CONFIDENTIAL — INTERNAL COMPLIANCE DOCUMENT

DATA SOVEREIGNTY & RESIDENCY POLICY

Texas Senate Bill 1188 Compliance Framework

The Texas Data Sovereignty Act

Effective Date:	February 8, 2026
Document Version:	1.0
Classification:	Internal — Compliance Use Only
Governing Statute:	Texas SB 1188 (88th Legislature, R.S.)
Companion Statute:	Texas HB 149 (AI Transparency)
Review Cycle:	Quarterly (Next Review: May 2026)
Prepared By:	KairoLogic Compliance Division

NOTICE: This document constitutes an internal compliance policy adopted pursuant to Texas Senate Bill 1188 (the Texas Data Sovereignty Act). It establishes binding operational requirements for all personnel, contractors, and digital service providers engaged by the Practice. Unauthorized distribution of this document is prohibited. This policy does not constitute legal advice and should be reviewed by qualified legal counsel.

TABLE OF CONTENTS

SECTION 1

PURPOSE & LEGISLATIVE AUTHORITY

The purpose of this policy is to establish strict, enforceable guidelines for the residency, processing, transmission, and storage of Protected Health Information (PHI) and Personal Identifying Information (PII) in accordance with **Texas Senate Bill 1188** (the "Texas Data Sovereignty Act"), as enacted by the 88th Texas Legislature, Regular Session.

This organization is committed to ensuring that all digital patient data remains exclusively within the continental United States at all times, across all systems, and through all processing stages. This commitment protects against foreign data exploitation, ensures compliance with state-mandated data residency requirements, and establishes documented "Reasonable Care" necessary for statutory Safe Harbor standing under SB 1188.

This policy further aligns with **House Bill 149** (AI Transparency) to ensure comprehensive compliance with Texas digital healthcare regulations enacted during the 88th Legislative Session.

SECTION 2

SCOPE OF APPLICABILITY

This policy applies to all individuals and entities that handle, access, store, process, or transmit data on behalf of the Practice, including but not limited to:

- All full-time, part-time, and temporary employees
- Independent contractors and consulting clinicians
- Third-party vendors, sub-processors, and digital service providers
- Virtual assistants (VAs), whether domestic or offshore
- Managed Service Providers (MSPs) and IT support organizations
- Cloud infrastructure providers (IaaS, PaaS, SaaS)
- AI, machine learning, and automated decision-making tool providers
- Website hosting, analytics, and marketing technology vendors

Jurisdictional Scope: This policy applies to all data originating from, processed within, or pertaining to patients located in the State of Texas, regardless of where the Practice's systems or personnel are physically located.

SECTION 3

DEFINITIONS

"Protected Health Information" (PHI)

Any individually identifiable health information as defined by HIPAA (45 CFR 160.103), including but not limited to patient names, diagnoses, treatment records, billing information, and biometric data.

"Personal Identifying Information" (PII)

Any data that could reasonably be used to identify an individual, including name, date of birth, Social Security Number, email address, IP address, device identifiers, and geolocation data.

"Data Residency"

The geographic location where digital data is physically stored, processed, cached, or transmitted, including transient processing and backup replication.

"Foreign Adversary Jurisdiction"

Any nation or territory designated by the U.S. government as a foreign adversary, including but not limited to: China (including Hong Kong), Russia, Iran, North Korea, Cuba, and the Maduro regime of Venezuela.

"Domestic Data Boundary"

The continental United States, including all 50 states, the District of Columbia, and U.S. territories where federal data protection laws apply.

"Sub-Processor"

Any third party engaged by a primary vendor to process, store, or transmit data on behalf of the Practice, including CDN providers, backup services, and AI model inference endpoints.

"Shadow IT"

Any software, application, cloud service, browser extension, or digital tool used by Practice personnel that has not been formally approved and verified for data sovereignty compliance.

"Certificate of Data Sovereignty"

A formal attestation from a vendor confirming the physical location of all servers, the legal jurisdiction of the corporate entity, and the absence of foreign sub-processor routing.

SECTION 4

DOMESTIC DATA RESIDENCY REQUIREMENTS

4.1 General Requirement

All digital systems utilized by the Practice must host and process data exclusively on servers and infrastructure located within the Domestic Data Boundary. This requirement applies at all stages of data lifecycle management, including:

- Collection and intake (website forms, patient portals, intake kiosks)

- Processing and computation (clinical decision support, billing, scheduling)
- Storage at rest (primary databases, backups, archives, disaster recovery)
- Transmission in transit (API calls, email routing, file transfers)
- Caching and edge processing (CDN nodes, edge computing, load balancers)
- Disposal and deletion (secure erasure, media destruction)

4.2 Covered Systems

The following system categories must demonstrate verified domestic data residency:

System Category	Examples	Residency Verification
Electronic Medical Records	Epic, Athenahealth, DrChrono, Kareo	Annual vendor attestation
Patient Portals	MyChart, FollowMyHealth, custom portals	Server IP geolocation audit
Practice Management	Dentrix, NextGen, AdvancedMD	Vendor data residency certificate
Website & Intake Forms	WordPress, Jotform, Typeform, custom	DNS + hosting verification
Communication Tools	Email servers, telehealth, patient SMS	MX record + routing analysis
AI & Automation	Chatbots, transcription, clinical AI	Model hosting + API endpoint audit
Billing & Revenue Cycle	Waystar, Availity, Change Healthcare	Processing location attestation
Imaging & Diagnostics	PACS, cloud radiology, pathology AI	Storage + processing verification
Backup & Disaster Recovery	Veeam, Datto, cloud backup services	Replication target audit

SECTION 5

PROHIBITED PRACTICES

The following activities constitute direct violations of this policy and of Texas SB 1188. Violation may result in disciplinary action, termination, and statutory penalties of up to **$250,000 per incident**:

5.1 Offshore Data Routing

The use of any digital tool, service, or platform that routes patient data through servers, proxies, processing centers, or relay nodes located outside the continental United States is strictly prohibited. This includes "pass-through" routing where data transiently crosses foreign infrastructure, even if the final storage destination is domestic.

5.2 Foreign Cloud Storage

Storage of patient data on cloud instances, virtual machines, object storage buckets, or database replicas located in non-U.S. regions is a violation of this policy. This applies to all cloud providers including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and any other infrastructure-as-a-service provider. Cloud regions must be explicitly configured to U.S.-only zones.

5.3 Unverified AI & Machine Learning Tools

Staff may not input, upload, or otherwise expose patient data to any artificial intelligence system, large language model, machine learning tool, or automated transcription service that has not been forensically verified for domestic data residency. This prohibition specifically includes consumer-grade AI tools such as non-enterprise ChatGPT, Bard, Claude (non-enterprise), and any foreign-hosted transcription, translation, or diagnostic AI services.

5.4 Unauthorized Communication Channels

Patient data may not be transmitted via personal email accounts, consumer messaging applications (WhatsApp, Telegram, WeChat, Signal), social media direct messages, or any communication platform that has not been approved by the Practice for HIPAA-compliant, domestically-hosted communication.

5.5 Shadow IT

The installation, use, or configuration of any software, browser extension, mobile application, or cloud service that has not been formally approved by Practice IT administration and verified for data sovereignty compliance is prohibited. This includes free-tier SaaS products, trial software, and browser-based tools.

SECTION 6

VENDOR DUE DILIGENCE & CERTIFICATION

Before engaging any new digital vendor, service provider, or sub-processor, the Practice Manager or designated compliance officer must complete the following due diligence process:

6.1 Certificate of Data Sovereignty

Every vendor that processes, stores, or transmits patient data must provide a signed Certificate of Data Sovereignty confirming:

- The physical address and geographic coordinates of all primary and backup data centers
- The legal jurisdiction and country of incorporation of the parent company and all subsidiaries
- Written confirmation that no sub-processors, CDN nodes, or processing endpoints route data outside the United States
- The specific cloud regions and availability zones in use, with contractual guarantees against automatic failover to non-U.S. regions
- Data encryption standards in transit (TLS 1.2+) and at rest (AES-256 or equivalent)

6.2 Vendor Risk Classification

Risk Tier	Data Access Level	Verification Requirement	Review Cycle
Critical	Direct PHI access (EMR, billing, clinical AI)	Full forensic audit + Certificate	Quarterly
High	Indirect PHI access (email, analytics, CDN)	Certificate + IP geolocation check	Semi-annually
Moderate	PII only (scheduling, marketing, CRM)	Written attestation + contract review	Annually
Low	No patient data (office supplies, facilities)	Standard procurement process	As needed

SECTION 7

AI TRANSPARENCY DISCLOSURE (HB 149 ALIGNMENT)

In alignment with **House Bill 149** (AI Transparency in Healthcare), the Practice shall maintain the following disclosures and operational controls:

7.1 Public-Facing Disclosure

If AI, machine learning, or automated decision-making tools are used to interact with patients, process clinical data, triage inquiries, or generate treatment recommendations, the Practice must maintain a clearly visible public disclosure on its website and in patient-facing materials. This disclosure must explicitly state: (a) the purpose and scope of AI usage, (b) confirmation of domestic data residency compliance, and (c) the patient's right to request human review of any AI-generated recommendation.

7.2 AI System Inventory

The Practice shall maintain a current inventory of all AI and automated systems in use, including the vendor name, processing location, data inputs, and decision-making scope. This inventory must be reviewed quarterly and updated within 72 hours of any system addition or change.

7.3 Clinical AI Governance

Any AI system that influences clinical decision-making must be supervised by a licensed healthcare professional. Fully autonomous clinical decisions by AI systems are prohibited without explicit physician oversight and documented approval workflows.

SECTION 8

EMPLOYEE & CONTRACTOR OBLIGATIONS

All employees, contractors, and temporary staff with access to patient data must:

- Complete data sovereignty awareness training within 30 days of hire and annually thereafter
- Sign the Employee Data Sovereignty Acknowledgment (Appendix B) prior to accessing any patient data system
- Report any suspected data sovereignty violation, unauthorized tool usage, or shadow IT to the Practice Manager or Compliance Officer within 24 hours of discovery
- Use only Practice-approved devices, applications, and communication channels for patient data
- Refrain from downloading, copying, or transmitting patient data to personal devices, accounts, or cloud storage
- Cooperate fully with quarterly compliance audits and provide access to work devices upon request

SECTION 9

INCIDENT RESPONSE & BREACH PROTOCOL

In the event that patient data is discovered to have been routed, stored, or processed outside the Domestic Data Boundary — whether through vendor failure, system misconfiguration, or unauthorized staff action — the following protocol shall be initiated:

Phase	Timeline	Actions Required
Detection	Within 1 hour	Isolate affected system. Document the data exposure scope. Notify Practice Manager.
Assessment	Within 4 hours	Determine data types exposed, volume, duration, and foreign jurisdictions involved.
Containment	Within 24 hours	Terminate foreign data routing. Revoke vendor access if applicable. Secure backup copies.
Notification	Within 72 hours	Notify affected patients per HIPAA Breach Notification Rule. Notify Texas Attorney General if 500+
Remediation	Within 30 days	Implement corrective controls. Update vendor agreements. Conduct root cause analysis.
Documentation	Within 45 days	Complete incident report. Update risk register. File amended BAA if applicable.

SECTION 10

AUDIT, MONITORING & ENFORCEMENT

10.1 Continuous Monitoring

The Practice will undergo quarterly **Sentry Watch** compliance scans to verify that no new third-party scripts, plugins, CDN configurations, or shadow IT have introduced offshore data routing. These automated forensic scans analyze DNS records, IP geolocation, HTTP headers, TLS certificates, and embedded resource origins.

10.2 Annual Forensic Audit

An annual comprehensive forensic audit shall be conducted, encompassing full vendor re-certification, infrastructure mapping, AI system inventory review, and staff compliance verification. Results shall be documented in the annual Sovereignty Audit Report.

10.3 Enforcement & Disciplinary Action

Any employee, contractor, or vendor found to be in violation of this policy shall be subject to:

- **First Offense:** Written warning, mandatory retraining within 7 days, and supervised system access for 90 days
- **Second Offense:** Suspension of system access, formal disciplinary action, and escalation to Practice leadership
- **Third Offense or Willful Violation:** Termination of employment or contract, with potential referral to legal counsel for statutory liability assessment
- **Vendor Violation:** Immediate contract suspension, cessation of data processing, and formal cure notice with 30-day remediation deadline

SECTION 11

SAFE HARBOR AFFIRMATION & CURE PROVISIONS

SAFE HARBOR DECLARATION

By adopting, maintaining, and actively enforcing this Data Sovereignty & Residency Policy, the Practice hereby affirms its intent to comply with Texas Senate Bill 1188 (the Texas Data Sovereignty Act) and demonstrates "Reasonable Care" as defined under the statute's Safe Harbor provisions.

This document, together with quarterly Sentry Watch scan results, vendor Certificates of Data Sovereignty, employee acknowledgments, and annual audit reports, constitutes the Practice's evidentiary portfolio of compliance — serving as primary evidence in the event of a state-level inquiry, regulatory audit, or Cure Notice under SB 1188.

Cure Provisions: In the event that a data sovereignty violation is detected through internal monitoring, external audit, or regulatory inquiry, the Practice shall initiate remediation within 72 hours and complete corrective action within the cure period specified by the applicable enforcement authority. Documentation of the cure process shall be retained for a minimum of six (6) years.

SECTION 12

POLICY GOVERNANCE & AMENDMENT

This policy shall be reviewed and updated **quarterly** or upon any of the following triggering events:

- Amendment or reinterpretation of Texas SB 1188 or HB 149 by the Texas Legislature or Attorney General
- Introduction of new federal data residency or AI governance legislation
- Material change in the Practice's digital infrastructure, vendor relationships, or AI tool usage
- Occurrence of a data sovereignty incident or near-miss event
- Annual audit findings that require policy clarification or strengthening

All amendments must be approved by the Practice Owner or designated Compliance Officer and communicated to all covered personnel within 14 days of adoption.

POLICY EXECUTION

By signing below, the undersigned acknowledges that they have read, understand, and agree to enforce the Data Sovereignty & Residency Policy as set forth in this document. This signature constitutes binding adoption of the policy on behalf of the Practice.

Practice Owner / Authorized Officer

Print name of authorized signatory

Signature

Title / Position

Date of Execution

Witness / Compliance Officer (Optional)

Name

Signature

Date

APPENDIX A

Vendor Data Sovereignty Certificate

This certificate is to be completed by each vendor that processes, stores, or transmits patient data on behalf of the Practice. Return the completed certificate to the Practice Compliance Officer prior to contract execution or renewal.

Vendor Legal Name:

Parent Company (if applicable):

Country of Incorporation:

Primary Data Center Location (City, State):

Backup/DR Data Center Location (City, State):

Cloud Provider & Region (e.g., AWS us-east-1):

Sub-Processors Used (list all):

ATTESTATION: I hereby certify that all data processed on behalf of the above-named Practice is stored and processed exclusively within the continental United States. No sub-processors, CDN nodes, caching layers, or processing endpoints route data outside the U.S. Domestic Data Boundary as defined by Texas SB 1188. I understand that providing false information in this certificate may result in immediate contract termination and potential statutory liability.

Vendor Authorized Signatory:

Title:

Date:

Signature:

APPENDIX B

Employee Data Sovereignty Acknowledgment

I, the undersigned, acknowledge that I have received, read, and understand the Practice's Data Sovereignty & Residency Policy (Version 1.0, Effective February 8, 2026). I agree to:

- Comply with all provisions of the policy, including the prohibition on offshore data routing, unauthorized AI tools, and shadow IT
- Use only Practice-approved devices, applications, and communication channels when handling patient data
- Report any suspected data sovereignty violation to the Compliance Officer within 24 hours
- Complete annual data sovereignty training as required
- Cooperate fully with compliance audits and system access reviews

I understand that violation of this policy may result in disciplinary action up to and including termination, and may expose both myself and the Practice to statutory penalties under Texas law.

Employee Name (Print): ______________________________

Employee Signature: ______________________________

Position / Department: ______________________________

Date: ______________________________

APPENDIX C

Quarterly Compliance Audit Checklist

Audit Period: ____________________ Auditor: ____________________

#	Audit Item	Status	Notes
1	Sentry Watch scan completed — no offshore data routing detected		
2	All vendor Certificates of Data Sovereignty current and on file		
3	AI system inventory reviewed and updated		
4	Employee acknowledgment forms current for all active staff		
5	Website hosting and DNS verified as domestic-only		
6	Email (MX) routing verified — no foreign relay servers		
7	Cloud infrastructure regions verified (no non-U.S. zones)		
8	Third-party scripts and plugins audited for data residency		
9	Telehealth platform verified for domestic processing		
10	HB 149 AI disclosure visible and accurate on website		
11	Shadow IT sweep completed — no unauthorized tools detected		
12	Incident log reviewed — all incidents resolved within SLA		
13	Policy version current — no amendments pending		
14	Staff training completion rate at or above 100%		

Audit Result: [ ] COMPLIANT [ ] NON-COMPLIANT [ ] REMEDIATION REQUIRED

Auditor Signature: ____________________

Date: ____________________

Practice Manager Acknowledgment: ____________________

Date: ____________________