REQUEST FOR PROPOSAL (RFP)

Analytics & Decision Intelligence Platform for Healthcare Cost and Utilization Insights

---

1. Issuing Organization

Organization Name:
HelixQuant Health Analytics, Inc.

Company Stage:
Growth-stage healthcare analytics startup (Series B)

Headquarters:
United States (Remote-first organization)

RFP Reference ID:
HQHA-RFP-2026-ANL-004

Issue Date:
April 2026

---

2. Organizational Background

HelixQuant Health Analytics, Inc. is a healthcare analytics company focused on enabling payers, providers, and employer groups to better understand healthcare cost drivers, utilization patterns, and performance variation across populations.

The organization operates exclusively in the **analytics and decision-support domain** and does not develop or deploy clinical decision systems, electronic health records, or patient-facing medical software.

HelixQuant's core mission is to transform complex healthcare data into **clear, explainable, and actionable insights** that support operational planning, cost management, and equity-focused analysis.

3. Purpose of This RFP

The purpose of this Request for Proposal is to engage a qualified vendor to design, implement, and support a **healthcare analytics and decision intelligence platform** that will serve as a foundational component of HelixQuant's internal analytics operations and client-facing reporting capabilities.

This engagement is intended to be a **time-bound consulting and delivery engagement**, focused on rapid value realization, knowledge transfer, and extensibility.

---

4. Engagement Overview

4.1 High-Level Summary

Attribute	Description
Engagement Type	Analytics platform design and implementation
Delivery Model	Remote-first
Contract Duration	4 months
Estimated Start Date	June 2026
Estimated Budget Range	USD 100,000 – 125,000
Cloud Environment	AWS (preferred) or Azure
Data Sensitivity	De-identified / aggregated healthcare data

---

5. Scope of Work (DELIVERY REQUIREMENTS)

Only the requirements explicitly stated in this section constitute delivery obligations.

5.1 Data Ingestion & Management

The vendor shall design and implement data ingestion pipelines capable of handling structured healthcare analytics datasets in a scalable, reliable, and auditable manner.

5.1.1 Supported Data Types

The system must support ingestion of the following data domains:

Data Domain	Description
Claims Summaries	Aggregated medical and pharmacy claims
Utilization Records	Encounter-level utilization summaries
Provider Metadata	Provider and facility reference data
Geographic Attributes	Regional and market-level indicators
Demographic Attributes	Age bands, gender, payer category

5.1.2 Data Volume & Frequency

Attribute	Requirement
Annual Record Volume	~8–12 million records
Update Frequency	Monthly
Historical Backfill	Up to 24 months

5.1.3 Data Management Requirements

- Data ingestion must be reproducible and idempotent.
- Validation checks must detect schema violations, missing fields, and duplicate records.

- Normalization logic must be documented and versioned.
- Published datasets must remain immutable after release.
- All analytical outputs must be traceable to a specific dataset version.

5.2 Analytics & Benchmarking Capabilities

The platform must support configurable healthcare analytics and benchmarking across cost, utilization, and performance dimensions.

5.2.1 Cost & Utilization Analytics

The system shall support:

- Cost trend analysis across multiple time horizons.
- Utilization rate calculations by service category.
- Cost-per-utilization metrics.
- Comparative benchmarks across defined cohorts.

5.2.2 Stratified Analysis

Analytics must support stratification across:

Dimension	Examples
Geography	Region, market
Payer Category	Commercial, Medicare Advantage
Demographics	Age band, gender
Provider Grouping	Facility type, specialty group

5.2.3 Trend & Pattern Identification

The analytics layer must enable:

- Identification of statistically significant deviations from historical trends.
- Detection of emerging utilization or cost patterns.
- Explainable representations of observed changes.

5.2.4 Analytics Requirements

- All benchmarks must be parameterized and configurable.

- Analytical logic must be explainable and documented.
- Outputs must be reproducible given identical inputs and configurations.

5.3 Reporting & Visualization

The vendor shall deliver reporting capabilities suitable for both internal analysts and external stakeholders.

5.3.1 Reporting Outputs

The platform must provide:

- Interactive dashboards for exploratory analysis.
- Exportable reports in common formats (CSV, PDF).
- Visual summaries suitable for executive review.

5.3.2 Reporting Requirements

- All reported values must be traceable to source data.
- Visualizations must reflect underlying analytical definitions consistently.
- Methodology changes must be versioned and documented.

5.4 Decision-Support (Non-Clinical)

The platform may include decision-support features intended to support business and operational planning.

Explicit constraints:

- The system must not generate clinical recommendations.
- Outputs must be descriptive rather than prescriptive.
- Assumptions and limitations must be clearly disclosed.

5.5 Knowledge Transfer & Enablement

The vendor shall provide:

- Technical documentation covering data models and analytics.
- Knowledge-transfer sessions for HelixQuant analysts.
- Guidance on extending analytics and reports post-engagement.

6. In-Scope vs Out-of-Scope

6.1 In-Scope

Included
Analytics platform implementation
Healthcare cost and utilization analysis
Dashboards and reporting
Documentation and knowledge transfer

6.2 Out-of-Scope

Excluded
Clinical decision support
EHR system development
Patient-facing applications
Ongoing managed services beyond contract

7. Security & Compliance Expectations

HelixQuant Health Analytics, Inc. places a high priority on information security, data protection, and operational integrity commensurate with the sensitive nature of healthcare analytics data and the trust placed in the organization by its partners and clients.

Vendors responding to this RFP are expected to demonstrate a **mature, risk-aware approach to security and compliance**, aligned with widely recognized industry standards and best practices.

7.1 Information Security Governance

The vendor should maintain an established information security program that:

- Defines roles and responsibilities for information security oversight;
- Incorporates documented security policies and procedures;
- Includes mechanisms for periodic review and continuous improvement;
- Supports accountability and traceability for security-related decisions.

Alignment with **ISO 27001 or equivalent information security frameworks** is strongly preferred.

7.2 Access Control and Identity Management

The solution must implement appropriate access control mechanisms to ensure that system access is granted strictly on a need-to-know basis.

Expectations include:

- Role-based access control (RBAC) aligned to functional responsibilities;
- Segregation of duties between administrative, development, and analytical roles;
- Secure authentication mechanisms for all system users;
- Timely provisioning and de-provisioning of user access.

Access controls must be consistently enforced across environments.

7.3 Auditability, Logging, and Monitoring

The platform should provide sufficient observability to support operational oversight, troubleshooting, and audit review.

This includes:

- Logging of authentication and access events;
- Logging of data access and analytical execution where appropriate;
- Retention of logs for a reasonable and defined period;
- Monitoring mechanisms to detect anomalous or unauthorized activity.

Audit logs must be protected from unauthorized modification and accessible to authorized personnel for review.

7.4 Data Protection and Privacy

The vendor must demonstrate the ability to handle healthcare data responsibly throughout its lifecycle.

Expectations include:

- Secure handling of **de-identified and aggregated healthcare data**;
- Protection of data at rest and in transit using industry-standard encryption mechanisms;
- Controls to prevent unauthorized data access, exfiltration, or misuse;
- Clear data handling practices covering ingestion, processing, storage, and disposal.

The solution must be designed to support privacy-preserving analytics and avoid re-identification risk.

7.5 Secure Development and Operations

The vendor should employ secure engineering and operational practices, including:

- Secure configuration of cloud infrastructure and services;
- Use of automated deployment and environment isolation where applicable;
- Monitoring and remediation of security vulnerabilities;
- Defined incident response and escalation procedures.

Operational security practices should be appropriate for a cloud-native analytics environment.

7.6 Compliance Posture and Assurance

Formal third-party security certifications are **not mandatory** for this engagement.

However, vendors must be able to:

- Describe how their security controls align with recognized frameworks (e.g., ISO 27001, SOC-style controls);
- Provide evidence of equivalent internal controls upon request;
- Participate in reasonable security review or due-diligence activities as part of the engagement.

The emphasis is on **effective controls and transparency**, rather than certification for its own sake.

7.7 Ongoing Responsibility

Security and compliance are expected to be treated as **ongoing responsibilities**, not one-time activities.

Vendors should demonstrate a commitment to:

- Maintaining security posture over the duration of the engagement;
- Adapting controls as system usage and requirements evolve;
- Communicating material security issues in a timely and responsible manner.

8. Timeline & Milestones

Milestone	Description	Target
Project Kickoff	Scope confirmation and planning	Week 1
Data Ingestion Complete	Pipelines operational	Week 5
Analytics Layer Ready	Core benchmarks implemented	Week 9
Dashboards Delivered	Reporting and visualization	Week 13
Knowledge Transfer	Documentation and handover	Week 16

9. Success Criteria

The engagement will be considered successful if:

- Data ingestion pipelines operate reliably with monthly updates.
- Core analytics are delivered on schedule and meet documented definitions.
- Dashboards support both exploratory and executive use.
- HelixQuant analysts are able to operate and extend the system independently.

10. Vendor Qualifications (ELIGIBILITY REQUIREMENTS)

Vendors must demonstrate:

- Experience delivering analytics or data platforms in healthcare or regulated domains.
- Capability to handle sensitive, non-public datasets responsibly.
- Proven experience delivering cloud-native analytics solutions.
- Ability to support a time-bound, high-impact delivery engagement.

11. Risks & Assumptions

Risk	Mitigation
Data availability delays	Early validation and phased ingestion
Evolving analytics definitions	Parameterized and versioned benchmarks
Stakeholder alignment	Regular review checkpoints

12. Proposal Response Instructions

- Proposals must include a technical approach and commercial summary.
- Responses must be submitted electronically.
- Clarification questions may be submitted prior to the response deadline.

13. Reservation of Rights

HelixQuant Health Analytics, Inc. reserves the right to modify, suspend, or cancel this RFP and to negotiate scope, pricing, and timelines with selected vendors.