CORERECON THREAT INTELLIGENCE | VETERINARY HEALTHCARE | JULY 2026

Texas Veterinary Hospitals:

Patient Data, Controlled Substances, PMS Compromise.

2026 Cybersecurity Reality for Texas Veterinary Hospitals & Emergency Practices

---

1.1M+ NVA pet owner records exposed (Feb 2024, LockBit affiliate)

18–24mo Exfiltration-to-fraud window for stolen pet-owner PII

3+ Active ransomware groups (BlackCat / LockBit / Rhysida)

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

SECTION 1 | EXECUTIVE SUMMARY

AVImark, Hippo Manager, and the Dispensary Drawer

NVA 1.1M+ supply-chain breach (LockBit affiliate, 2024). Southern Veterinary Partners confirmed. AVImark/Hippo Manager credential campaigns. 207-day median dwell. TVMDL premise-ID submission exposure when vet EMR encrypted.

!’ NVA (National Veterinary Associates, Feb 2024): 1.1M+ pet owner records exfiltrated via LockBit 3.0 affiliate — hundreds of TX-affiliated hospitals compromised through cloud AVImark/Cornerstone PIMS vendor

!’ Southern Veterinary Partners (SVP, 2024): 70+ hospital DSO confirmed — parent-company compromise; AVImark IDEXX credential exposure implicated

!’ Median dwell time for veterinary & healthcare sector: 207 days (IBM X-Force Threat Intelligence Index 2024) — credential theft !’ lateral movement !’ dispensary-event exfiltration timeline

!’ AVImark IDEXX & Hippo Manager credential compromise campaigns (2024–2025) — branches harvested via phishing + dark-web vet-PII markets

!’ DEA Title 21 CFR §1304.04 inventories + §1305.06 CSOS electronic-records binding for every Schedule II–V dispense event — recordkeeping authorship gaps are the auditor pathway

!’ TX Veterinary Medical Examiners 22 TAC §575 records — every dispensing DVM subject to Board documentation expectations

!’ TVMDL premise-ID submission workflow (CWD / EIA / brucellosis / rabies) — when the vet EMR is encrypted, premise-ID traceability breaks at submission time

!’ TX HB 300 (Texas HSC Ch. 181) sweeps in pet-owner health data as covered protected health information — 60-day breach notification applies alongside HIPAA Security Rule where Medicaid-billing / service-animal practices operate

SECTION 2 | TX VET-HOSPITAL THREAT LANDSCAPE 2024–2026

Four TX-Anchored Veterinary Hospital Breaches

01 NVA (National Veterinary Associates) — Feb 2024

LockBit 3.0 affiliate compromised NVA's cloud AVImark / Cornerstone PIMS environment through contracted vendor. 1.1M+ pet owner records exfiltrated — names, addresses, payment cards, clinical history, prescription records. Hundreds of TX-affiliated veterinary hospitals impacted. HHS OCR + multi-state AG notification.

02 Southern Veterinary Partners (SVP) — May 2024

Multi-state DSO with 70+ animal hospitals — significant TX footprint. Confirmed breach via parent-company compromise; AVImark IDEXX credential exposure implicated. Pet-owner PII exfiltrated. TX AG breach notification followed.

03 VCA / BluePearl / Banfield TX — 2024–2025

Mars Petcare subsidiaries (VCA, BluePearl) and Banfield Pet Hospital TX locations surfaced in PIMS credential exposure investigations. Integrator-cloud supply chain remains the common attack thread; high pet-owner PII volume amplifies blast radius.

04 AVImark IDEXX credential compromise campaign — 2024–2025

Multiple regional AVImark-hosted veterinary hospitals compromised via stale third-party AVImark-integrated vendor credentials. Client pet-owner PII + payment card data exfiltrated before encryption. TX state notification reached.

SECTION 3 | REGULATORY / COMPLIANCE STACK

Five Frameworks That Bind Vet Hospitals

Veterinary hospitals operate inside a multi-track regulatory environment that does not map cleanly onto CPA firms or dental practices. PHI scope turns on whether the practice bills Medicaid or handles service-animal records. DEA scope turns on whether the practice dispenses Schedule II–V. TVMDL premise-ID scope turns on whether the practice submits specimens. TX HB 300 sweeps in protected health data even where HIPAA does not. TDPSA enumerates sensitive pet-owner PII.

HIPAA Security Rule (where in-scope)

45 CFR §164.308 (administrative safeguards) + §164.312 (technical safeguards). Applies where a vet practice bills Medicaid, handles service-animal records, or contracts with covered entities for clinical research. Risk analysis, access controls, audit logging, MFA, encryption, IR plan.

DEA 21 CFR §1304.04 + §1305.06 + CSOS

§1304.04 inventories + §1305.06 electronic records for every Schedule II–V dispense. CSOS two-factor verification for e-prescribe. Recordkeeping authorship must survive a ransomware event — backup immutable, MSB-compliant, audit-ready.

TVMDL premise-ID submission rules

Texas Veterinary Medical Diagnostic Laboratory premise-ID traceability for CWD / EIA / brucellosis / rabies submissions. When the vet EMR is encrypted, premise-ID submission workflow must continue from immutable backup; otherwise regulatory exposure accrues during the incident.

TX HB 300 (Texas HSC Ch. 181) + AVMA Ethics

TX HB 300 sweeps pet-owner health data into covered protected health information — 60-day breach notification. AVMA Principles of Veterinary Medical Ethics confidentiality baseline binds client-consent workflow design.

TX Vet Board 22 TAC §575 + TDPSA §541.062

22 TAC §575 licensing & documentation expectations for dispensing DVMs. TDPSA §541.062 enumerates sensitive pet-owner data — name + payment card + prescription tied together is sensitive data by definition. Civil penalty up to $7,500/violation.

SECTION 4 | TOP 5 ATTACK VECTORS

The Five Patterns TX Vet Hospitals Face in 2026

01 BEC Targeting Dispensing DVMs

Phishing impersonates pet-owner invoice, lab result, or reference-lab callback. DVMs with CSOS e-prescribe authority authorize controlled-substance dispense lines under pressure. Average vet BEC loss trail CPA firms in dollar size but the regulatory exposure is larger — DEA Diversion Investigators refer the dispensary-drawer event.

02 AVImark / Hippo Manager PMS Credential Theft

Vet-tech turnover is the highest in clinical settings. Phishing + reused passwords + token theft harvest AVImark cloud SSO, Hippo Manager ezyVet admin, and Cornerstone IDEXX console credentials. One compromised tech workstation = full client base readable.

03 DEA Controlled-Substance Diversion via Credential Theft

Vet staff with CSOS access — DVMs, registered techs, office managers — become the diversion pathway. Exfiltrated dispensary logs become feedstock for black-market veterinary opioid diversion, illegal online pet pharmacies, and DEA Diversion Investigator referrals.

04 IoT Medical Device Exposure

Idexx lab analyzers, ultrasound, anesthetic monitors, and digital dental X-ray are flat on the L2 network alongside AVImark and payment terminals. Vendor-default credentials and unpatched firmware are open reconnaissance footholds — often the entry point not the AVImark cloud itself.

05 Pet-Owner HR-Data Portal Risk (Third-Party SSO)

Cornerstone, VetData, PetDesk, ezyVet SSO portals consolidate pet-owner HR data into one breach. Compromise of any single portal exposes payment cards + insurance billing tied to hundreds of pets at once. The third-party SSO pathway is the modern supply-chain attack surface.

SECTION 5 | CORERECON TIER MAPPING

Sentinel / Fortress / Command for Vet Hospitals (10–100 endpoints)

SENTINEL — $89/endpoint/month

Best for: Small 1-DVM practices (1 location, 10–25 endpoints)

- 24/7 SOC monitoring — TX-resident analysts
- Endpoint detection & response (EDR) on vet workstations
- AVImark cloud SSO enrollment + Hippo Manager credential health
- Monthly vulnerability summary report
- Dispensary-drawer access logging baseline

FORTRESS — $109–$129/endpoint/month

Best for: Multi-DVM / emergency vet hospitals (1–3 locations, 25–75 endpoints)

- Everything in Sentinel, plus:

- PIMS-aware EDR (AVImark / Hippo Manager / Cornerstone / ImproMed)
- DEA §1304.04 recordkeeping authorship + CSOS 2FA enforcement
- TVMDL premise-ID submission workflow gap assessment
- Quarterly vCISO report to practice leadership
- 24-hour emergency hospital topology coverage

COMMAND — $2,500+/mo flat retainer

Best for: DSO / specialty hospitals (3–12+ locations, 75–250+ endpoints)

- Everything in Fortress, plus:
- Dedicated vCISO (contracted as security officer)
- Full DEA §1304/§1305 recordkeeping binder + annual review
- TVMDL premise-ID continuity plan across incident response
- On-site incident response capability within 60 miles

' Direct line to 24/7 IR team — no queue

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

What to Do — and When

30 DAYS

- Reset AVImark admin credentials; rotate all cloud-PMS service-account credentials older than 90 days
- Enforce MFA on Hippo Manager, Cornerstone, ImproMed Infinity, ezyVet, PetDesk, VetData, and all PIMS vendor portals
- CSOS two-factor verification review on every dispensing DVM — print CSOS audit trail; confirm 2FA enrolled at the DEA CSOS site
- TVMDL submission workflow continuity test — practice the premise-ID submission from immutable backup so the workflow survives a vet EMR encryption event

60 DAYS

- PIMS-aware EDR deployed on every workstation running AVImark IDEXX, Cornerstone IDEXX, Hippo Manager ezyVet, or ImproMed Infinity
- IoT medical-device segmentation: Idexx lab analyzers, ultrasound, anesthetic monitors, digital dental X-ray moved off the L2 network with payment terminals
- DEA Form 222 file integrity review + §1304.04 inventory binding — backup tested against immutable retention requirement
- Phishing awareness training + incident simulation on the dispensing DVM cohort specifically — credential theft on CSOS access is the target vector

90 DAYS

- Quantified gap assessment against the 5-framework stack (HIPAA Security Rule §164.308/§164.312 + DEA §1304–§1305 + TVMDL + TX HB 300 + TDPSA §541.062); written binder delivered
- TVMDL premise-ID continuity plan formalized; rehearsal with TX VMDL diagnostic lab counterparts under simulated EMR-encryption incident
- Annual vulnerability assessment + IR tabletop with DEA Diversion Investigator simulation; results in writing
- Cyber insurance binder renewal with current AVImark credential posture, dispensary-drawer audit trail, and TVMDL submission continuity plan

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 veterinary PIMS topologies — AVImark IDEXX, Cornerstone IDEXX, Hippo Manager ezyVet, ImproMed Infinity. Corpus Christi, TX headquarters.

Why Veterinary Practices Choose CoreRecon

- AVImark / Cornerstone / Hippo Manager / ImproMed PIMS-aware EDR — not generic endpoint protection
- DEA Title 21 CFR §1304.04 recordkeeping authorship with dispensary-event monitoring
- TVMDL premise-ID continuity plan rehearsed across incident-response tabletop exercises
- TX HB 300 + HIPAA Security Rule (where in-scope) + TDPSA §541.062 stack assessment
- 24-hour emergency hospital topology coverage — overnight credential usage, weekend boarding batches
- DSO multi-location rollout — central PIMS administration included in aggregate coverage
- SDVOSB contracting for USDA APHIS / DoD-adjacent veterinary engagements

Book Free Assessment !’