# 🧭 Clinical DriftOps Platform — Expanded CPMAI Roadmap (I–VII)

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase (CPMAI)** | **Objective** | **Key Actions / Deliverables** | **Output Example** |
| I. Business Understanding | Define the why — what problem in clinical AI you’re solving and how it ties to compliance or safety. | • Identify 2–3 clinical model use cases prone to drift (e.g., sepsis risk, readmission, medication adherence). • Frame measurable KPIs: false-alert reduction %, drift detection latency, clinician trust scores. • Document regulatory scope (HIPAA, FDA GMLP, EU AI Act). | “Clinical DriftOps Platform Charter” PDF outlining goals, KPIs, stakeholders, and regulatory touchpoints. |
| II. Data Understanding | Audit and benchmark the data environment. | • Pull de-identified clinical tables (MIMIC-IV v2.2 or synthetic FHIR). • Profile historical drift patterns and bias. • Map metadata lineage and bias sources. • (GenAI assist): use LLM to summarize data gaps and surface potential drift correlations. | Jupyter notebook + EvidentlyAI baseline report with PSI and KS tests + GenAI-generated summary of data risk zones. |
| III. Data Preparation | Build the monitoring pipeline. | • Create “baseline vs live” data snapshots in Parquet. • Encode PII-safe transformations. • Implement feature store with version tags. • (GenAI assist): generate data-quality narratives and auto-document schema evolution for audit trails. | data\_prep.py + metadata JSON documenting dataset versioning and PII removal + GenAI-authored Data ReadMe. |
| IV. Model Development | Integrate drift & bias detection models. | • Implement EvidentlyAI drift dashboards. • Add SHAP explainability and bias metrics by race, gender, age. • Containerize with Docker for CI/CD. • (GenAI assist): embed an LLM-based “root-cause explainer” translating drift stats into plain-language insights. | driftops\_service.py microservice with API endpoints for drift, bias, explainability + GenAI summary API for clinicians. |
| V. Model Evaluation | Validate reliability & compliance. | • Define pass/fail thresholds for PSI and AUC degradation. • Build validation dashboard (Streamlit or Grafana). • Conduct bias audits for clinical review. • (GenAI assist): auto-generate plain-language “Trustworthy AI Audit Reports” summarizing bias, drift, and actions. | “Trustworthy AI Audit v1.0” PDF with drift history, bias findings, and GenAI-authored executive summary. |
| VI. Operationalization | Deploy and govern in real time. | • Connect MLflow for model lineage and rollback. • Add regulatory monitor service (“Policy-as-Code”) that flags new FDA/HIPAA changes. • Schedule automated retraining requests with human-in-loop approval. • (GenAI assist): use LLMs to summarize alerts and generate human-readable incident reports. | Live Streamlit dashboard + CI/CD workflow YAML + MLflow artifact registry + GenAI incident summaries. |
| VII. GenAI Compliance Sentinel (Extension) | Continuous regulatory and trust monitoring through LLM automation. | • Deploy RAG-powered agent to monitor FDA, HIPAA, EU AI Act updates. • Map new clauses to affected models via a Compliance Knowledge Graph. • Auto-draft “Regulatory Delta Reports” with impacted policies, teams, and remediation steps. • Maintain human review for approvals and traceability. | GenAI Compliance Sentinel microservice with vector DB for regulatory text + RAG query pipeline + Slack/email alerts + YAML policy updates. |

## ⚖️ Why the GenAI Extension Matters

• Reduces compliance latency — detects regulatory shifts within hours instead of weeks.  
• Enhances explainability — turns drift and bias data into narratives clinicians can trust.  
• Preserves trustworthy AI principles — humans stay in the loop, GenAI handles analysis & drafting.  
• Ensures audit readiness — every LLM output is logged and traceable for regulators.

## 🧩 Clinical DriftOps Platform — GenAI Integration Scorecard

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Current Score** | **Future Target** | **Example Impact** |
| ML Governance & Compliance | 9.5 | 10 | Fully automated audit trails via LLM summaries |
| GenAI Utilization | 5.5 | 9.0 | RAG-based monitoring & LLM explainability layers |
| Trust & Transparency | 9.0 | 9.5 | Auto-generated plain-language regulatory reports |
| Clinical Usability | 8.5 | 9.3 | Clinician-friendly drift narratives & alert summaries |