Texas Behavioral Health Cybersecurity

Patient Data | Ransomware | Compliance

A concise operating brief for Texas behavioral-health and mental-health clinics, IOP/PHP programs, psychiatry practices, MAT providers, and BH-MSO networks.

---

01 Patient-data exposure across BH-EHR, portal, telehealth, and shared administration

02 Ransomware readiness from identity compromise through recovery

03 42 CFR Part 2, HIPAA, Texas, TDPSA, and FTC practical concerns

04 30/60/90-day actions and managed-service fit

Informational security and compliance guidance; not legal advice. Verify current requirements with qualified counsel and regulators.

SECTION 1 | PATIENT-DATA EXPOSURE

The BH-EHR Is the Perimeter

Sensitive records are exposed through identity, workflow, vendor, and physical-data paths—not only through a server breach.

Texas behavioral-health organizations combine psychiatric records, SUD treatment history, safety assessments, consent artifacts, and telehealth material. A single administrator credential can open a clinic network, its consent-management workflow, and downstream reporting tools.

-> BH-EHR administrators in Credible, Kipu, Netsmart myEvolv, and similar platforms need privileged-access controls, phishing-resistant MFA, session review, and prompt offboarding.

-> MSO SSO reuse creates a cross-clinic blast radius. Review impossible travel, county-to-county reuse, dormant accounts, service accounts, and emergency access.

-> Patient portals and clinician workflows can bypass MFA or create incomplete audit trails. Test enrollment, recovery, delegated access, and break-glass paths.

-> Telehealth recordings, intake scans, exports, and local downloads are PHI repositories. Inventory buckets, shares, retention, encryption, and disposal vendors.

-> Hosted BH-EHR and billing vendors concentrate risk. Confirm BAA coverage, access logging, incident notice terms, backup ownership, and evidence delivery.

EXPOSURE TEST | Can the security lead produce, in one hour, every BH-EHR administrator, privileged vendor, recording repository, consent log, and export location?

SECTION 2 | RANSOMWARE READINESS

Interrupt the Kill Chain Before Encryption

Readiness is a sequence of tested controls, owners, and decisions—not a policy document stored in the same tenant.

Behavioral Health Group TX, Deer Oaks TX APC, Lifepoint, Ardent, and Community Health Systems incidents show why patient-care continuity and data-disclosure planning must run together.

-> Identity: require MFA for workforce, vendors, VPN, email, EHR, and backup administration; remove standing privilege and rotate exposed credentials.

-> Detect: deploy EDR on EHR operator workstations and servers; alert on mass archive creation, unusual exports, consent-log changes, portal anomalies, and encryption behavior.

-> Contain: keep an isolation playbook for EHR, identity, telehealth, and backup systems; define clinical downtime procedures before the next outage.

-> Recover: maintain immutable, offline-capable backups; test restore of scheduling, medication, clinical notes, consent records, and communications—not just a file share.

-> Decide: assign incident commander, clinical continuity lead, privacy/compliance lead, counsel, insurer, and communications owner.

-> TABLETOP TEST: begin with a compromised BH-EHR administrator account and end with a verified clinical restore, evidence hold, and notification decision matrix.

SECTION 3 | PRACTICAL COMPLIANCE CROSSWALK

Several Review Tracks Can Run Together

The correct response depends on the organization, data, vendor role, and facts of the incident. The frameworks below are not interchangeable.

HIPAA Security / Breach	Risk analysis, access control, audit controls, integrity, transmission security.	45 CFR §§164.308, 164.312, and 164.408.
42 CFR Part 2	SUD records, written consent, re-disclosure limits, and separate incident-language review.	SAMHSA / Part 2 review; 42 USC §290dd-2.
TX HB 300 / HSC Ch. 181	Texas health-data safeguards and breach response for covered organizations.	Review AG and individual-notice clocks.
TX HSC Ch. 611	Mental-health record custody, consent, and disclosure controls.	Separate state-law review with counsel.
TDPSA §541.062	Sensitive health and mental-health data inventory and consent.	Confirm applicability, exemptions, and duties.
FTC HBNR	Non-HIPAA health apps and similar health-data vendors.	16 CFR Part 318; 30-day clock where applicable.

NON-LEGAL-ADVICE CAVEAT | This crosswalk is an operational starting point, not legal advice. Rules, deadlines, exemptions, consent requirements, and regulator interpretations change; involve qualified privacy counsel before sending a notice or disclosing Part 2 or Texas mental-health records.

SECTION 4 | TEXAS BH INCIDENT LESSONS

Use Incidents to Test the Controls

Named incidents are useful control tests; they are not predictions and should not replace fact-specific investigation.

01 **Behavioral Health Group TX**

Ransomware-mediated SUD record exposure illustrates why Part 2 review and HIPAA/Texas response tracks must be planned together.

02 **Deer Oaks Behavioral Health TX APC**

The reported $225K ransom and BH/ALF record exposure illustrate the combined clinical-continuity, insurance, and disclosure problem.

03 **Acuity Brands / LockBit**

The 2.5M+ record incident illustrates how broader enterprise exposure can touch behavioral-health populations and create downstream review.

04 **Lifepoint, Ardent, CHS**

Service disruption, third-party access, and large-scale exfiltration patterns show why vendor access, downtime, and recovery exercises belong together.

A practical incident file should preserve identity and EHR logs, export history, consent records, backup evidence, vendor notifications, insurance correspondence, and the exact language considered for every recipient. Treat “we have a BAA” as a starting fact, not a completed response.

SECTION 5 | 30 / 60 / 90-DAY ACTIONS

Turn the Brief into a Measurable Program

Sequence the work so the first month reduces exposure, the second validates resilience, and the third proves readiness.

DAYS 0–30 | MAP AND CONTAIN

Inventory BH-EHR, identity, portal, telehealth, consent, backup, and vendor access. Require MFA for privileged and remote access; remove stale administrators; confirm backup immutability and incident contacts.

DAYS 31–60 | TEST AND HARDEN

Check EDR and logging coverage. Review exports, recording buckets, portal recovery, break-glass access, and physical intake disposal. Tabletop a compromised admin account, exfiltration, encryption, restore, and Part 2 language review.

DAYS 61–90 | PROVE AND GOVERN

Perform a clinical and administrative restore test. Close high-risk findings with owners and evidence. Review BAAs, Part 2 flow-down, incident notice terms, cyber-insurance requirements, and M&A diligence.

ONGOING GOVERNANCE

Report control health to leadership quarterly and repeat the tabletop after material change, acquisition, EHR change, or major vendor change.

SECTION 6 | MANAGED-SERVICE FIT

Choose the Operating Layer You Need

The right managed-service layer should close a named gap: identity visibility, EDR coverage, clinical recovery, response, diligence, or accountability.

SENTINEL | $89 / endpoint / month

Best for: Single clinic, solo practitioner, or small IOP/PHP program.

24/7 SOC monitoring, BH-EHR-aware EDR, MFA baseline, vulnerability summary, and patient-portal / telehealth monitoring.

FORTRESS | $109–$129 / endpoint / month

Best for: Mid-market clinic group or multi-county psychiatry practice.

Sentinel plus consent-aware Part 2 and Texas notification runbooks, sensitive-data inventory, quarterly vCISO reporting, and tabletop support.

COMMAND | $2,500+ / month

Best for: Large BH-MSO, multi-state roll-up, or M&A-active platform.

Fortress plus 30-minute IR engagement, CISA-aligned retainer, BH-EHR vendor and acquisition diligence, insurance posture, and executive response support.

Managed cybersecurity services: https://corerecon.polsia.app/verticals/tx-behavioral-health-mental-health-clinics

Related behavioral-health threat analysis: https://corerecon.polsia.app/blog/texas-behavioral-health-cyber-threats-2026

SECTION 7 + 8 | CTA + SOURCES

Make the Next Review Specific

Use the assessment to turn the three brief themes into a prioritized control conversation.

BOOK A FREE BEHAVIORAL-HEALTH POSTURE ASSESSMENT

https://corerecon.polsia.app/assessment/?industry=Behavioral%20Health

PLAIN-TEXT LINKS

https://corerecon.polsia.app/verticals/tx-behavioral-health-mental-health-clinics

https://corerecon.polsia.app/assessment/?industry=Behavioral%20Health

https://corerecon.polsia.app/blog/texas-behavioral-health-cyber-threats-2026

https://corerecon.polsia.app/verticals/tx-behavioral-health-mental-health-clinics/threat-brief

Sources: HHS OCR and breach-notification materials; SAMHSA Confidentiality of Substance Use Disorder Patient Records / 42 CFR Part 2; HIPAA 45 CFR §§164.308, 164.312, and 164.408; Texas Health & Safety Code Chapters 181 and 611; Texas Business & Commerce Code Chapter 541 / TDPSA §541.062; FTC Health Breach Notification Rule, 16 CFR Part 318; HHSC reportable-event guidance; CISA healthcare and ransomware guidance; CrowdStrike 2024 Global Threat Report; SANS 2024 Incident Response Survey; repository-maintained Texas BH incident notes for Behavioral Health Group TX, Deer Oaks TX APC, Acuity Brands, Lifepoint, Ardent, and Community Health Systems.

Informational only; not legal advice. Confirm current law, agency guidance, facts, and applicability with qualified counsel and the relevant regulator.