STAFF TRAINING GUIDE | INTERNAL USE ONLY

Digital Sovereignty & Patient Privacy Standards

Mandatory compliance training for all employees, contractors, and temporary staff with access to patient data. Covers Texas Senate Bill 1188 (Data Sovereignty) and House Bill 149 (AI Transparency) requirements, prohibited tools, approved workflows, and incident reporting procedures.

TRAINING DURATION: 15 MINUTES
This guide is designed for front-office staff, clinical assistants, billing teams, and any personnel who handle patient information in any form — digital or physical.

Subject:	Digital Sovereignty & Patient Privacy Standards
Governing Statutes:	Texas SB 1188 (Data Sovereignty) + HB 149 (AI Transparency)
Audience:	All staff with patient data access
Frequency:	Required at hire; annual refresher thereafter
Version:	1.0 — February 2026
Prepared By:	KairoLogic Compliance Division

NOTICE: This training guide contains confidential compliance procedures. Distribution outside the practice is prohibited. Completion of this training and the accompanying attestation form is a condition of employment for all staff with access to patient data systems.

TRAINING MODULES

MODULE 1

The Core Rule — What Is Data Sovereignty?

Starting in 2026, Texas law requires that **all patient information** — medical records, appointment details, billing data, even text messages about scheduling — must stay within the United States at all times. This isn't just a HIPAA issue. It's a **Data Sovereignty** issue, governed by a new state law called **Senate Bill 1188**.

> **KEY POINT:** If **any** digital tool you use at work processes patient data outside the U.S. — even briefly, even accidentally — our practice could face fines up to **$250,000 per violation**. That is not a typo. A quarter of a million dollars. Per incident.

What does "data sovereignty" mean in plain English?

It means patient data must **physically exist on computers located inside the United States**. When you type a patient's name into an app, that information travels to a server somewhere. If that server is in Germany, Ireland, Singapore, or any other foreign country — even for a split second — it violates Texas law.

Why should I care? I'm not in IT.

Because most data sovereignty violations don't happen in the server room. They happen at the front desk, in the break room, or on a staff member's phone. Someone copies a patient name into a free AI tool. Someone texts a colleague about a patient on WhatsApp. Someone installs a "helpful" browser extension. These everyday actions are where violations happen, and under SB 1188, the practice — and potentially the individual — is held responsible.

REAL-WORLD EXAMPLE: The Front Desk Shortcut

Maria at the front desk is behind on chart notes. She copies three patients' visit summaries into her personal ChatGPT account to "clean them up." ChatGPT processes that text on servers in Ireland. The data has now left the United States. Under SB 1188, this is a violation — even though Maria was trying to be efficient, even though she deleted the conversation afterward, and even though no harm came to the patients. **The violation is the data leaving the country. Period.**

MODULE 2

The Prohibited Tools List — Common Data Leaks

The following tools and behaviors are **strictly prohibited** for any task involving patient information. This includes scheduling, notes, billing, messaging, transcription, and any other activity that touches patient names, dates, conditions, or contact information.

Category	Prohibited Tools	Why It's Dangerous
Personal AI Accounts	ChatGPT (free/personal), Google Gemini, Microsoft Copilot (personal), Claude (free), DeepSeek, any free AI chatbot	Data is processed on global servers. You cannot verify where patient data goes. Free tiers have zero data residency guarantees.
Foreign Browser Extensions	Grammarly (free), LanguageTool, Google Translate extension, AI writing assistants, "productivity" plugins	These extensions read everything you type — including patient data in your EMR. Text is sent to foreign servers for processing.
Unauthorized Messaging	WhatsApp, Telegram, Signal (personal), Facebook Messenger, Instagram DMs, personal iMessage, personal SMS	Messages route through global server clusters. Even "encrypted" apps may store metadata overseas. None are HIPAA-compliant.
Personal Email	Gmail (personal), Yahoo Mail, Outlook.com (personal), ProtonMail (personal), any non-practice email	Personal email servers are unverified for data residency. You have no control over where backups are stored.
Free Cloud Storage	Personal Google Drive, personal Dropbox, personal OneDrive, Box (free), WeTransfer, any file-sharing not approved by practice	Files may replicate to servers outside the U.S. for "global redundancy." Free tiers offer zero residency control.
Unapproved AI Transcription	Otter.ai (free), Whisper (self-hosted without verification), foreign transcription services, voice-to-text apps	Audio containing patient information is processed on unknown servers. Transcription AI often trains on your data.

WARNING: Using **any** of the tools above for patient-related tasks is a policy violation. First offense: written warning and mandatory retraining within 7 days. Second offense: suspension of system access and formal disciplinary action. Third offense or willful violation: termination.

What CAN I use?

Only tools on the practice's **Approved Software List**. If you're not sure whether a tool is approved, **ask your Practice Manager or Data Sovereignty Officer before using it**. The 30-second question could save the practice $250,000.

Function	Approved Tool(s)	Notes
Patient Records	[Your EMR — e.g., eClinicalWorks]	Only access through practice-issued devices
Email	[Practice email — e.g., Google Workspace]	Never forward patient data to personal email
Messaging	[Practice system — e.g., Weave]	Patient messaging only through approved platform

Telehealth	[Approved platform — e.g., Doxy.me]	HIPAA-compliant, US-hosted video platform
AI Transcription	[If applicable — e.g., Freed Health]	Enterprise version only; verified for US residency
File Storage	[Practice drive — e.g., Google Drive (Workspace)]	Enterprise account with US-only data residency

PRACTICE MANAGER NOTE
Customize the "Approved Tool(s)" column above with your specific vendors before distributing this guide to staff. The approved list should match the vendors documented in your Evidence Ledger.

MODULE 3

Working with AI — HB 149 Transparency Rules

Texas House Bill 149 requires healthcare practices to be **transparent** with patients about AI usage. This means if we use AI for anything — scheduling, transcription, note-taking, reminders, or clinical support — patients have the right to know.

Rule 1: Always Be Honest About AI

If a patient asks "Is this an AI?" or "Did a computer write this?" — always answer truthfully. Never deny or hide that AI is being used. Here are sample responses:

Patient Asks...	You Say...
"Is this message from a computer?"	**"Yes, we use an AI tool to help draft reminders, but a real team member reviews everything before it goes out to you."**
"Are you using AI on my records?"	**"We use a US-based AI transcription tool to help document your visit notes accurately. Your doctor reviews and approves everything before it's added to your chart."**
"I don't want AI touching my data."	**"Absolutely, I'll make a note of that in your chart. You can opt out of specific AI-assisted processes at any time. Your data privacy is our top priority."**
"Is my data safe?"	**"Yes. All our AI tools are verified to keep your data exclusively within the United States. We comply with Texas data sovereignty laws, and your information is protected by HIPAA."**

Rule 2: Human-in-the-Loop — AI Never Gets the Final Word

Every piece of content generated by AI — whether it's a clinical note, a patient message, a billing code suggestion, or a diagnostic insight — must be **reviewed and approved by a human staff member** before it is sent to a patient, entered into a medical record, or used in any clinical decision. No exceptions.

> **KEY POINT:** AI is a **tool**, not a decision-maker. Think of it like spell-check: it helps, but you always read the final version before hitting send. If AI generates something that looks wrong, override it. You are the quality control.

MODULE 4

The 3-Step Vendor Check — Before You Sign Up for Anything

Many data leaks start when a well-meaning staff member signs up for a "free trial" of a cool new app. Before creating an account, downloading software, or entering patient data into **any new tool** — even free ones — you must get approval. Here's how:

Step 1: STOP. Do not sign up yet.

No matter how useful the tool looks, do not create an account or enter any information until it has been verified. Free trials collect your data from the moment you register.

Step 2: Ask the vendor these three questions:

#	Question to Ask the Vendor	What You Need to Hear
1	"Is your data storage and processing 100% based in the United States?"	"Yes" — with a specific answer about server locations. Vague answers like "we use secure servers" are not acceptable.
2	"Do you use any offshore sub-processors, CDNs, or AI models hosted outside the U.S.?"	"No" — with confirmation that ALL processing stays domestic. Watch for phrases like "global infrastructure" which may indicate foreign routing.
3	"Can you provide a written Data Residency Certificate for Texas SB 1188 compliance?"	"Yes" — a real document confirming U.S.-only data residency. If they say "we're HIPAA compliant" instead, that is NOT the same thing.

Step 3: Bring the answers to your Practice Manager.

Forward the vendor's responses to your Practice Manager or Data Sovereignty Officer. They will verify the tool, add it to the Evidence Ledger if approved, and give you the go-ahead. This process typically takes 1-3 business days.

REMEMBER
"HIPAA compliant" and "SB 1188 compliant" are NOT the same thing. HIPAA protects data **security**. SB 1188 protects data **location**. A tool can be perfectly HIPAA-compliant and still violate Texas law by storing data on a server in Ireland.

MODULE 5

Reporting a Data Leak — What to Do If Something Goes Wrong

Mistakes happen. What matters is how quickly you respond. Under Texas law, a practice that **self-reports and remediates** a data sovereignty issue within 30 days may qualify for Safe Harbor protection — meaning reduced or eliminated penalties. But only if you act fast.

The 4-Step Incident Response (for any staff member):

STEP 1: STOP
Immediately stop using the tool. Close the app, browser tab, or service. Do not attempt to "clean up" or delete data — that may destroy evidence needed for the investigation.

STEP 2: REPORT
Notify your Practice Manager or Data Sovereignty Officer within 1 hour. This is not optional. You will not be punished for honest reporting. You WILL face consequences for covering it up.

STEP 3: DOCUMENT
Write down: What tool you used, what patient data was involved, when it happened, and how you discovered the issue. Be specific. This will be logged in the Evidence Ledger.

STEP 4: COOPERATE
Your Practice Manager will initiate the formal incident response process. Cooperate fully with any investigation. The goal is to remediate the issue within 30 days to protect the practice.

KEY POINT: No retaliation. This practice has a strict no-retaliation policy for good-faith incident reporting. You will never be punished for reporting a suspected data leak. You WILL be held accountable for failing to report one.

MODULE 6

Real-World Scenarios — Test Your Knowledge

For each scenario below, think about what you would do before reading the answer.

Scenario 1: The Grammar Checker

SITUATION

You're typing a referral letter in the EMR and realize you have a Grammarly browser extension installed. It's highlighting errors in real-time. Is this okay?

CORRECT RESPONSE: NO. Free Grammarly sends all text to external servers for processing — including any patient information visible on screen. Disable the extension on work devices immediately and notify your Practice Manager. Use your EMR's built-in spell check instead.

Scenario 2: The Helpful Coworker

SITUATION

A coworker shows you a cool AI app that can summarize patient intake forms in seconds. They've been using it for a week. What do you do?

CORRECT RESPONSE: Report it to your Practice Manager or Data Sovereignty Officer immediately. Even if the tool seems helpful, it hasn't been verified for U.S. data residency. Your coworker isn't in trouble for being unaware, but the tool must be assessed before further use. This is exactly the kind of "shadow IT" that causes SB 1188 violations.

Scenario 3: The After-Hours Text

SITUATION

A doctor texts you on your personal phone asking you to look up a patient's medication list and text it back. What do you do?

CORRECT RESPONSE: Decline politely. Patient data should never be sent via personal text messages. Respond: "I'd be happy to help, but I need to pull that up through our approved system. I'll send it through [approved platform] first thing in the morning." Log the request with your Practice Manager.

Scenario 4: The Vendor Demo

SITUATION

A sales rep is showing your office a new scheduling tool. During the demo, they ask you to enter some "test patient data" to see how it works. Is this okay?

CORRECT RESPONSE: NO. Never enter real patient data into an unverified system, even as a "test." Use obviously fake data (e.g., "John Doe, 555-0100") during vendor demonstrations. If the vendor asks for real data, that's a red flag.

MODULE 7

Quick Reference Card — Print & Post

Print this page and post it at every workstation, in the break room, and at the front desk.

DATA SOVEREIGNTY — STAFF QUICK REFERENCE

THE RULE: ALL patient data must stay in the United States. No exceptions.

NEVER USE: Personal ChatGPT/AI, WhatsApp, personal email, free browser extensions, unapproved apps, free cloud storage — for ANY patient-related task.

ALWAYS USE: Practice-approved tools only. If it's not on the approved list, don't use it.

IF A PATIENT ASKS ABOUT AI: Be honest. "Yes, we use US-based AI to help with [function]. Your doctor always reviews everything. Your data never leaves the country."

BEFORE SIGNING UP FOR ANYTHING NEW:
1. Is data stored 100% in the U.S.?
2. Any offshore sub-processors?
3. Can they provide a Data Residency Certificate?
Then bring the answers to your Practice Manager.

IF YOU MAKE A MISTAKE: STOP using the tool. REPORT to Practice Manager within 1 hour. DOCUMENT what happened. No retaliation for honest reporting.

THE PENALTY: Up to $250,000 per violation. This is everyone's responsibility.

Questions? Contact: [Data Sovereignty Officer Name] | [Phone/Email]

STAFF ATTESTATION

Data Sovereignty Training Acknowledgment

This attestation must be completed by every employee, contractor, and temporary staff member with access to patient data. Signed attestations are retained in personnel files and serve as documented evidence of compliance training under the practice's Safe Harbor™ program.

ATTESTATION

I, the undersigned, hereby attest that:

1. I have read and understood the Practice's Data Sovereignty & Residency Policy in its entirety.

2. I have completed the Staff Training Guide on Digital Sovereignty & Patient Privacy Standards.

3. I understand that Texas Senate Bill 1188 requires all patient data to remain within the United States and that violations may result in fines up to $250,000 per incident.

4. I understand that Texas House Bill 149 requires transparency with patients about AI usage and that I must disclose AI use honestly when asked.

5. I agree to use ONLY practice-approved digital tools for all patient-related tasks, including scheduling, documentation, communication, and data processing.

6. I will NOT use personal AI accounts, unauthorized messaging apps, personal email, unapproved browser extensions, or any unverified digital tool for patient data.

7. I will report any suspected data sovereignty violation to the Practice Manager or Data Sovereignty Officer within one (1) hour of discovery.

8. I understand that violation of the Data Sovereignty Policy may result in disciplinary action up to and including termination of employment.

9. I understand that the practice maintains a no-retaliation policy for good-faith reporting of suspected data sovereignty incidents.

Employee Name (Print): _____

Employee Signature: _____

Position / Department: _____

Date of Training Completion: _____

Training Administered By: _____

Trainer Signature: _____

Date: _____

This form should be completed within 30 days of hire and annually thereafter during refresher training. Store signed forms in employee personnel files and maintain digital scans in the compliance documentation folder.