CIAF + LCM Code Map (One-Page)

A compact reference to wire any AI workflow into CIAF's verifiable lifecycle: **Framework → Wrapper → Dataset Anchor → Model Anchor → Inference Receipt**.

---

1) Objects & Responsibilities

Framework - Purpose: Global governance context (org, jurisdictions, regs, crypto settings) - Holds: registry of policies, keys, evidence store, audit channels - You configure this once per deployment/tenant

Wrapper (Industry Module) - Purpose: Domain guard-rails (sector regs, vocab, defaults) - Adds: sector policies (HIPAA, SOX, EU AI Act…), role gates, PII controls - One per product/domain (e.g., Healthcare, Banking, Defense)

DatasetManager - Purpose: Canonicalize and **anchor** datasets with hashes, lineage, consent - Emits: `dataset_anchor_id` + Merkle proofs - Enforces: data retention, residency, privacy, provenance

ModelManager - Purpose: Build/validate and **anchor** models against dataset anchors - Captures: training config, metrics, explainability artifacts, approvals - Emits: `model_anchor_id` bound to `dataset_anchor_id`

InferenceReceiptManager - Purpose: Issue tamper-evident receipts for every serve/inference - Links: inputs → `model_anchor_id` → outputs → explanations → policy checks - Emits: `inference_receipt_id` (+ selective-disclosure proofs)

---

2) End-to-End Flow (LCM Lifecycle)

```
Framework
  └─ Wrapper (vertical)
      ├─ DatasetManager  ──>  [Dataset Anchor]
      ├─ ModelManager    ──>  [Model Anchor] ──(binds to Dataset Anchor)
      └─ InferenceReceiptManager ──> [Inference Receipt per request]
```

Evidence Chain: Dataset Anchor → Model Anchor → Inference Receipt(s)

---

3) Minimal Integration Pattern (pseudocode)

```
# 1) Context
fw = CIAFFramework(org="Acme", jurisdictions=["US","EU"], crypto="Ed25519")
wrap = HealthcareCIAFWrapper(fw, regs=["HIPAA","EU_AI_ACT"], pii_controls=True)

# 2) Data → Dataset Anchor
dsm = DatasetManager(wrap)
dataset_anchor = dsm.create_dataset_anchor(
    name="rad-imaging-v1",
    sources=["s3://…/dicom"],
    schema_hash="…", consent_map={"PHI": "minimized"}
)

# 3) Model → Model Anchor
mm = ModelManager(wrap)
model_anchor = mm.create_model_anchor(
    name="nodule-detector-r50",
    dataset_anchor_id=dataset_anchor.id,
    train_cfg={"lr":1e-4,"epochs":30},
    metrics={"AUROC":0.94},
    xai=["gradcam"], approvals=["clin board #2025-10-01"]
)

# 4) Serve → Inference Receipt
irm = InferenceReceiptManager(wrap)
receipt = irm.issue(
    model_anchor_id=model_anchor.id,
    input_ref="dicom:study/123",
    output={"risk":"high","bbox":[…]},
    checks=["HIPAA_min","bias_scan","safety_limits"],
)
```

4) Where to Plug In Your Model (by role)

- **Data Scientists:** call `DatasetManager.create_dataset_anchor()` right after dataset freeze; log splits, filters, consent.
- **ML Engineers:** wrap train/eval pipeline to call `ModelManager.create_model_anchor()` on each promoted build; attach metrics & XAI.
- **Platform/Serving:** intercept every predict call to `InferenceReceiptManager.issue()`; persist receipt IDs with business event IDs.
- **Risk/Compliance:** register policies on `Framework/Wrapper`; review anchors & receipts in the evidence store.

5) Vertical-Specific Hooks

- **Healthcare:** DICOM metadata, FDA/IEC artifacts, clinical approvals → added to model anchor & receipts (de-identified views)
- **Banking:** SR 11-7, SOX, model risk tiers; fair-lending metrics; consent/GLBA → dataset & model anchors + decision receipts
- **Insurance:** actuarial justifications, underwriting thresholds; consumer notice receipts
- **Retail:** consent & preference flags; FTC transparency; recommendation diversity metrics
- **Defense/Gov:** export/ITAR tags; chain-of-custody; FOIA-ready redactions & selective disclosures

---

6) Policy/Control Surfaces

- **Framework.register_policy(...)** → global (e.g., EU AI Act Art. 10 data governance)
- **Wrapper.defaults(...)** → sector presets (HIPAA min-necessary, PHI masking)
- **Manager hooks:** pre/post validators (schema locks, bias gates, redaction)

---

7) Evidence & Crypto

- All anchors/receipts are hashed; parents/children form a metadata-Merkle tree
- Sign with org keys; publish roots to your ledger or WORM store
- Selective proof generation enables least-privilege audits

---

8) What “Good” Looks Like

- No model runs without a bound **model anchor**
- No prediction exits without an **inference receipt**
- Every anchor/receipt references active policies and passes validators
- Evidence is reproducible, tamper-evident, and regulator-ready

Use this map as your checklist when onboarding a new model or vertical.