30-DAY COMPLIANCE ROADMAP | SAFE HARBOR™ VERIFICATION

The 30-Day Path to Sovereign Verification

A structured, phase-by-phase implementation plan to transition your practice from "Pre-Audited" (At-Risk) to "Verified Sovereign" (Safe Harbor) status on the Texas Sovereignty Registry — establishing documented compliance with SB 1188 and HB 149 within 30 calendar days.

> **OBJECTIVE**
> Transition from **"Pre-Audited" (At-Risk)** to **"Verified Sovereign" (Safe Harbor)**
>
> Upon completion, your practice will have: a signed Data Sovereignty Policy, deployed AI disclosures, verified vendor residency records, trained staff with signed attestations, and a Verified Sovereign listing on the Texas Sovereignty Registry — a complete evidentiary portfolio that constitutes "Reasonable Care" under SB 1188.

Phase	Days	Focus	Outcome
Phase 1	Days 1–7	Forensic Diagnostic	Complete inventory of digital supply chain; identify compliance gaps
Phase 2	Days 8–14	Policy Adoption & Transparency	Signed policy on file; AI disclosures deployed; vendor verification initiated
Phase 3	Days 15–21	Vendor Hardening & Staff Training	All vendors verified or flagged; staff trained and attestations collected
Phase 4	Days 22–30	Verification & Defense	Registry verification complete; Safe Harbor evidence portfolio assembled
Ongoing	Every 90 days	Maintenance & Monitoring	Quarterly audit; Sentry Watch scan; evidence ledger updated

Audience: Practice Managers, Compliance Officers, Medical Directors

Prerequisite: KairoLogic Safe Harbor™ Policy Bundle (purchased)
Version: 1.0 — February 2026

PHASE 1

The Forensic Diagnostic

<div style="text-align:center">

DAYS 1 – 7

</div>

Before you can fix compliance gaps, you need to know where they are. Phase 1 is a complete forensic inventory of your practice's digital footprint — every vendor, every tool, every script running on your website. This is the diagnostic that tells you exactly what needs to change.

1.1 Digital Supply Chain Inventory

Open the Evidence Ledger (Tab 1: Digital Supply Chain). Systematically document every software vendor and digital service that touches patient data:

[ ]	Task	Owner	Deliverable
[ ]	List your EMR / EHR system with server location and contract details	Practice Mgr	Ledger Row 1
[ ]	List your website hosting provider and verify DNS records for US-only hosting	IT / Web Dev	Ledger + DNS audit
[ ]	List your email service provider (Google Workspace, Microsoft 365, etc.)	Practice Mgr	Ledger Row
[ ]	List your appointment scheduling and patient communication tools	Front Desk Mgr	Ledger Row
[ ]	List your telehealth / video conferencing platform	Practice Mgr	Ledger Row
[ ]	List your billing, RCM, and insurance verification tools	Billing Mgr	Ledger Row
[ ]	List ALL AI tools in use (transcription, chatbots, clinical AI, etc.)	Practice Mgr	Ledger + AI Inventory
[ ]	List your backup and disaster recovery services	IT Admin	Ledger Row
[ ]	List any marketing tools (CRM, newsletter, review management)	Marketing	Ledger Row
[ ]	List VoIP, phone system, and fax services	Office Mgr	Ledger Row

1.2 Digital Perimeter Sweep

Perform a forensic scan of your practice website to identify hidden scripts, tracking pixels, embedded resources, and third-party integrations that may be routing data through offshore servers. Many practices are unaware that their website contains foreign-hosted scripts added by marketing plugins, analytics tools, or theme

components.

[ ]	Task	Owner	Deliverable
[ ]	Run a KairoLogic Sentry Scan on your practice website URL	Practice Mgr	Sentry Report PDF
[ ]	Review scan results for any foreign-hosted scripts or resources	Practice Mgr	Gap list
[ ]	Identify all third-party tracking pixels (Google Analytics, Facebook, etc.)	Web Dev	Script inventory
[ ]	Check for CDN endpoints that may route through foreign edge nodes	IT / Web Dev	CDN config docs
[ ]	Review website form handlers (intake, contact, appointment request)	Web Dev	Form routing audit
[ ]	Check for embedded chat widgets or AI chatbots and their hosting origins	Practice Mgr	Widget audit

1.3 Compliance Gap Analysis

Compare your current digital footprint against the requirements of both SB 1188 (Data Sovereignty) and HB 149 (AI Transparency). Identify every gap that must be closed before verification.

Compliance Area	SB 1188 Requirement	Your Status
Data Residency Policy	Signed, entity-specific policy on file	[ ] Complete [ ] Incomplete
Vendor Verification	All Critical/High vendors verified for US residency	[ ] Complete [ ] Incomplete
AI Disclosure (Website)	Public-facing notice on website per HB 149	[ ] Complete [ ] Incomplete
AI Consent (Intake)	Patient consent form in intake packet	[ ] Complete [ ] Incomplete
Privacy Policy Update	AI Transparency section added	[ ] Complete [ ] Incomplete
Employee Training	All staff trained + attestations signed	[ ] Complete [ ] Incomplete
Evidence Ledger	Complete vendor inventory with proofs	[ ] Complete [ ] Incomplete
Foreign Script Removal	No offshore scripts on practice website	[ ] Complete [ ] Incomplete
Shadow IT Sweep	No unauthorized tools in use by staff	[ ] Complete [ ] Incomplete

PHASE 1 DELIVERABLE: A completed Evidence Ledger (Tab 1) with every vendor documented, a Sentry Scan report identifying any foreign-hosted scripts, and a Gap Analysis showing exactly what must be remediated in Phase 2. You should now know precisely where your practice stands.

PHASE 2

Policy Adoption & Transparency Deployment

<div style="text-align:center">

DAYS 8 – 14

</div>

With your diagnostic complete, Phase 2 focuses on establishing the foundational compliance documents: your signed Data Sovereignty Policy, public-facing AI disclosures, and the initiation of vendor verification outreach.

2.1 Adopt & Execute the Data Sovereignty Policy

[ ]	Task	Owner	Deliverable
[ ]	Open SB 1188 Data Sovereignty Policy; replace all [Practice Name] placeholders with legal entity name	Practice Mgr	Customized policy
[ ]	Designate a Data Sovereignty Officer by name and title (typically Office Manager)	Med Director	Officer designation
[ ]	Review the policy with Medical Director or Practice Owner	Med Director	Review confirmed
[ ]	Print the finalized policy and obtain "wet ink" signatures on execution page	Practice Mgr	Signed original
[ ]	Scan signed policy as PDF; file original in HIPAA binder, digital copy in compliance folder	Practice Mgr	3 copies secured

2.2 Deploy AI Transparency Disclosures (HB 149)

[ ]	Task	Owner	Deliverable
[ ]	Deploy website footer AI Transparency Notice (from AI Disclosure Kit, Asset 1) on all pages	Web Dev	Screenshot evidence
[ ]	Add AI Consent Form (Asset 2) to new-patient intake packet, after HIPAA Notice of Privacy Practices	Front Desk Mgr	Updated packet

[ ]	Task	Owner	Deliverable
[ ]	Insert AI Transparency section (Asset 3) into website privacy policy	Web Dev	Updated policy page
[ ]	Print and post waiting room signage (Asset 7) in patient-facing areas	Office Mgr	Signage displayed
[ ]	Train front desk staff on phone inquiry scripts (Asset 4, all 3 scenarios)	Practice Mgr	Training log
[ ]	Post Staff AI Guidelines (Asset 5) in breakroom and add to employee handbook	Practice Mgr	Posted + handbook

2.3 Initiate Vendor Verification Outreach

[ ]	Task	Owner	Deliverable
[ ]	Send Vendor AI Verification email (Asset 8) to all CRITICAL-tier vendors in your Evidence Ledger	Practice Mgr	Sent emails logged
[ ]	Send Vendor AI Verification email to all HIGH-tier vendors	Practice Mgr	Sent emails logged
[ ]	Set 14-business-day deadline in calendar for vendor responses	Practice Mgr	Calendar reminder
[ ]	Request Data Processing Addendums (DPAs) or Data Residency Certificates from each vendor	Practice Mgr	Requests sent

> **PHASE 2 DELIVERABLE:** A signed Data Sovereignty Policy filed in your HIPAA binder, AI disclosures live on your website and in patient intake forms, waiting room signage displayed, staff briefed on AI scripts, and vendor verification emails sent to all Critical and High-tier vendors.

PHASE 3

Vendor Hardening & Staff Training

DAYS 15 – 21

Phase 3 closes the two most common compliance gaps: unverified vendors and untrained staff. By the end of this phase, every vendor should be verified (or flagged for replacement) and every staff member should have completed the sovereignty training with a signed attestation.

3.1 Vendor Verification & Hardening

[ ]	Task	Owner	Deliverable

[ ]	Task	Owner	Deliverable
[ ]	Collect and review vendor responses to verification emails sent in Phase 2	Practice Mgr	Responses on file
[ ]	For each confirmed vendor: save reply as PDF, update Evidence Ledger status to "SOVEREIGN"	Practice Mgr	Ledger updated
[ ]	For vendors providing formal DPAs or Certificates: file in /Compliance/Vendor-Confirmations/	Practice Mgr	Certs on file
[ ]	For non-responsive vendors: send follow-up email with 7-day deadline	Practice Mgr	Follow-up sent
[ ]	For vendors that CANNOT confirm US residency: flag as "NON-COMPLIANT" in Ledger	Practice Mgr	Flagged in Ledger
[ ]	For non-compliant vendors: begin researching US-sovereign alternatives and create migration plan	Practice Mgr + IT	Migration plan
[ ]	Remove or replace any foreign-hosted scripts identified in Phase 1 Sentry Scan	Web Dev	Clean scan result
[ ]	Update Evidence Ledger Tab 2 (Technical Residency Signals) with all network endpoints	IT Admin	Tab 2 complete

3.2 Staff Training & Attestation

[ ]	Task	Owner	Deliverable
[ ]	Schedule 15-minute "Sovereignty Huddle" training session for all staff	Practice Mgr	Meeting invite
[ ]	Conduct training using Staff Training Guide (Modules 1–5)	Practice Mgr	Training delivered
[ ]	Walk through real-world scenarios (Module 6) with staff	Practice Mgr	Discussion complete
[ ]	Distribute and collect signed Staff Attestation forms from every employee	Practice Mgr	Signed forms
[ ]	File signed attestations in personnel files (physical + digital scan)	Practice Mgr / HR	Filed + scanned
[ ]	Post Quick Reference Card (Module 7) at all workstations and in breakroom	Office Mgr	Cards posted
[ ]	Distribute Approved Software List to all staff (from Training Guide Module 2)	Practice Mgr	List distributed

> **PHASE 3 DELIVERABLE:** All vendors verified or flagged with migration plans, foreign scripts removed from website, Evidence Ledger fully populated with proofs, all staff trained with signed attestations on file, Quick Reference Cards posted at workstations.

PHASE 4

Verification & Safe Harbor Defense

<div align="center">

DAYS 22 – 30

</div>

The final phase brings everything together: a comprehensive audit of your evidence portfolio, verification on the Texas Sovereignty Registry, and assembly of your Safe Harbor defense package.

4.1 Final Evidence Audit

[ ]	Task	Owner	Deliverable
[ ]	Review Evidence Ledger Tab 1: confirm all vendors have status of SOVEREIGN or documented migration plan	Practice Mgr	Ledger audit
[ ]	Review Evidence Ledger Tab 2: confirm all network endpoints are documented and sovereign	IT Admin	Tab 2 audit
[ ]	Verify all vendor confirmation PDFs are saved and organized in compliance folder	Practice Mgr	File audit
[ ]	Confirm all employee attestation forms are signed, scanned, and filed	Practice Mgr	HR file check
[ ]	Verify AI disclosure is live on website footer (screenshot for evidence)	Practice Mgr	Screenshot PDF
[ ]	Verify AI Consent Form is in current patient intake packet	Front Desk Mgr	Packet check
[ ]	Verify waiting room signage is displayed	Office Mgr	Photo evidence
[ ]	Complete the Quarterly Audit Checklist (Appendix C of Policy Pack) for Q1	Practice Mgr	Checklist signed

4.2 Registry Verification

[ ]	Task	Owner	Deliverable

[ ]	Run a final KairoLogic Sentry Scan on your practice website to confirm clean results	Practice Mgr	Final scan report
[ ]	Visit kairologic.com/registry and locate your practice listing	Practice Mgr	Listing found
[ ]	Click "Claim & Verify" and complete identity verification steps	Practice Mgr	Verification submitted
[ ]	Confirm practice status updates from "Pre-Audited" to "Verified Sovereign"	Practice Mgr	Status confirmed

4.3 Assemble Safe Harbor Evidence Portfolio

Compile the following documents into a single compliance binder (physical and digital). This portfolio is your definitive Safe Harbor defense:

#	Document	Status
1	**Signed Data Sovereignty Policy (SB 1188)**	[ ] On file
2	**Evidence Ledger (all tabs complete)**	[ ] On file
3	**Vendor Data Residency Certificates / Confirmation PDFs**	[ ] On file
4	**AI Disclosure Kit deployment evidence (website screenshots)**	[ ] On file
5	**Signed Patient AI Consent Forms (sample batch)**	[ ] On file
6	**Signed Employee Attestation Forms (all staff)**	[ ] On file
7	**Staff Training completion log**	[ ] On file
8	**KairoLogic Sentry Scan Report (baseline + final)**	[ ] On file
9	**Quarterly Audit Checklist (Q1 completed)**	[ ] On file
10	**Registry Verification confirmation**	[ ] On file

CONGRATULATIONS — YOU'RE SOVEREIGN.

Your practice now has a complete, documented Safe Harbor defense under Texas SB 1188 and HB 149. Your signed policy, verified vendor records, deployed disclosures, trained staff, and Registry verification collectively establish "Reasonable Care" — the strongest protection available against civil penalties, Cure Notices, and regulatory action. You have transitioned from "Pre-Audited" to "Verified Sovereign."

ONGOING

Quarterly Maintenance & Monitoring

<div align="center">

EVERY 90 DAYS

</div>

Safe Harbor standing requires **ongoing compliance**, not a one-time implementation. The most common way practices lose their Verified Sovereign status is through "Shadow IT drift" — new marketing plugins, staff installing unapproved tools, or vendors changing their infrastructure without notice. The quarterly maintenance cycle prevents this.

> **THE QUARTERLY SWEEP — Set a recurring calendar reminder for every 90 days.**
>
> Failure to maintain quarterly audits degrades your Safe Harbor evidence portfolio over time. A signed policy from 2026 with no subsequent audit trail tells a regulator in 2027 that you "set it and forget it" — undermining your Reasonable Care defense.

[ ]	Task	Owner	Deliverable
[ ]	Run a KairoLogic Sentry Watch scan on your practice website	Practice Mgr	Scan report PDF
[ ]	Review scan results for any new foreign scripts, plugins, or tracking pixels	Practice Mgr	Clean scan confirmed
[ ]	Review Evidence Ledger Tab 1: update any vendors that have changed or been added	Practice Mgr	Ledger current
[ ]	Re-verify any vendor whose contract has been renewed or modified	Practice Mgr	Updated certs
[ ]	Check for new employees needing Data Sovereignty training + attestation	Practice Mgr / HR	New attestations
[ ]	Verify AI disclosure is still live and accurate on website footer	Practice Mgr	Screenshot PDF
[ ]	Review AI system inventory for any new or discontinued tools	Practice Mgr	Inventory updated
[ ]	Conduct Shadow IT sweep: check for unapproved tools on staff devices	IT Admin	Sweep results
[ ]	Complete the Quarterly Audit Checklist (Appendix C of Policy Pack)	Practice Mgr	Signed checklist
[ ]	Log the audit in Evidence Ledger Tab 4 (Quarterly Audit Trail)	Practice Mgr	Audit trail row

[ ]	Update the "Last Updated" date on your Evidence Ledger	Practice Mgr	Ledger timestamp

Recommended Quarterly Schedule

Quarter	Target Date	Focus Areas	Completed
Q1 2026	March 31	Initial implementation complete. Baseline audit.	[ ]
Q2 2026	June 30	First 90-day review. New vendor check. Staff refresher.	[ ]
Q3 2026	September 30	Mid-year audit. Website re-scan. Shadow IT sweep.	[ ]
Q4 2026	December 31	Annual review. Policy version control. Full re-certification.	[ ]
Q1 2027	March 31	Anniversary audit. Vendor contract renewals. Annual training.	[ ]

Support & Escalation

Need	Contact
Implementation questions	support@kairologic.net
Website disclosure help	support@kairologic.net (subject: "HB 149 Website Help")
Vendor won't confirm residency	support@kairologic.net (subject: "Vendor Escalation")
Registry status issue	support@kairologic.net (subject: "Registry Update")
Request a re-scan	kairologic.com — Scan section (immediate)
Upgrade to Sentry Watch monitoring	kairologic.com — Services page
Legal questions (SB 1188 / HB 149)	Consult your practice attorney

Roadmap Completion Sign-Off

Practice Manager Name:
_____

Signature:
_____

Date Roadmap Completed:
_____

Next Quarterly Audit Date:
_____