

Financial Planning & Analysis Platform

Horizon Behavioral Health

RFP Information	Details
RFP issue date	October 1, 2026
Questions	Questions are due no later than October 15, 2026, 5:00 PM EST. Questions are to be sent by e-mail to purchasing@horizonbh.org . Questions must contain "RFP 16972" in the subject line
Proposal due	October 23, 2026, 5:00 PM EST
Submission method	Submissions may be made either by PDF delivery via e-mail to purchasing@horizonbh.org or physical delivery to 2241 Langhorne Rd, Lynchburg VA 24501, Attn: Purchasing. In either case, submissions must be marked "RFP 16972"
RFP contact	Purchasing@horizonbh.org

1. Organization and Procurement Overview

Horizon Behavioral Health (Horizon) invites qualified vendors to submit proposals for a financial planning and analysis (FP&A) platform. Horizon is a behavioral health organization with approximately 600 employees and approximately \$40 million in annual revenue.

We anticipate the need for 20 users consisting of seven (7) Finance department staff who will utilize the system daily, ten (10) managerial users who will access the system monthly for program financial reviews and semi-annually for budget and forecast revisions, and three (3) Horizon IT resources to provide system support.

Horizon currently uses ADP for payroll and human resources, Credible Behavioral Health as its electronic health record (EHR), and MIP Fund Accounting as its accounting system. Horizon seeks an Excel-centered platform that can combine financial, workforce, and operational data in a secure and governed environment.

2. Project Objectives

- Replace fragmented spreadsheet consolidation with a controlled planning process while retaining Excel as a primary user interface.
- Integrate MIP actuals, ADP workforce/payroll data, and Credible operational data into a common dimensional model.
- Support budgeting and forecasting by department, program, location, service line, payer, funding source, and workforce dimension, as applicable.
- Allow managers to participate in planning without exposing employee-level compensation or data outside their authorized scope.
- Enable rolling forecasts, scenario analysis, workforce planning, revenue modeling, and actual-to-budget and actual-to-forecast reporting.
- Provide a solution that Horizon Finance can administer with limited ongoing reliance on IT resources or vendor consulting.

3. Proposal Preparation and Response Instructions

Respondents must provide a complete response organized in the order below. A response that refers only to marketing materials or states that a capability is available without explaining how it will be delivered may be treated as nonresponsive.

Executive summary and proposed solution.

Company qualifications, relevant experience, and customer references.

Completed functional requirements response.

Completed integration response for ADP, MIP Fund Accounting, and Credible Behavioral Health.

Completed Security, Privacy & Controls response, including requested evidence and all exceptions.

Implementation approach, timeline, staffing, responsibilities, training, and support.

Completed pricing response and three-year total cost of ownership.

Exceptions, assumptions, dependencies, and requested contract terms.

3.1 Capability Response Codes

For each functional, integration, and security requirement, use one of the following response codes and provide the requested explanation:

Code	Meaning	Required Explanation
Native	Included as a standard product capability.	Identify the module and describe how Horizon would use it.
Configurable	Available through configuration without custom code.	Describe configuration, responsible party, timing, maintenance, and cost.
Custom	Requires custom development or scripting.	Describe design, responsible party, testing, maintenance, upgrade impact, timing, and cost.
Third Party	Requires another product, service, or middleware provider.	Identify the provider, contractual relationship, data flow, responsibilities, risks, and all one-time and recurring costs.
Roadmap	Not currently available but planned.	State committed availability date and whether the commitment will be contractual. Roadmap items will not be treated as current capabilities.
Not Available	Cannot meet the requirement.	Describe any alternative approach or limitation.

4. Functional and Integration Requirements

4.1 Functional Requirements

For each requirement, provide the response code, a concise explanation of how the proposed solution meets the requirement, the module or component used, implementation assumptions, and any one-time or recurring cost not included in the base proposal.

ID	Area	Requirement	Priority	Respondent Response
F-01	Excel & usability	Provide an Excel add-in or Excel-native planning and reporting experience that preserves familiar formulas and workflows where practical.	Critical	
F-02	Excel & usability	Provide a short learning curve for Finance users and occasional budget owners; describe navigation, training needs, and use outside Excel.	Critical	

ID	Area	Requirement	Priority	Respondent Response
F-03	Planning	Support annual budgets, rolling forecasts, scenario and version management, driver-based planning, allocations, and top-down and bottom-up planning.	Critical	
F-04	Workforce planning	Model employee/FTE, position, vacancy, wage, benefits, payroll taxes, start/end dates, merit, and other compensation assumptions.	Critical	
F-05	Behavioral health modeling	Model operational drivers including clinician FTE, available hours, utilization, encounters/services, units, payer, program, location, and reimbursement assumptions.	Critical	
F-06	Reporting	Provide actual-to-budget and actual-to-forecast reporting, departmental/program P&Ls, variance analysis, management reporting, and drill-down.	Critical	
F-07	Workflow	Support budget submissions, approvals, task status, comments, audit history, locking, and version controls.	High	
F-08	Administration	Allow Horizon Finance to maintain dimensions, mappings, reports, and models with limited vendor dependence.	High	

4.2 Required Data Integrations

The respondent must propose a specific, supportable architecture for each source system. Generic statements such as “we have an API” or “we can integrate with any system” are insufficient. For each integration, identify the extraction method, data movement path, refresh process, responsible party, monitoring and reconciliation controls, error handling, security, maintenance, dependencies, implementation schedule, and all one-time and recurring costs.

ID	System	Required Data	Information the Respondent Must Provide
I-01	ADP	Employee/position identifiers; department/program; status; FTE; wages; benefits; payroll taxes; hire/termination dates; and other workforce-planning fields.	Identify connector/API/file method; available fields; refresh frequency; field-level restrictions; historical load; mapping; reconciliation; error handling; implementation ownership; prior ADP experience; and cost.
I-02	MIP Fund Accounting	GL actuals and relevant dimensions, including core service, account, department, program, fund/grant, location, and budget data, as applicable. Additionally, MIP uses Distribution Tables (DTs) to allocate salary and benefit data from ADP to relevant reporting dimensions (core service, department, program, fund/grant, and location). This allocation functionality will be critical to our ability forecast ADP salary and benefit costs at the reporting segment level within the FP&A tool. As such, integration should eliminate the need to manually build and maintain duplicate DTs in both MIP and the FP&A tool.	Identify extraction method; dimensional mapping; full and incremental loads; refresh frequency; reconciliation to MIP; rejected-record and error handling; write-back, if proposed; implementation ownership; prior MIP experience; and cost. Identify the methodology for creating and syncing Distribution Tables between MIP and the FP&A tool.
I-03	Credible Behavioral Health	Operational data for analysis and forecasting, including service/encounter, clinician, program, location, payer, units, and available charge/revenue fields.	Describe the exact extraction mechanism and data path; fields available; refresh cadence; historical load; mappings; validation and error handling; PHI minimization; sensitive-field controls; prior Credible experience; implementation ownership; dependencies; and cost.

5. Security, Privacy & Controls

The proposed solution may contain sensitive financial information, employee compensation data, and data derived from Horizon's EHR. The respondent must complete the response requirements below for the proposed

production environment and for any third-party or subcontractor component that stores, processes, transmits, or can access Horizon data.

For every item, the respondent must: (a) state Comply, Partially Comply, Does Not Comply, or Not Applicable; (b) explain how the control operates in the proposed solution; (c) identify whether the capability is native, configurable, custom, or third-party; (d) identify any edition, license, service, configuration, or cost required; (e) describe material limitations, exceptions, shared responsibilities, and implementation dependencies; and (f) provide or identify the requested evidence. If evidence is confidential, describe the document and the process for Horizon to review it under a nondisclosure agreement.

ID	Control Requirement	Minimum Requirement	Required Response and Evidence
S-01	Independent assurance	Maintain an independent assurance report or recognized security certification appropriate to the hosted service.	Identify current SOC 1 and/or SOC 2 report type and coverage period; ISO 27001 or other certifications; scope, carve-outs, subservice organizations, exceptions, and remediation status. Provide the current report/certificate or review process.
S-02	Identity and SSO	Support centralized authentication using Horizon's identity provider.	Identify supported SSO protocols and identity providers (including Microsoft Entra ID, if supported); describe setup, just-in-time provisioning, group/role mapping, login fallback, deprovisioning behavior, required license tier, implementation responsibility, and evidence such as configuration documentation.
S-03	MFA	Support and enforce multi-factor authentication for privileged and non-privileged users.	State whether MFA is native, enforced through SSO, or both; supported factors; whether enforcement can be mandatory; treatment of service accounts and emergency access; required license tier; and screenshots or product documentation.
S-04	Authorization	Restrict access by role/profile and organizational dimensions such as entity, department, program, location, fund/grant, and scenario/version.	Describe the permission model and inheritance; row-, dimension-, object-, report-, and field-level controls; how conflicting roles are resolved; who administers permissions; whether access can be time-limited; and provide a sample role/permission matrix.
S-05	Compensation confidentiality	Permit managers to budget or view authorized labor expense without exposing employee-level compensation or other programs' information.	Explain how detailed payroll data can be masked, suppressed, aggregated, or separated while preserving planning functionality. Describe drill-down behavior, exports, formulas, reports, data extracts, and administrator access. Demonstrate this use case and provide sample configuration.
S-06	Segregation of duties	Provide distinct read, write, submit, approve, data-load, security-administration, and system-administration privileges.	Identify available privileges, incompatible-role controls, delegated administration, approval rules, override capabilities, and evidence through a privilege list or sample workflow.
S-07	Audit logging	Record security and user activity necessary to reconstruct material changes.	Describe logging for logins, failed access, role/permission changes, data loads, mapping changes, assumption and formula changes, submissions, approvals, exports, and administrator activity. State retention, timestamp/user detail, immutability, search/export capability, customer access, and sample audit output.
S-08	Encryption and key management	Protect Horizon data in transit and at rest.	State protocols/standards and minimum versions; encryption coverage for databases, files, backups, logs, and integrations; key ownership, storage, access, and rotation; customer-managed key options; exceptions; and supporting documentation.
S-09	Data minimization and PHI	Support an architecture that excludes PHI where it is not required and restricts any sensitive Credible-derived fields that are included.	Identify the minimum Credible data proposed; list any direct identifiers or sensitive fields; describe transformation, tokenization/pseudonymization, aggregation, field suppression, access restrictions, nonproduction masking, exports, and data-flow documentation. State whether the vendor will sign a BAA if required and identify any limitation on handling PHI.
S-10	Data location and subprocessors	Disclose where Horizon data is stored, processed, backed up, and supported.	Identify hosting provider, production and disaster-recovery regions/countries, remote-support access locations, subprocessors and their functions, data transferred to each, subprocessor change-notification process, and available data-residency options. Provide a subprocessor list and data-flow diagram.
S-11	Backup, resilience and recovery	Maintain backup, continuity, and disaster-recovery capabilities appropriate to the service.	Describe backup frequency, encryption, retention, immutability/offline protections, restore testing, redundancy, recovery time objective (RTO), recovery point objective (RPO), disaster-recovery test frequency and latest test result, customer notification, and contractual commitments.
S-12	Vulnerability management	Maintain secure development, testing, patching, and vulnerability-remediation processes.	Describe secure SDLC, code review, dependency scanning, penetration testing frequency and independence, vulnerability scanning, severity definitions, remediation targets, exception process, last test date, and executive summary or attestation available for review.

ID	Control Requirement	Minimum Requirement	Required Response and Evidence
S-13	Security incidents	Maintain an incident response process that addresses suspected or confirmed compromise of Horizon data.	Describe detection, investigation, containment, preservation of evidence, customer cooperation, notification timing and method, content of notices, post-incident reporting, cyber insurance, and contractual notification commitment. Provide incident-response policy summary and disclose material incidents affecting the service during the past three years.
S-14	Data retention, return and deletion	Allow Horizon to obtain and remove its data throughout the contract lifecycle.	Describe configurable retention, legal-hold support, export formats, export timing and cost, deletion from production and backups, deletion verification, post-termination access period, portability assistance, and exceptions required by law.
S-15	Environment separation and nonproduction data	Separate customer tenants and production from development/test environments.	Describe tenant isolation, production/nonproduction separation, use of customer data in testing, masking requirements, developer access, support access, approval and logging, and safeguards against cross-customer access.
S-16	Monitoring and access review	Support monitoring and periodic review of access and security-relevant activity.	Describe security monitoring coverage, alert handling, privileged access monitoring, access-certification reports, inactive-account controls, review frequency, customer-visible reports, and integration with customer security monitoring if available.
S-17	AI and data use	Disclose any use of artificial intelligence or machine learning involving Horizon data.	Identify AI-enabled features, whether enabled by default, data sent to models/providers, retention, human review, opt-out controls, auditability, subprocessors, and whether Horizon data is used to train shared/general models. State licensing and security implications.

5.1 Required Security Attachments

Submit the following with the proposal, or identify how Horizon may review confidential materials:

- Completed Section 5 response matrix, including all exceptions and shared responsibilities.
- Current independent assurance report(s) or certification(s), bridge letter if applicable, and explanation of material findings relevant to the proposed service.
- Current subprocessor list and a data-flow or architecture diagram showing Horizon data sources, integration components, hosting environment, storage, backups, and administrative access paths.
- Sample role/permission matrix and sample audit-log output demonstrating the granularity available to Horizon administrators.
- Business continuity/disaster recovery summary, including stated RTO and RPO and the date and outcome of the most recent test.
- Incident-response summary and standard security-incident notification commitment.
- Data retention, export, return, and deletion schedule applicable at termination.
- Sample or standard Business Associate Agreement if the proposed design requires the vendor or a subprocessor to create, receive, maintain, or transmit protected health information.

6. Required Demonstration

Finalists must demonstrate the following scenario using representative data or explain precisely how it will be configured. The demonstration must identify any capability that requires custom code, third-party middleware, professional services, or an additional license.

- Load representative MIP GL actuals, ADP workforce data, and Credible operational data.
- Produce a departmental/program P&L with drill-down and actual-to-forecast reporting.
- Forecast salary and benefit expense using employee/FTE, vacancy, and compensation assumptions.
- Forecast revenue using clinician capacity, utilization, services/units, payer, and reimbursement assumptions.
- Demonstrate ability to mask sensitive data and restrict access based on role assignments by
 - allowing a user to view and update actual and forecast information in a program for which they are authorized while simultaneously preventing access to individual compensation data in that program.

- Allow the user to attempt to access other programs for which they are not authorized.
- Consolidate submissions into an organizational forecast and create an Excel-based management report.
- Create and compare a second scenario and show how changes are logged, approved, and rolled forward.
- Show user provisioning/deprovisioning, role assignment, permission testing, restricted drill-down/export behavior, and the audit history for a change to a workforce assumption.

7. Implementation, Training and Support

The proposal must address each item below and distinguish firm commitments from assumptions or optional services.

- Proposed Implementation scope, deliverables, milestones, implementation timeline, acceptance criteria, and go-live approach.
- Named or representative implementation resources and responsibilities of the vendor, Horizon, and each third party.
- Data migration and historical data included, with the recommended number of years and any volume assumptions.
- Testing, reconciliation, issue management, change control, and deployment methodology.
- Training plan for Finance administrators, Finance users, approvers, and occasional budget owners, including materials and recorded sessions.
- Post-go-live support model, service levels, escalation path, support hours, included hours, release management, and customer-success services.
- Estimated ongoing Horizon Finance and IT administration effort after stabilization.
- Process, lead time, and cost for adding dimensions, reports, source systems, integrations, and planning models.
- At least two references for customers of comparable complexity; behavioral health, healthcare, governmental, or nonprofit experience is preferred.
- Any prior implementation involving Credible Behavioral Health or MIP Fund Accounting, including the integration architecture and the vendor's direct role.

8. Pricing and Total Cost of Ownership

Provide firm one-time and recurring pricing for the proposed scope. Identify all assumptions, user counts and license types, usage or storage limits, minimum commitments, taxes, travel, optional services, and annual price increases. Do not combine required and optional costs. All required integration and middleware costs must be included.

Cost Component	Required Pricing Detail	Year 1	Year 2	Year 3
Software subscription	License edition; named/concurrent users by type; minimums; modules; usage/storage limits; price escalator.			
Implementation services	Itemized fixed fee by workstream and deliverable			
ADP integration	All configuration, development, testing, connector, and recurring costs; Components must be itemized.			
MIP integration	All configuration, development, testing, connector, and recurring costs; Components must be itemized.			
Credible integration	All configuration, development, testing, connector, and recurring costs; Components must be itemized			

Cost Component	Required Pricing Detail	Year 1	Year 2	Year 3
Third-party/middleware	Identify each provider, contract holder, one-time fees, recurring fees, and usage assumptions.			
Training	Included and optional training, audience, format, quantity, and rates.			
Support/managed services	Included support and separately priced optional services and hourly rates.			
Other required costs	Data storage, environments, security features, SSO/MFA, assurance-report access, travel, or other mandatory charges.			
Three-year total	Total expected cash cost for the complete proposed solution.			

9. Exceptions, Assumptions and Dependencies

List every exception to the requirements, proposed contract terms, implementation scope, security requirements, pricing instructions, and requested deliverables. Identify assumptions about Horizon resources, data availability, third-party licenses, source-system access, and technical dependencies. Silence will be interpreted as acceptance of the applicable requirement, subject to contract negotiation.

Reference	Exception / Assumption / Dependency	Impact	Proposed Resolution	Cost or Schedule Effect

10. Evaluation Criteria

Horizon anticipates evaluating responsive proposals using the criteria below. Horizon may request clarification, demonstrations, reference checks, security review, revised pricing, or contract discussions before making a selection. The lowest-priced proposal will not necessarily be selected.

Evaluation Category	Weight
Excel experience and usability	15%
Planning and forecasting	20%
Data integration and architecture	15%
Security, privacy, and controls	15%
Behavioral health and operational modeling	10%
Implementation and ongoing administration	10%
Cost and three-year value	10%
Vendor fit, support, and references	5%

11. Mandatory Conditions

A proposal must satisfy the following conditions unless Horizon expressly accepts an alternative in writing:

- The solution provides an Excel-centered experience that is considered acceptable by Horizon. Acceptability will be based on the degree to which the solution achieves or approaches parity with Excel in terms of functionality, flexibility, and syntax used in formulas.
- The proposed security design can restrict sensitive workforce and organizational information at the required level.
- The proposal includes a specific, maintainable integration architecture for Credible, MIP and ADP
- Horizon Finance can reasonably administer the platform after implementation with the resources and services identified in the proposal.

12. Proposal Certification

By submitting a proposal, the respondent certifies that the information provided is accurate to the best of its knowledge; that all required one-time and recurring costs, dependencies, and exceptions have been disclosed; and that the individual signing below is authorized to submit the proposal on behalf of the respondent.

Certification Item	Respondent Information
Legal name of respondent	
Authorized representative	
Title	
Signature	
Date	
Proposal validity period	