 per violation. TDPSA §541.062 enumerates sensitive data including SUD and psychiatric information. The FTC Health Breach Notification Rule (16 CFR Part 318, updated 2024) covers non-covered-entity apps and vendors that handle health data outside HIPAA — a 30-day notification clock applies to vendors of health apps and similar non-HIPAA-covered entities. When a TX BH app or mental-health platform falls outside HIPAA (e.g., direct-to-consumer wellness apps), the FTC HBNR clock runs. The dual-track calendar — TX HB300 60-day AG + FTC HBNR 30-day — runs in parallel when applicable.

!’ TX HSC Ch. 181 (HB300, effective Sept 1, 2011 + subsequent amendments) — covered-entity definition includes BH providers, MSOs, hospitals, clinics, and any entity that maintains PHI

!’ 60-day Texas Attorney General breach notification clock — clock starts on discovery; substantial penalty for late notification; AG maintains public breach-notification database

!’ Civil penalty up to $7,500/violation under TX HB300 — each breached record is a separate violation; BH breach volumes push penalties into the millions

!’ 30-day individual-notice clock under TX HB300 — concurrent with the 60-day AG clock; HHSC notification may trigger additional obligations for licensed facilities

!’ TDPSA §541.062 sensitive-data enumeration — SUD records, psychiatric records, and mental-health records are explicitly enumerated as sensitive personal information

!’ TDPSA §541 opt-in consent requirement for sensitive-data processing — opt-in consent required; BH MSO web-portal designs must capture affirmative consent

!’ FTC Health Breach Notification Rule (16 CFR Part 318, 2024 update) — 30-day notification clock applies to non-HIPAA-covered entity apps that handle personal-health-record information

!’ FTC enforcement against mental-health apps — FTC has aggressively enforced HBNR against non-covered apps (BetterHelp $7.8M, GoodRx $1.5M, Flo Health $2023); TX BH apps outside HIPAA face FTC HBNR exposure

!’ Dual-track TX BH app disclosure calendar — TX HB300 60-day AG clock + FTC HBNR 30-day clock + HIPAA 60-day OCR clock (if applicable) all running in parallel

!’ TX HB300 training/audit obligations — covered entities must train workforce on PHI handling; audit trail requirements on PHI access; BH MSOs whose BAA flow-down lacks HB300 training are exposed

!’ HHSC reportable event for licensed BH facility — TX Health & Human Services Commission requires incident reports; HHSC-aligned notice to patients required; CY 2024 HHSC enforcement actions on BH breaches

!’ TDPSA small-business exemption — does NOT apply to BH MSOs handling SUD/psychiatric data; the sensitive-data carve-out removes the small-business exemption for BH under TDPSA

!’ Cyber-insurance underwriting now requires TX HB300 + TDPSA posture — carriers demand documented 60-day AG-notice runbook, 30-day individual-notice runbook, and FTC HBNR-only-state app inventory

SECTION 5 | NAMED TX BH INCIDENTS — INCIDENT ANATOMY

Behavioral Health Group + Deer Oaks + Acuity Brands BH Slice

01 Behavioral Health Group TX (ransomware-mediated SUD record exposure) — 2024

Largest TX MAT (medication-assisted treatment) provider. 2024 ransomware event mediated SUD record exposure including Part 2-protected records. Dual-track disclosure: 42 CFR Part 2 SAMHSA pathway + HIPAA 60-day OCR clock + TX HB300 60-day AG clock + TX HB300 30-day notice-to-individuals. HHSC reportable event. Cyber-insurance carrier coverage litigation pending.

02 Deer Oaks Behavioral Health TX APC (ransomware / BH + ALF records) — 2024

$225,000 ransom disclosed (industry reporting). BH patient records + ALF resident records exfiltrated; BH Patients include SUD treatment arm — Part 2 dual-track disclosure triggered. Cyber-liability insurance coverage accepted with retention. HHSC reportable event.

03 Acuity Brands BH workforce slice (LockBit 3.0 affiliate) — Feb 2024

Acuity Brands exposed 2.5M+ records to LockBit 3.0 affiliate in Feb 2024. The BH-affiliated workforce slice carried psychiatric/SUD disclosure history; HHS OCR enforcement pending. Acuity represents the broader corporate-cyber-exposure pattern that touches BH EAP populations.

Discovery !' clock start:	TX HB300 60-day AG clock begins on date of discovery; Part 2 SAMHSA pathway begins immediate on identification of SUD record exposure
Dual-track disclosure:	Part 2 SAMHSA pathway + HIPAA 60-day OCR + TX HB300 60-day AG + 30-day individual notice all run in parallel when SUD records + PHI + TX residents
Cyber-liability:	BHG TX carriers excluding Part 2 carve-out; Deer Oaks coverage accepted with retention; underwriter now requires Part 2 disclosure history at underwriting
Regulatory penalty stack:	HHS OCR penalty ($100–$50,000/violation, $1.5M annual cap per identical violation), TX HB300 civil penalty (up to $7,500/violation), 42 USC §290dd-2 federal criminal (felony for pattern), TDPSA enforcement

SECTION 6 | CORERECON WEDGE — 30-MIN SLA, SDVOSB, TX-RESIDENCY

Why BH MSOs Choose CoreRecon Over Generic MSSPs

CoreRecon's contractual 30-minute IR SLA measures against attacker speed (ransomware kill chain completes in 45–90 minutes per CrowdStrike 2024 Global Threat Report) — not the MSSP industry median 1–4 hour containment (SANS 2024 IR Survey). SDVOSB-certified (CVE-verified) — unlocks TX DIR cooperative contracting (TIPS, BuyBoard, TXMAS) for TX BH agencies and TX MSO procurement. TX data residency: SOC stationed in Corpus Christi, TX; no offshore tier-1. 24/7 SOC + BH-EHR-aware EDR — Credible, Kipu, myEvolv, Netsmart telemetry; behavioral twin-engine EDR over legacy AV; standalone CISA-aligned IR retainer; BH-EHR vendor pivot-aware incident playbook (BHG, Deer Oaks, Green Ridge TX incident patterns reverse-engineered into runbook).

30-MIN IR SLA PROOF

Contractual 30-minute detection-to-engagement SLA. Industry median: 1–4 hours (SANS 2024 IR Survey). BH MSOs operating under Part 2 SAMHSA pathway need faster engagement than MSSP industry average. CrowdStrike 2024 Global Threat Report: ransomware kill chain completes in 45–90 minutes.

SDVOSB SET-ASIDE

Service-Disabled Veteran-Owned Small Business (CVE-verified). Unlocks TX DIR cooperative contracting (TIPS, BuyBoard, TXMAS) for TX BH agencies and TX MSO procurement. SDVOSB set-aside is a procurement-side differentiator no generic MSSP can offer.

TX DATA RESIDENCY

Corpus Christi, TX SOC headquarters. No offshore tier-1. BH patient records and SUD treatment data never leave the US / never reach a non-US analyst terminal. BH-EHR vendor compliance posture includes US-only data flow.

24/7 SOC + BH-EHR EDR

Credible, Kipu, myEvolv, Netsmart telemetry feeds custom EDR detections. BH-EHR admin console credential-health monitoring. Patient-portal login anomaly baseline. Telehealth recording-bucket monitoring.

BEHAVIORAL TWIN-ENGINE EDR

Behavioral analysis-driven EDR layered over legacy signature AV. Two independent detection engines produce independent incident timelines — BH MSOs see fewer false-positive pages and faster BH-EHR-specific detection.

STANDALONE CISA-ALIGNED IR RETAINER

CISA-aligned incident-response retainer — no dependency on hourly-billed incident response. Pre-staged disclosure-decision matrix; pre-staged Part 2 SAMHSA pathway activation.

BH-EHR VENDOR PIVOT-AWARE PLAYBOOK

BH Group, Deer Oaks TX, Green Ridge TX, Acuity Brands BH slice, Lifepoint BH footprint, Ardent TX, CHS Fortra — incident pattern reverse-engineered into the runbook. BH-EHR vendor pivot path documented.

SECTION 7 + 8 | ENGAGEMENT ANCHORS + 30-DAY ACTIVATION ROADMAP

Sentinel $89 • Fortress $109–$129 • Command $2,500+

SENTINEL — $89/endpoint/month

Best for: TX solo BH practitioners, single-clinic outpatient, small IOP/PHP (10–40 endpoints)

- 24/7 SOC monitoring — TX-resident analysts
- BH-EHR-aware EDR on Credible/Kipu/myEvolv/Netsmart operator workstations
- Patient-portal MFA enforcement + clinician-portal MFA baseline
- Telehealth recording-bucket monitoring
- BH-EHR admin credential-health monitoring
- Monthly vulnerability summary report

FORTRESS — $109–$129/endpoint/month

Best for: Mid-market TX BH clinics, MSO roll-ups, multi-county psychiatry practices (40–120 endpoints)

- Everything in Sentinel, plus:
- 42 CFR Part 2 consent-managed disclosure language library

- TX HB300 60-day AG notification runbook pre-staged
- TDPSA §541.062 sensitive-data inventory + opt-in consent capture
- FTC HBNR 30-day notification runbook (non-covered apps)
- Quarterly vCISO report to executive leadership
- Tabletop: Part 2 SAMHSA + HB300 dual-track rehearsal

COMMAND — $2,500+ flat monthly retainer

Best for: Large TX BH MSO networks, multi-state roll-ups, M&A-active BH platforms (120–250+ endpoints)

- Everything in Fortress, plus:
- BH-EHR M&A cyber-due-diligence binder authorship (Part 2 + HIPAA + HB300 + TDPSA)
- Hosted BH-EHR vendor SOC 2 / HITRUST renewal tracking
- Direct 30-min IR engagement line — no queue
- CISA-aligned IR retainer pre-staged
- BH-EHR vendor pivot-aware incident playbook
- Cyber-insurance underwriting posture binder

Book Free Posture Assessment !’

https://corerecon.polsia.app/assessment?industry=Behavioral+Health | (800) 955-2596

Sources: HHS OCR enforcement actions (Lifepoint, Ardent TX, CHS Fortra GoAnywhere Feb 2023); 42 CFR Part 2 (SAMHSA Confidentiality of Substance Use Disorder Patient Records; 2024 Part 2/HIPAA single-consent alignment final rule, HHS Feb 2024); 42 USC §290dd-2 federal criminal liability; SAMHSA NIMDAT integration guidance; HIPAA Security Rule 45 CFR §164.308/§164.312; HIPAA Breach Notification Rule 45 CFR §164.408; Texas Health & Safety Code Ch. 181 (TX HB300, 60-day AG notification clock); Texas Business & Commerce Code §541 (TDPSA, sensitive-data enumeration under §541.062); FTC Health Breach Notification Rule (16 CFR Part 318, 2024 update); FTC enforcement actions against mental-health apps (BetterHelp, GoodRx, Flo Health); Texas Civil Practice & Remedies Code Ch. 573–577 (court-ordered mental-health disclosure exceptions); TX HSC Ch. 611 mental-health records; HHSC reportable events for licensed BH facilities; Acuity Brands LockBit 3.0 affiliate (Feb 2024, 2.5M+ records); Lifepoint Health ALPHV/BlackCat (Oct 2023); Ardent Health Services TX (Nov 2023, 30+ hospitals offline); Community Health Systems Fortra GoAnywhere (Feb 2023, CVE-2023-0669, 1M+ records); Behavioral Health Group TX (2024 ransomware-mediated SUD record exposure); Deer Oaks Behavioral Health TX APC ($225K ransom, BH/ALF records exfiltrated, HHSC reportable); Green Ridge Behavioral Health TX (roll-up M&A 2025); Credible, Kipu EMR, Netsmart myEvolv vendor security advisories (2024 credential-stuffing advisories); CrowdStrike 2024 Global Threat Report (45–90 minute ransomware kill chain); SANS 2024 Incident Response Survey (industry median 1–4 hour containment); TX Medicaid TAC §354.1432 telehealth session recording; SDVOSB CVE-verified set-aside; TX DIR cooperative contracting (TIPS, BuyBoard, TXMAS).