REQUEST FOR PROPOSAL (RFP)

Autonomous Analytics & Decision Intelligence Platform for Public Health Performance Benchmarking

---

1. Issuing Authority

Organization Name:
National Health Outcomes & Policy Council (NHOPC)

Type:
Independent public health oversight and analytics body operating under statutory mandate

Geographic Scope:
National (multi-state data coverage)

RFP Reference Number:
NHOPC-RFP-2026-DAI-017

Issue Date:
15 March 2026

Proposal Submission Deadline:
30 April 2026, 17:00 UTC

---

2. Background & Context

The National Health Outcomes & Policy Council (NHOPC) is responsible for monitoring, analyzing, and publicly reporting on healthcare system performance across cost, quality, access, and equity dimensions.

NHOPC oversees multi-year benchmarking initiatives designed to:

- assess healthcare cost growth trends,
- evaluate utilization and efficiency patterns,
- measure equity outcomes across demographic and socioeconomic dimensions,

- inform policy interventions and regulatory actions.

NHOPC currently manages large-scale, multi-source healthcare datasets, including claims, encounter summaries, provider metadata, and population indicators. While significant data assets exist, analytical workflows are fragmented, slow to adapt, and heavily dependent on manual processes.

NHOPC seeks a qualified vendor to design, implement, and operate an **analytics and decision-support platform** that enables continuous, transparent, and auditable healthcare benchmarking.

---

3. Objectives of This RFP

The primary objectives of this engagement are:

1. To design and implement a **healthcare analytics platform** capable of supporting cost, quality, and equity benchmarking.
2. To enable **repeatable, explainable, and auditable analytical workflows** suitable for public reporting.
3. To provide **decision-support insights** for policymakers without engaging in clinical decision-making.
4. To ensure **long-term sustainability**, knowledge transfer, and operational continuity.

---

4. Scope of Work (DELIVERY REQUIREMENTS)

> ⚠️ **Important:**
> Only the requirements explicitly stated in this section constitute delivery obligations. Proposal formatting, submission instructions, certifications, or administrative clauses elsewhere in the RFP must **not** be interpreted as delivery requirements.

4.1 Data Ingestion & Data Management

The vendor shall design, implement, and maintain a robust, scalable, and auditable data ingestion and management layer that serves as the foundation for all downstream analytics and reporting.

The ingestion system must be capable of handling **large-scale, longitudinal healthcare datasets** originating from multiple sources and evolving over time.

4.1.1 Supported Data Domains

The ingestion pipelines shall support structured and semi-structured healthcare datasets, including but not limited to:

a) Claims and Financial Data

- Medical claims summaries
- Pharmacy claims summaries
- Allowed amounts, paid amounts, member cost-sharing fields
- Claim adjudication status indicators
- Service dates, submission dates, and payment dates

b) Utilization and Encounter Data

- Encounter-level utilization summaries
- Service category indicators (e.g., inpatient, outpatient, emergency)
- Procedure and service groupings
- Volume and frequency indicators

c) Provider and Facility Metadata

- Provider identifiers (hashed or anonymized as required)
- Facility identifiers and attributes
- Provider specialty classifications
- Facility type and ownership indicators

d) Member, Geographic, and Demographic Attributes

- Age bands and gender indicators
- Geographic attributes (state, county, region, urban/rural classification)
- Socioeconomic indicators where available
- Race and ethnicity categories (aggregated and privacy-preserving)
- Insurance and payer classifications

4.1.2 Ingestion Scale & Performance

The data ingestion architecture must:

- Support ingestion volumes of **tens of millions of records per year**, with the ability to scale beyond this threshold as data availability expands.
- Handle both:
    - batch ingestion (e.g., monthly or quarterly submissions), and
    - incremental ingestion (e.g., periodic updates or corrections).
- Support ingestion of historical backfills without disrupting active analytical workflows.

4.1.3 Validation & Quality Assurance

The vendor shall implement automated data validation mechanisms to ensure data integrity and consistency prior to downstream use.

Validation processes must include, at minimum:

- Schema validation (required fields, data types, constraints)
- Referential integrity checks across datasets
- Range and sanity checks for numeric fields
- Detection of missing, duplicate, or anomalous records
- Version-to-version consistency checks

Validation outcomes must be recorded and made available for audit and review.

4.1.4 Normalization & Standardization

The ingestion layer shall normalize incoming data to standardized internal representations, including:

- Harmonization of coding systems and categorical values
- Standardization of date and time representations
- Consistent handling of null, missing, or suppressed values
- Alignment of historical data to current schema versions where feasible

Normalization logic must be explicitly documented and versioned.

4.1.5 Versioning, Lineage, and Provenance

The system must provide full transparency into how data enters, evolves, and is consumed within the platform.

The vendor shall:

- Implement dataset versioning to track changes across ingestion cycles
- Maintain data lineage linking analytical outputs back to:
    - source files,
    - ingestion timestamps,
    - transformation steps,
    - validation results
- Enable auditors and analysts to reconstruct analytical outputs from specific data versions

---

4.1.6 Atomic Data Ingestion Requirements

The following requirements are **mandatory and atomic**:

1. **Reproducibility**
    - Given the same source data and configuration, ingestion must produce identical outputs.
2. **Idempotency**
    - Re-ingesting the same dataset must not create duplicate records or inconsistent state.
3. **Fault Tolerance**
    - Failed ingestion events must:
        - be logged with sufficient diagnostic detail,
        - support targeted retries without full reprocessing.
4. **Immutability**
    - Once a dataset version is published for analytical use, it must remain immutable.

- Corrections must result in a **new version**, not overwriting prior data.

4.2 Analytics & Benchmarking Capabilities

The vendor shall implement an analytics layer capable of supporting **repeatable, explainable, and policy-relevant healthcare benchmarking** across cost, utilization, and equity dimensions.

The analytics framework must support both scheduled reporting and exploratory analysis by authorized users.

4.2.1 Cost Growth Benchmarking

The platform must support cost benchmarking across multiple temporal and analytical perspectives, including:

- Year-over-year cost growth
- Multi-year rolling averages
- Trend comparisons against baseline periods
- Cost growth stratified by service category and payer type

Cost calculations must be clearly defined, documented, and consistently applied.

4.2.2 Utilization and Efficiency Metrics

The analytics system shall compute utilization and efficiency indicators, including but not limited to:

- Service utilization rates
- Encounter frequency metrics
- Cost per utilization unit
- Relative efficiency indicators across comparable cohorts

Metrics must support aggregation at multiple levels (e.g., regional, payer, provider category) without exposing sensitive individual-level data.

4.2.3 Stratified and Equity-Focused Analysis

The platform must enable stratified analytics to support equity assessment and transparency.

Stratifications must include:

- Race and ethnicity categories (aggregated)
- Income or socioeconomic proxies
- Geographic groupings
- Insurance and coverage categories

The system must support comparisons across stratifications while ensuring privacy-preserving aggregation.

4.2.4 Trend Detection and Anomaly Identification

The analytics layer must support detection of:

- Significant deviations from historical trends
- Outliers in cost or utilization patterns
- Emerging patterns that may warrant further investigation

Trend and anomaly detection methods must be explainable and reproducible.

4.2.5 Analytical Configuration & Parameterization

The analytics framework must be configurable to accommodate evolving policy definitions and benchmarks.

At a minimum:

- Benchmark thresholds must be parameterized, not hard-coded.
- Time windows and aggregation rules must be adjustable.
- Changes to parameters must be versioned and auditable.

4.2.6 Explainability and Documentation

All analytical logic must be transparent and explainable.

The vendor shall:

- Document calculation methodologies in clear, non-proprietary language.

- Describe assumptions, limitations, and known edge cases.
- Enable analysts to trace reported values back to underlying data and formulas.

4.2.7 Atomic Analytics Requirements

The following requirements are **mandatory and atomic**:

1. **Reproducibility**
    - Given identical inputs, configurations, and parameters, analytics outputs must be identical.
2. **Configurability**
    - Benchmarks and thresholds must be adjustable without code changes.
3. **Explainability**
    - All metrics must be explainable to non-technical stakeholders.
4. **Auditability**
    - Analytical outputs must be traceable to specific data versions and configurations.

4.3 Interdependency Between Ingestion and Analytics

The vendor must ensure tight coupling between ingestion and analytics layers such that:

- Analytics cannot execute on partially validated or unpublished datasets.
- Each analytical output references:
    - dataset version,
    - ingestion timestamp,
    - parameter configuration version.
- Corrections in source data result in controlled re-analysis rather than silent drift.

4.4 Explicit Non-Clinical Boundary (Delivery Constraint)

The system delivered under this scope must **not**:

- Provide clinical diagnoses or treatment recommendations.
- Replace clinician judgment.
- Be marketed or represented as a clinical decision-support system.

All analytics are intended for **policy, oversight, and operational planning** purposes only.

4.3 Equity & Transparency Analysis

The vendor shall implement equity-focused analyses designed to surface disparities without attributing causality.

Atomic Requirements:

- Equity metrics must be computed consistently across reporting periods.
- Aggregations must avoid re-identification risks.
- Equity analyses must be separable from cost-only analyses.

4.4 Reporting & Visualization

The system must provide:

- Interactive dashboards for internal analysts.
- Exportable reports for public dissemination.
- Visualizations suitable for non-technical stakeholders.

Atomic Requirements:

- All reported figures must be traceable to underlying datasets.
- Changes to methodology must be versioned and documented.
- Dashboards must support filterable views without altering base data.

4.5 Decision-Support (Non-Clinical)

The platform may include decision-support features intended for **policy and operational planning**, not clinical use.

Explicit Boundary:

- The system must **not** provide clinical recommendations, diagnoses, or treatment guidance.

Atomic Requirements:

- Decision-support outputs must be descriptive, not prescriptive.
- Assumptions and limitations must be clearly surfaced.

4.6 Knowledge Transfer & Enablement

The vendor shall:

- Provide documentation for data models, analytics, and workflows.
- Conduct structured knowledge-transfer sessions.
- Enable NHOPC analysts to operate and extend the system.

---

5. Technical Environment & Constraints

5.1 Cloud Environment

- The preferred deployment environment is **Microsoft Azure**.
- Equivalent cloud architectures may be proposed with justification.

5.2 Security & Compliance

The solution must align with:

- ISO 27001-aligned security practices,
- data privacy principles consistent with HIPAA and GDPR,
- role-based access controls,
- audit logging and access traceability.

---

6. Engagement Structure & Timeline

6.1 Contract Duration

- Initial term: **5 years**
- Optional extensions: **up to 2 additional years**

6.2 Delivery Model

- Incremental delivery with quarterly milestones.
- Continuous analytics updates rather than fixed “end-state” delivery.

---

7. Vendor Qualifications (ELIGIBILITY REQUIREMENTS)

Vendors responding to this Request for Proposal must demonstrate organizational maturity, technical depth, and operational credibility commensurate with the complexity, sensitivity, and public accountability associated with this engagement.

The issuing authority seeks partners with a proven track record of delivering **enterprise-scale analytics and data-driven systems** within environments characterized by regulatory oversight, high data volumes, and evolving policy requirements.

7.1 Enterprise Analytics Delivery Experience

Vendors must provide evidence of prior experience designing, implementing, and operating **large-scale analytics platforms** that:

- Support complex, multi-dimensional analytical workloads;
- Process high-volume, longitudinal datasets;
- Enable repeatable and auditable analytical outcomes;
- Serve diverse stakeholder groups, including technical and non-technical users.

Demonstrated experience should reflect an ability to move beyond proof-of-concept solutions and deliver **production-grade, mission-critical systems**.

7.2 Domain Experience in Regulated and Public Environments

Vendors must demonstrate prior engagement within one or more of the following domains:

- Healthcare and health-related analytics environments;
- Public sector or quasi-governmental organizations;
- Highly regulated industries subject to formal compliance, audit, and reporting requirements.

Experience in these domains should reflect familiarity with:

- regulatory constraints,
- procurement and governance processes,
- heightened expectations around transparency, accountability, and risk management.

7.3 Data Sensitivity, Privacy, and Security Capability

Vendors must demonstrate the organizational capability to responsibly manage **sensitive, non-public, and restricted-access datasets**.

This includes experience with:

- data privacy and confidentiality controls;
- secure handling of regulated or protected information;
- access control, logging, and auditability mechanisms;
- alignment with recognized information security and data protection frameworks.

Vendors should be able to articulate processes for safeguarding data across its full lifecycle, from ingestion through analysis and reporting.

7.4 Cloud-Native Delivery and Operational Excellence

Vendors must demonstrate proven experience delivering **cloud-native solutions** using modern architectural principles, including:

- scalable and resilient infrastructure design;
- automated deployment and operational workflows;
- environment isolation and role-based access control;
- monitoring, observability, and incident response practices.

Cloud delivery experience should reflect an ability to operate systems reliably over extended periods, adapt to evolving requirements, and maintain service continuity under changing demand conditions.

7.5 Organizational Readiness and Sustainability

Vendors must demonstrate sufficient organizational capacity and stability to support a **multi-year engagement**, including:

- availability of appropriately skilled personnel;
- continuity planning and knowledge retention practices;
- governance structures to manage risk and stakeholder engagement.

The issuing authority seeks partners capable of functioning as **long-term collaborators**, not solely short-term implementation resources.

Classification Note (for internal evaluation)

The requirements in this section are **eligibility and qualification criteria only**.
They do not constitute delivery obligations and must not be evaluated as technical implementation requirements.

---

8. Explicit Exclusions

The following are **out of scope**:

- Clinical decision support systems.
- Medical device software.
- Electronic Health Record (EHR) core system development.
- Patient-facing clinical applications.

---

9. Evaluation Criteria

Proposals will be evaluated based on:

1. Technical approach and architecture.
2. Demonstrated analytics and data engineering capability.
3. Experience with compliance-aware systems.
4. Risk identification and mitigation strategy.
5. Ability to support long-term, evolving programs.

---

10. Proposal Submission Instructions (PROCEDURAL)

⚠️ This section is **procedural only** and must not affect delivery feasibility scoring.

- Proposals must be submitted electronically in PDF format.
- Submissions must include a technical proposal and pricing summary.
- All questions must be submitted via email by the clarification deadline.

---

11. Budget & Commercial Considerations

- Vendors may propose pricing models including:
    - time-and-materials,
    - fixed-price components,
    - hybrid structures.
- NHOPC seeks value-based proposals aligned with long-term sustainability.

---

12. Risk & Governance Expectations

Vendors are expected to:

- Identify delivery, data, and operational risks.
- Propose mitigation strategies.
- Participate in joint governance and review forums.

---

13. Clarifications & Assumptions

Vendors should explicitly state:

- key assumptions,
- dependencies,
- areas requiring clarification.

NHOPC reserves the right to seek clarification without penalty.

---

14. Reservation of Rights

NHOPC reserves the right to:

- accept or reject any proposal,

- negotiate scope and pricing,
- modify timelines,
- cancel this RFP without award.
