



# Week 1: AI Tool Inventory

Seven PDF AI Governance Survival Kit™ | AI Safety Enforcement Arsenal  
for California Clinics & Nonprofits | CREATE IN 1 DAY | 7-WEEK ZERO-  
VIOLATION PROCESS | California Certified AI Compliance Officer™ |  
AICAREAGENTS247 Nonprofit Corporation | #AICAREAGENTS247

# The Shadow AI Multiplier: Unmanaged Tools Trigger Catastrophic Legal Liability



Under the **California Privacy Rights Act (CPRA)**, every single unauthorized data ingestion event by a third-party AI is a distinct violation.

**Shadow AI** is not an IT issue; it is an existential financial threat.

# Week 1 Mandate: Discover, Document, and Neutralize the Threat



## 7-Week Zero-Violation Process



# 1

## Audit the Perimeter

Identify all sanctioned and unsanctioned AI tools currently operating on clinic devices.

# 2

## Classify the Risk

Determine if tools are interacting with Protected Health Information (PHI) or making autonomous decisions.

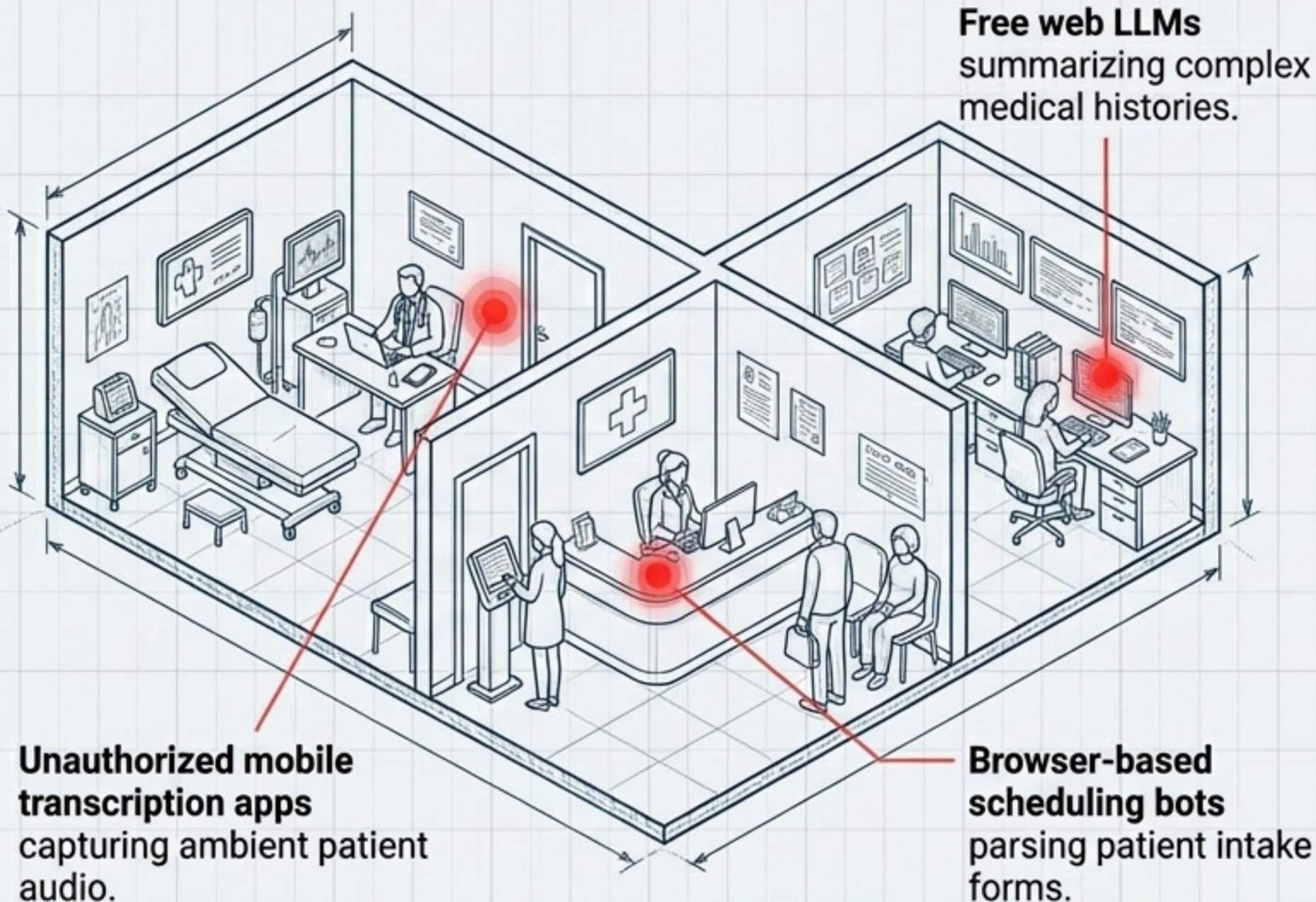
# 3

## Lock the Vendor

Demand contractual compliance or force an immediate halt to usage.

# Locating the Blind Spots: Clinical Workflows and The Triage Matrix

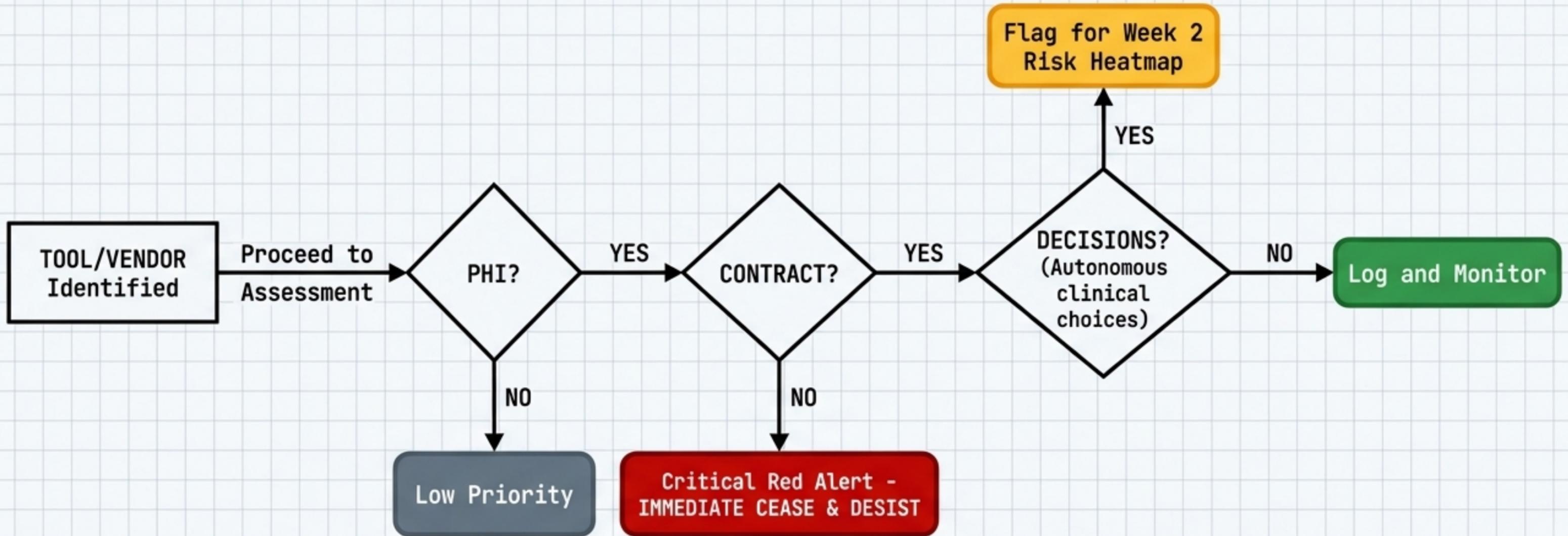
## The Shadow AI Anatomy Diagram



## The Triage Matrix

Verified Green Compliant Triggers	Critical Red Toxic Triggers
<ul style="list-style-type: none"><li>Local processing only</li><li>No PHI ingested</li><li>Explicit BAA signed</li><li>Clear patient consent</li></ul>	<ul style="list-style-type: none"><li>Cloud-based LLM processing</li><li>Ambient patient data ingestion</li><li>No explicit vendor contract</li><li>Opaque data retention</li></ul>

# The Inventory Logic: Assessing Tool Viability Through Data Flow



Every tool MUST pass this logic gate. Any tool processing PHI without an executed contract violates CPRA and HIPAA immediately.

# AI Tool Inventory Master Log [Clinical & Diagnostic]

TOOL	VENDOR	PHI?	PURPOSE	DECISIONS?	CONTRACT?
Nuance DAX	Microsoft	YES	Ambient Scribe	NO	YES
ChatGPT Free	OpenAI	YES	Chart Summarization	NO	NO -> ACTION REQUIRED
Aidoc	Aidoc Medical	YES	Radiology Triage	YES	YES

 Log all clinical ingestion points. If CONTRACT is blank and PHI is YES, isolate the tool immediately.

# AI Tool Inventory Master Log [Administrative & Operational]

TOOL	VENDOR	PHI?	PURPOSE	DECISIONS?	CONTRACT?
Drift Bot	Drift	[NO]	Patient FAQ	[NO]	[YES-GREEN]
Otter.ai	Otter	[YES-RED]	Staff Meeting Transcripts	[NO]	[NO-RED] -> ACTION REQUIRED
Grammarly	Grammarly	[POTENTIAL-AMBER]	Email Drafting	[NO]	[NO-RED] -> ACTION REQUIRED

**i** Shadow AI frequently enters through administrative efficiency tools. Audit all browser extensions and scheduling applications.

# The Interrogation Protocol: Forcing Vendor Compliance

Neutralizes shadow ingestion risks.

Establishes baseline HIPAA compliance.

Plain-text email,

Provide immediate verification of your data retention policy regarding patient data inputs.

Confirm whether our data is being used to train your underlying machine learning models.

If you cannot provide an executed BAA, consider this a formal request to delete all associated data.

Invokes CPRA Right to Delete.

Triggers the 45-day legal compliance window.

Deploy this template to all vendors lacking a 'YES' in the CONTRACT column of your inventory

# Week 1 Certification Tracker: Securing the Perimeter



Week 1 Arsenal Deployed. Proceed to Week 2: Risk Heatmap.