Texas Healthcare & Medical Practices: Under Siege.

2026 Cybersecurity Reality for TX Medical Practices & Hospitals

192.7M	Change Healthcare breach (Feb 2024) — largest healthcare data exposure in U.S. history
$9.5M	Scripps Health OCR settlement (Dec 2024) — HIPAA Risk Analysis failure precedent
$408	Per-record healthcare breach cost — highest of any sector (IBM 2025)
12 Steps	Action checklist for TX medical practice security posture

SECTION 1 | EXECUTIVE SUMMARY

Healthcare Is Now the Highest-Cost Breach Sector

192.7M records in one breach. $408/record cost. OCR settlements climbing. 30-min IR SLA is not optional in healthcare.

!’ 192.7M individuals affected by Change Healthcare ransomware (ALPHV/BlackCat, Feb 2024) — largest healthcare breach in U.S. history

!’ $9.5M Scripps Health OCR settlement (Dec 2024) — first OCR penalty specifically citing failure to conduct an accurate HIPAA Risk Analysis

!’ $408 average per-record healthcare breach cost — highest of any sector for 14 consecutive years (IBM Cost of a Data Breach 2025)

!’ Ascension Health ransomware (May 2024, Black Basta) — 5.9M patient records; clinical operations disrupted across 140+ hospitals

!’ Texas Health Resources + HCA Healthcare 11M+ records exposed via vendor breaches (2024–2025)

!’ McLaren Health Care 2.1M records (2024) — 5th major breach in 5 years; class-action overlay

!’ OCR breach portal reports 350+ healthcare breaches of 500+ records each in 2025 — averaging nearly 1/day

SECTION 2 | ATTACK VECTORS

Four Attack Patterns Hitting TX Healthcare

01 Ransomware — Exfil First, Then Encrypt

ALPHV/BlackCat (Change Healthcare 192.7M), Black Basta (Ascension Health), Daixin Team, and LockBit all target healthcare with double-extortion. PHI is exfiltrated before encryption — then posted to leak sites. Average healthcare dwell time before detection: 79 days (IBM 2025).

02 Business Email Compromise — Patient Billing Fraud

BEC against clinics and hospitals is underreported. W-2 phishing for staff data, vendor invoice redirection, and patient refund fraud all weaponize compromised inboxes. Impersonation of revenue cycle vendors (Availity, Change Healthcare clearinghouse workflows) is the new variant.

03 Third-Party EHR & Clearinghouse Vendor Breaches

Epic, Cerner/Oracle Health, athenaOne, MEDITECH, and NextGen are high-value targets. A single Epic Hyperdrive or athenaOne credential compromise exposes every connected provider. Change Healthcare clearinghouse attack cascaded to 70% of U.S. medical claims flow.

04 IoMT — Infusion Pumps, OmniCell, Imaging Devices

Internet of Medical Things (IoMT) has poor patch discipline and rarely-segmented networks. OmniCell, Baxter Spectrum IQ infusion pumps, CareFusion ventilators, and imaging modalities (CT, MRI) are persistent footholds. FDA Section 524B (Patches for Medical Devices) tightens this.

SECTION 3 | REGULATORY EXPOSURE

HIPAA Risk Analysis Is the Recurring OCR Finding

HIPAA Security Rule (§164.308/310/312)

Administrative, physical, and technical safeguards. Annual Security Risk Assessment (SRA) is the bedrock — and the most-cited deficiency in OCR enforcement. Scripps ($9.5M), Wellenstein ($3.9M), and most OCR Resolution Agreements begin with "incomplete SRA."

HITECH Breach Notification (60-Day Rule)

Breach affecting 500+ individuals requires media notice + HHS Secretary notice within 60 days. Failure to notify triggers separate penalties. Texas AG parallel notification encouraged for breaches of Texas-resident PHI.

TX HB 300 (Encrypted PHI on Portable Devices)

Texas-specific requirement for encryption of PHI on laptops, phones, USB drives, and removable media. Failure is a state-law violation on top of HIPAA. Texas AG (Paxton) actively enforces — separate cause of action.

TX HCS Ch. 181 (TX Medical Records Confidentiality)

Stricter than HIPAA on consent for certain disclosures. Applies to electronic health records and any disclosure beyond treatment/payment/operations. Class-A misdemeanor for violations; civil damages.

TDPSA + CMS CoP + 42 CFR Part 2

TDPSA covers consumer health data outside HIPAA scope. CMS Conditions of Participation for hospitals require safeguards. 42 CFR Part 2 governs behavioral health and substance abuse records — separate consent regime.

KEY PRECEDENT — SCRIPPS HEALTH

OCR fined Scripps Health $9.5M (Dec 2024) for failure to maintain an accurate, thorough HIPAA Risk Analysis. The 2021 ransomware attack exfiltrated 147,000+ patient records. The size of the breach did not matter — the absence of a documented, enterprise-wide SRA did.

SECTION 4 | COST OF A BREACH

When Ransomware Hits a TX Medical Practice

OCR Civil Penalty

$9.5M

Scripps Health (2024) — failure to conduct accurate HIPAA Risk Analysis

OCR Civil Penalty

$1.5M

Banner Health — 2016/2020 (early precedent; 2025 OCR fine ranges $5K–$1.9M annually/ standard)

Class Action Settlement

$65M

Universal Health Services (2024) — 2020 ransomware, 4.5M individuals affected

Class Action Settlement

$5.5M

McLaren Health Care — 2.1M records, Black Cat ransomware

Operational Downtime

$1.96M/day

Healthcare highest downtime cost per IBM 2025; 5–14 day outages not uncommon

Change Healthcare Cascade

Nationwide

70% of U.S. medical claims flow halted for 3+ weeks; patient billing and pharmacy operations nationwide

SECTION 5 | WHY TRADITIONAL IT FAILS

The Gap That Kills: No 24/7 Monitoring on EHR

Most small and mid-size Texas medical practices rely on daytime IT support — a managed services provider (MSP) that handles helpdesk, network maintenance, and EHR patching. This model works perfectly for keeping the lights on. It is catastrophically inadequate for security operations — and the EHR cannot be taken offline.

THE HEALTHCARE DWELL TIME PROBLEM

79 days

= average time between initial access and detection in healthcare (IBM 2025)

A practice that relies on its daytime IT provider detects breaches at step 4 of the ransomware playbook — when the ransom note appears. By then, exfiltration of PHI has been ongoing for months and a SIXTY-DAY notification clock is already running. The patient trust impact is asymmetric to the technical reality: one OCR investigation costs more than a decade of monitoring.

Daytime-only coverage

No detection between 6pm Friday and 9am Monday — exactly when ransomware detonates

No behavioral analytics on EHR logs

EHR audit logs are generated but never reviewed. Failed login bursts, role-elevation events, and bulk PHI exports are invisible

Flat network assumption

IoMT devices, EHR servers, billing, and guest Wi-Fi share one VLAN. Lateral movement is trivial

No OCR notification playbook

HITECH 60-day clock starts without a template, a media list, or an HHS portal workflow

No PHI-specific ransomware IR

MSP ransomware playbooks treat data as generic. PHI requires HIPAA breach analysis + state-AG workflow

SECTION 6 | CORERECON APPROACH

30-Minute IR SLA. HIPAA-Native. SDVOSB.

SENTINEL — $89/endpoint/month

Best for: Solo/small practices (1–10 providers)

- 24/7 SOC monitoring + SIEM correlation
- Email security with BEC impersonation defense
- MFA deployment on EHR and practice management SaaS
- Security awareness training + HIPAA Security Officer attestation
- Monthly TX healthcare sector threat digest
- Annual HIPAA Security Risk Assessment (SRA) baseline

FORTRESS — $109/endpoint/month

Best for: Mid-size practices, multi-location, specialty

- Everything in Sentinel

' EDR deployment with behavioral + exfil detection on PHI-bearing endpoints

' EHR/SIEM log forwarding (Epic/Cerner/athenaOne/NextGen/MEDITECH)

' PHI-aware immutable offsite backup + monthly restore test

' TX HB 300 + HITECH 60-day notification playbook

' OCR / HHS breach portal pre-engagement

COMMAND — $129/endpoint/month

Best for: Hospitals, large practices, MSOs

' Everything in Fortress

' IoMT segmentation + medical device risk register

' Vendor risk assessment (Epic Hyperdrive, Athena, clearinghouse BAA review)

' PHI tabletop with executive and compliance officer participation

' Continuous SRA monitoring (CCSR-style)

' OCR enforcement response support + outside counsel coordination

SECTION 7 | 12-STEP ACTION CHECKLIST

12 Steps Every TX Medical Practice Should Take Now

01

02

03

04

05

06

07

08

09

10

11

12

YOUR NEXT MOVE

Book Free Assessment !’

https://corerecon.polsia.app/assessment | (800) 955-2596

' SDVOSB Certified | ' 30-Min IR SLA | ' TX SOC — Corpus Christi | ' AT&T TX State Vendor

Sources: OCR Resolution Agreement — Scripps Health ($9.5M, Dec 2024); Change Healthcare ransomware (ALPHV/BlackCat, Feb 2024, 192.7M records); Ascension Health ransomware (Black Basta, May 2024); HHS HPH Sector Threat Brief (2024–2025); IBM Cost of a Data Breach 2025 ($408/healthcare record); HIPAA Journal annual breach report; 42 USC §164.308/310/312; Texas Health & Safety Code Ch. 181; Texas HB 300.