PDF 6: INCIDENT CRISIS PLAYBOOK - WEEK 6 OF 7

CREATE IN 1 DAY | 7-WEEK ZERO-VIOLATION IMPLEMENTATION PROCESS

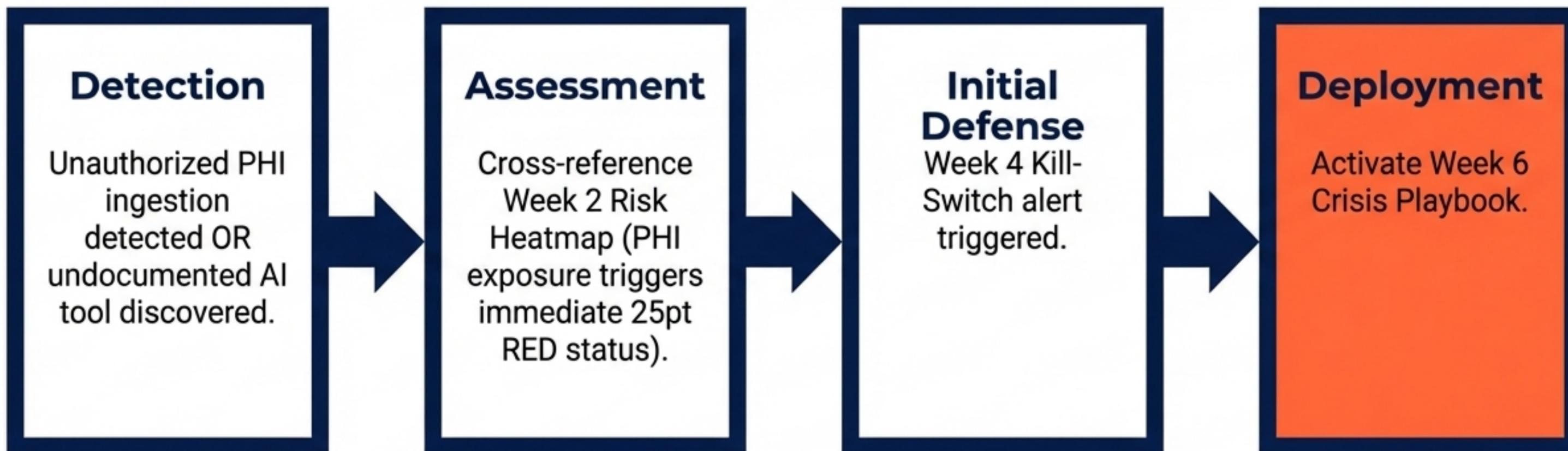| Seven PDF AI Governance Survival Kit™ | AI Safety Enforcement Arsenal for California Clinics & Nonprofits | California Certified AI Compliance Officer™ | AICAREAGENTS247 Nonprofit Corporation Education Board™ | The California Association of AI Compliance Officers (CAAIC)™ | AICAREAGENTS247 AI Governance Research™ | #AICAREAGENTS247 |

We exist to protect California clinics, faith-based providers, and under-resourced nonprofits from AI and data-misuse risk, and we use this 7-PDF Survival Kit as our core toolbox.

Playbook Activation Triggers

Detection

Unauthorized PHI ingestion detected OR undocumented AI tool discovered.

Assessment

Cross-reference Week 2 Risk Heatmap (PHI exposure triggers immediate 25pt RED status).

Initial Defense

Week 4 Kill-Switch alert triggered.

Deployment

Activate Week 6 Crisis Playbook.

Do not attempt to parse dense CPRA/HIPAA legal jargon during an active event. Follow the subsequent chronological triage protocol strictly to avoid $7,500 CPRA fines per undocumented tool.

PHASE 1: CONTAIN

24:00:00

Hour 0 to 24

Stop the bleeding. Isolate the threat, restrict all vendor access, and execute emergency shutdown protocols. Do not wait for complete information to take defensive action.

Hour 0-24 Tactical Checklist

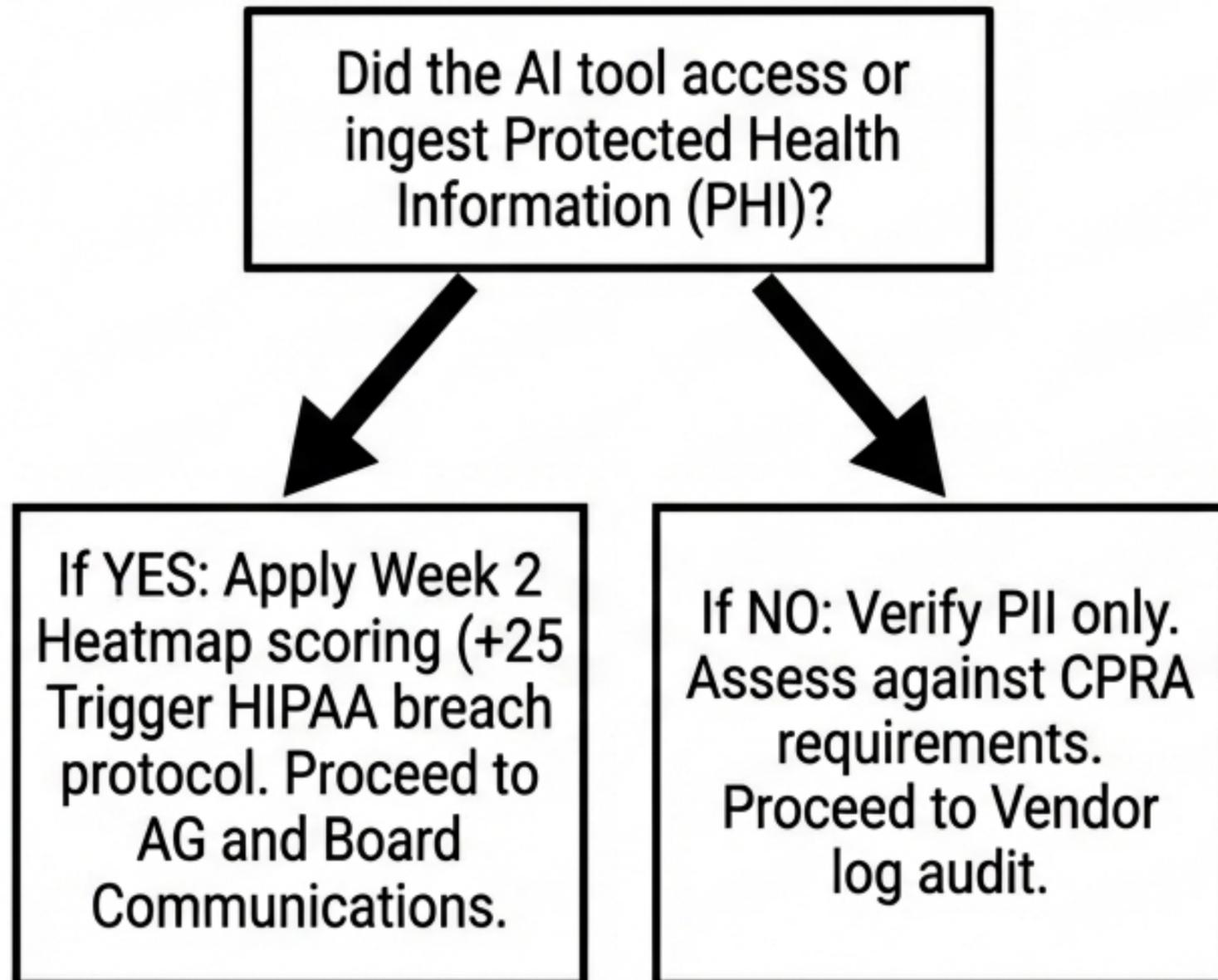|	
☐	**Activate Kill-Switches** Deploy Week 4 Tampermonkey protocol **(if(!localStorage.aiConsent){PAUSE AI})** across affected networks.
☐	**Sever Vendor Access** Immediately revoke API keys and block IP addresses associated with the compromised AI tool.
☐	**Quarantine Data** Lock down databases or servers where unauthorized PHI/PII ingestion is suspected.
☐	**Internal Escalation** Notify IT Lead and newly appointed AI Compliance Officer.
☐	**Halt Automated Decisions** Pause any AI-driven patient scheduling, triage, or diagnostic support tools tied to the breached system.

PHASE 2: INVESTIGATE

Day 1 to 3

Map the exposure. Determine exactly what data was ingested, trace the AI tool's decision pathways, and assess legal liability.

NotebookLM

Day 1-3 Tactical Checklist & Exposure Mapping

PHI Exposure Flowchart

Did the AI tool access or ingest Protected Health Information (PHI)?

If YES: Apply Week 2 Heatmap scoring (+25 Trigger HIPAA breach protocol. Proceed to AG and Board Communications.

If NO: Verify PII only. Assess against CPRA requirements. Proceed to Vendor log audit.

- [ ] **Audit Vendor Logs:** Request and review 30-day activity logs from the AI vendor.
- [ ] **Assess Staff Involvement:** Identify which personnel bypassed Week 3 Consent Banners.
- [ ] **Quantify Scope:** Document the exact number of patient/client records potentially exposed.
- [ ] **Draft Incident Summary:** Compile findings into a preliminary internal timeline.

NotebookLM

PHASE 3: REPORT
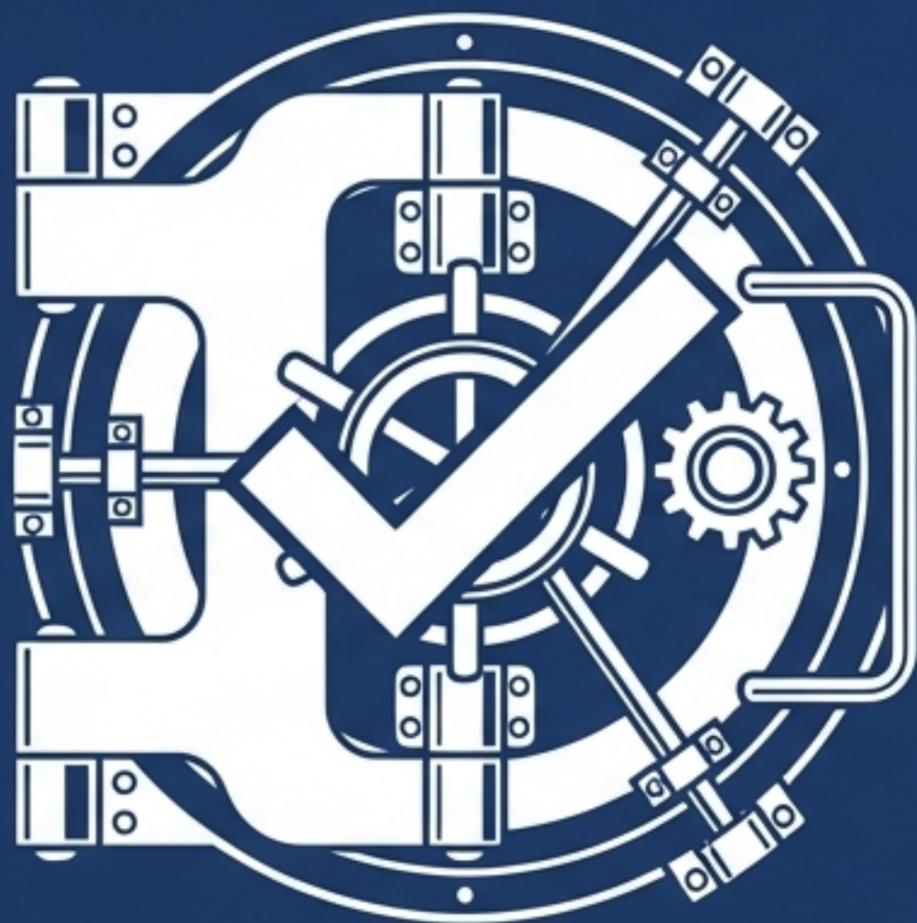
Day 4 to 7

Fulfill regulatory obligations. Deploy targeted communications, update risk architecture, and officially close the incident loop.

Day 4-7 Tactical Checklist

DAY 4

☐ **Deploy Required Notices**
Send legally mandated communications (AG Notice, Board Brief) based on the Phase 2 investigation results.

DAY 5

☐ **Update Week 2 Heatmap**
Re-score the involved AI tool (Likely shifting to RED/100pt status) and document the failure point.

DAY 6

☐ **Retrain Personnel**
Mandate affected staff to retake Week 5 Certification Modules (specifically Module 6: Incident Escalation).

DAY 7

☐ **Finalize Incident Log**
Store the completed operational timeline in the Week 7 Google Sheets Incident dashboard.

NotebookLM

Communication Deployment Matrix

Communication Type	Trigger Phase	Recipient	Legal/Compliance Mandate
Vendor Alert	Phase 1 (0-24H)	External Software Provider	CPRA §1798.185 Right to Audit
Board Brief	Phase 3 (D4-7)	Exec Leadership / Directors	Fiduciary Duty & AI Governance
AG Notice	Phase 3 (D4-7)	CA Attorney General	CPRA/HIPAA Mandatory Breach (Avoids $7.5k fine)
Staff Memo	Phase 3 (D4-7)	Internal Clinic Personnel	Week 5 Internal Policy Enforcement

Comm 1: Vendor Alert Template

URGENT: IMMEDIATE CEASE OF DATA PROCESSING & LOG REQUEST

To **[Vendor Name]** Legal/Security Team:

We have detected unauthorized processing of data originating from **[Clinic/Nonprofit Name]**. Under CPRA mandates and our existing agreements, you are hereby directed to instantly halt all model training or data ingestion involving our account.

Provide complete access logs for the past 30 days within 24 hours to **[Compliance Officer Name]**.

NotebookLM

Comm 2: Board Brief Template

CONFIDENTIAL: AI Governance Incident & Containment Report

Dear Board of Directors,

On **[Date]**, our Week 4 AI tracking protocols detected an anomaly **regarding [AI Tool Name]**. Containment protocols were successfully activated within **[X] hours**.

Our preliminary Phase 2 investigation indicates **[Exposure Level summary]**. The tool has been isolated, and there is no ongoing threat to patient/client operations.

A full regulatory assessment is attached.

Comm 3: Attorney General Notice Template

NOTICE OF DATA INCIDENT / CPRA COMPLIANCE REPORT

To the Office of the Attorney General:

Pursuant to California regulatory requirements, [Clinic/Nonprofit Name] is submitting this notification regarding a contained data incident involving a third-party AI processor, [Vendor Name].

We have executed our **7-Week Zero-Violation** protocol, isolated the third-party system, and verified that protective kill-switches were deployed on [Date].

A detailed log of impacted records (if applicable under HIPAA/CPRA) is enclosed.

NotebookLM

Comm 4: Staff Memo Template Template

IMPORTANT: Updates to AI Software Usage & Compliance

Team, ensuring the privacy of our **[patients/clients]** is our highest mandate.

Effective immediately, access to **[AI Tool Name]** has been suspended pending a compliance review. Please rely on **[Alternative Tool/Process]** until further notice.

Reminder: No unauthorized AI tools may be used for clinical notes or data processing without completing the Week 1 AI Tool Inventory process with the Compliance Officer.

NotebookLM

Week 6 Completion Tracker

Triage Complete
✅ Containment (H0-24)
✅ Investigation (D1-3)
✅ Reporting (D4-7)

Communications Deployed
✅ Vendor
✅ Board
✅ AG
✅ Staff

System Updated
✅ Week 2 Heatmap Adjusted
✅ Week 7 Compliance Log Updated

CRISIS CONTAINED. WEEK 6 COMPLETE ✔.
Playbook ready for integration into the final Week 7 Certified Compliance Officer Dashboard.