MCP for Pryima: A Governance-Ready Protocol for Safe, Auditable Tool Use in Precision Health

Pryima Research Series · September 2025
Authors: Pryima Intelligence Lab

Abstract

Transformer-class LLMs excel at reasoning over text, but real-world healthcare requires more than raw language capability. Systems must **safely call tools, fetch and ground context, preserve privacy, and produce audit-ready outputs** across a shifting landscape of EHRs, labs, wearables, and patient-reported data. Ad-hoc integrations are brittle and non-verifiable. This paper outlines **Pryima's adoption of the Model Context Protocol (MCP)** as the core interface for tools, memory, and retrieval—turning a capable model into a **governance-ready clinical assistant**. We describe how MCP standardizes tool discovery and invocation, enforces **capability-scoped permissions**, and yields **structured provenance** suitable for HIPAA environments and rigorous quality management.

> **Thesis:** MCP turns "tool-using LLMs" into **policy-enforced, auditable systems** by separating what the model *can* do (capabilities), what it *may* do (policy), and what it *did* (traceable evidence).

Why MCP (Model Context Protocol) for Pryima

Healthcare AI must meet four hard constraints simultaneously: **privacy**, **safety**, **reliability**, and **regulatory auditability**. MCP addresses each by design.

- **Standardized Tooling:** A uniform way for assistants to **discover, describe, and call tools** (EHR fetch, lab ordering, biosensor import, cohort analytics) via MCP "servers," avoiding one-off adapters.
- **Capability Security: Least-privilege capability tokens** and human/automated policy checks ensure a tool is only used with allowed parameters and scopes.
- **Context & Memory:** Structured retrieval (RAG) plus **tiered memory** (ephemeral, session, governed durable) to avoid long-term PHI leakage and enable selective forgetting.

- **Provenance-by-Default:** Every call yields **signed traces** (inputs, outputs, model prompts, tool schemas, policy decisions), enabling **post-hoc review**, incident analysis, and CFR-11-style records.

Pryima's MCP Topology (Overview)

- **MCP Assistant:** Orchestrates reasoning, calls tools via MCP servers, and enforces conversation-level policies.
- **MCP Tool Servers (Zero-Trust Boundaries):**
    1. **Clinical Data Server:** read-only EHR, FHIR APIs, claims; PHI gatekeeping.
    2. **Biometrics Server:** Dexcom/CGM, wearables, EMG, sleep, HRV, load.
    3. **Bioinformatics Server:** pipelines for labs, omics, reference ranges, derived features.
    4. **Cohort Analytics Server:** de-identified aggregates for research/ops.
    5. **Communications Server:** templated, approved patient/provider messaging.
- **Policy & Verification Layer:** pre-/post-conditions, **guardrails for contraindications**, safety classifiers, and human-in-the-loop stops.
- **Audit & Governance Bus: tamper-evident traces** to secure storage; real-time dashboards for compliance and quality.

[PASTE FIGURE HERE]
Figure 1. Pryima's MCP-orchestrated health-intelligence stack with PHI boundaries, policy checks, and provenance streams.

Design Objectives (Clinical-Grade)

1. **Safety-by-Design:** hard stops on risky actions; verified tool schemas; unit tests for prompts/tools.

2. **Privacy First:** PHI minimization, scoped redaction, differential access by role, **on-prem/edge options**.

3. **Reliability:** idempotent, observable tool calls; retries with backoff; SLOs for latency/availability.

4. **Auditability:** cryptographically signed **execution traces**; evidence packages for reviews and incidents.

5. **Interoperability:** FHIR, HL7, and common wearable SDKs wrapped as MCP tools; future-proof to vendor churn.

Contributions (This Work)

- A reference **MCP topology for HIPAA-aware environments** in precision wellness and bioinformatics.

- A **capability model** mapping clinical tasks (e.g., CGM import, lab interpretation, protocol drafting) to least-privilege tools.

- A **tiered memory architecture** separating ephemeral reasoning from governed durable context.

- A **verification flow** that pairs policy checks with human attestation for high-impact actions.

- An **audit & provenance schema** aligned with internal quality management and external review needs.

---

1. Problem Context: Fragmented Tools, High Stakes

Pryima operates at the intersection of **AI, bioinformatics, precision health, and real-time physiological monitoring**. The platform must ingest structured EHR data, continuous wearable signals, and lab results; reason about them; and draft **clinically sensible, compliance-ready** outputs. Without a protocol, tool use becomes opaque, permissions sprawl, and auditing is after-the-fact. **MCP replaces bespoke glue with a principled, reviewable contract** between models, tools, and policy—so every recommendation carries a verifiable trail.

Keywords: Model Context Protocol, tool orchestration, HIPAA, provenance, verification, RAG, bioinformatics, precision health.