



Request for Information #RFI-DOH27-02C: Washington State Immunization Information System Consumer Access Tool & School Immunization Management Solution

October 09, 2026

This RFI is for informational purposes only. Responses will be used solely for information and planning purposes, and no contract will be awarded as a result of this effort.

Request for Information Process

Your voluntary response to this RFI is greatly appreciated. The Department reserves the right to freely utilize any ideas and information received as a result of this RFI in developing potential solutions to the Department's current or future requirements.

How to Respond to this RFI

Please submit your responses via email to the RFI Coordinator, Frank Webley; BIDS@doh.wa.gov in accordance with the RFI Timeline below.

IMPORTANT NOTE: Respondents must utilize **ATTACHMENT A – TECHNICAL RESPONSE FORM** when submitting their response.

The RFI Coordinator is the sole point of contact in the DOH for this Request for Information. Upon release, all communications in regard to this solicitation shall be directed, via email, to the RFI Coordinator or their designee.

RFI Coordinator:

Name:	Frank Webley
E-Mail Address:	Bids@doh.wa.gov
When submitting your response, ensure the email includes the following: • Subject line: Response to RFI-DOH27-02C • Email content: Ensure your email includes: ○ Vendor name, point of contact, and contact information (email, phone number) ○ Please reference any key sections or topics from the RFI that you have addressed in any attached documents.	

RFI Timeline

- RFI Release Date: October 09, 2026
- Deadline for Questions: no later than 2:00 PM, October 23, 2026
- DOH Answers to Contractor Question: October 30, 2026
- Responses Due: 2:00 PM, November 12, 2026



→All times are listed as local time, Tumwater, WA 98501←



Additionally, all Respondents must register as a vendor in WEBS (Washington's Electronic Business Solution) using an appropriate commodities code, listed below, and must download the RFI document(s) from WEBS.

Vendors must rely solely on WEBS for all Request for Information document(s).

208-11-Application Software, Microcomputer
208-37-Database Software
208-53-Integrated Software
208-80-Software, Microcomputer (Not Otherwise Classified)
209-13-Application Software, Minicomputer
209-38-Database Software
918-71-IT Consulting
920-03-Application Service Provider (ASP) (Web Based Hosted)
920-07-Applications Software for Microcomputer Systems: Business, Mathematical/Statistical, Medical, Scientific, etc.
920-14-Applications Software (For Minicomputer Systems)
920-22-Data Preparation and Processing Services (Including Bates Coding)
920-24-Data Conversion Services
920-40-Programming Services, Computer (Including Mobile Device Applications)
920-46-Software Updating Services
920-49-Systems/Executive Software, Main Frame
920-56-Systems/Executive Software, Microcomputer
920-63-Systems/Executive Software, Minicomputer
920-64-System Implementation and Engineering Services
924-16-Course Development Services, Instructional/Training
924-35-In-Service Training (For Employees)



Desired Outcomes from this RFI

This Request for Information is not a competitive solicitation that will result in the award of a contract to one or more bidders. Rather, it is intended to obtain information that may assist the Department in determining the availability of solutions and services that may be required by the Department. Participation in this RFI is voluntary and responses are not considered proposals. This document does not obligate the Department to issue a competitive solicitation to evaluate the services of any responding organization or to enter into any contract. The Department reserves the right to explore any and all options for meeting its needs for services including, but not limited to, options that are brought to its attention through this RFI. The Department shall not be responsible for any cost that may be incurred by people responding to this RFI.

Confidentiality

The Department of Health is subject to public records laws (Chapter 42.56 RCW). As a result, responses are not confidential and are subject to public disclosure. We ask that you not submit any confidential and proprietary information in response to this RFI.

1. Purpose and Background

The Washington State Department of Health (DOH) is seeking information from qualified vendors regarding applications that can support and enhance public access to immunization records and school & childcare immunization compliance management.

DOH is evaluating capabilities for two related solution areas:

1. **MyIR Mobile** – a secure, public-facing application that enables individuals and families to access official Washington State immunization records.
2. **School and Child Care Immunization Module (SCCIM)** – a secure application component that enables authorized schools, school districts, and childcare organizations to manage student immunization records and compliance requirements.

The preferred solution should support secure data linkage to Washington's Immunization Information System (WAIS), improve user experience, reduce administrative burden, improve data quality, and provide reliable tools for immunization compliance, reporting, communications, and system administration.

Responses should describe the vendor's existing capabilities, configurable capabilities, capabilities requiring customization, planned capabilities, and capabilities that are not currently supported.

2. Current-State Overview

2.1 MyIR Mobile

MyIR Mobile is a web-based digital application that provides individuals and families with access to official state immunization records. The application securely connects to the Washington State Immunization Information System (WAIS), allowing authorized users to view vaccination information for themselves and their dependents.

Current and desired capabilities include:

- Viewing official immunization histories for individuals and dependents.
- Downloading and printing state-verified immunization records.



- Generating or accessing the Certificate of Immunization Status (CIS).
- Supporting school, employment, travel, health care, and other documentation needs.
- Viewing recommended, upcoming, overdue, or missing immunizations.

2.2 School and Childcare Immunization Module

The School and Childcare Immunization Module (SCCIM) is an add-on component of WAIIS designed to support schools, school districts, and childcare organizations in managing student immunization compliance. The module provides authorized users with secure access to immunization records maintained within WAIIS and enables organizations to leverage provider-verified immunization information.

Desired capabilities include:

- Monitoring student compliance with Washington State immunization requirements.
- Creating and maintaining student rosters.
- Managing students by school, district, grade, and program.
- Identifying students who are compliant, at risk, or non-compliant.
- Generating parent/guardian communications.
- Generating required regulatory and compliance reports.
- Supporting outbreak response activities.
- Reducing manual recordkeeping and duplicate data entry.

3. Current-State Challenges and Desired Outcomes

DOH seeks solutions that address the following challenges.

3.1 MyIR Mobile Challenges

Identity and Record Matching

Users may be unable to connect their accounts to vaccination records because demographic or contact information does not match information maintained in WAIIS. This can result in failed record matching, user frustration, and increased customer support volume.

User Experience

The current registration and account-access experience may be confusing for some users. Error messages may not adequately explain the problem or provide actionable instructions for resolution.

Security and Convenience

Multi-factor authentication (MFA) is necessary to protect sensitive health information; however, authentication requirements should balance security with accessibility and ease of use. DOH is interested in expanding available MFA and account recovery options.

Customer Support Volume

Login problems, password resets, authentication issues, and record-matching failures generate support requests that could potentially be resolved through improved self-service capabilities and workflow automation.

Data Quality

Misspelled names, duplicate patient records, merged records, missing demographic information, or incomplete vaccination records in WAIIS may result in inaccurate or incomplete information being displayed to users.



Accessibility

The solution must support users with disabilities, older adults, users with limited technical proficiency, and users who require alternative languages or assistive technologies.

3.2 School Module Challenges

Application Reliability

Software defects may affect the reliability or usability of reports and other critical functions.

Vendor Responsiveness

DOH seeks timely resolution of critical and significant software issues, clear communication regarding defects, and reliable commitments to remediation timelines.

Quality Assurance

- Software releases, enhancements, and bug fixes should undergo comprehensive vendor-managed quality assurance and testing before deployment. DOH seeks to reduce the amount of testing required from internal DOH resources.
- Roster and Data Management
- DOH seeks improved centralized roster management capabilities that reduce duplicate data entry, simplify enrollment updates, improve data accuracy, and support efficient management across schools and districts.

4. Scope of Requested Solution

Vendors should describe how their proposed solution addresses the following functional requirements.

For each requirement, vendors should identify whether the capability is:

- **Available – Standard:** Available without customization.
- **Available – Configurable:** Available through configuration.
- **Available – Customization Required:** Requires development or customization.
- **Planned:** Included on the product roadmap.
- **Not Available:** Not currently supported.

Vendors should provide additional details, limitations, dependencies, and estimated implementation effort where applicable.

5. MyIR Mobile Functional Requirements

5.1 Core Functionality

The solution should:

1. Provide simplified account creation and identity verification.
2. Improve matching between users and their immunization records in WAIS.
3. Provide clear navigation and intuitive workflows.
4. Provide actionable and understandable error messages.
5. Provide step-by-step guidance for registration, record matching, login, and account recovery.
6. Support multiple languages.
7. Support accessibility standards and assistive technologies.



8. Provide a public-facing system-status or outage notification capability.
9. Display recommended, due, overdue, or missing vaccinations using applicable DOH guidelines.
10. Provide explanatory information regarding why a vaccination may appear to be missing or recommended
11. Support display of titer/immunity results where applicable.
12. Automatically retrieve the most current available immunization information when a user accesses the application.
13. Provide digital vaccine certificates and other applicable documentation.
14. Support both web browsers and mobile devices.

5.2 Identity Matching and Account Management

The solution should:

- Automatically match users with immunization records in WAIS using configurable demographic matching logic.
- Support required demographic fields during registration, including date of birth and phone number where appropriate.
- Provide mechanisms to resolve or escalate unmatched records.
- Allow users to update contact information.
- Allow users to manage communication preferences and notification settings.
- Provide secure password reset and account recovery.
- Support multiple MFA methods, including email, SMS/text, and voice/telephone where permitted.
- Support secure account recovery for users who cannot access their primary authentication method.

5.3 Workflow Automation

The solution should support:

- Automated record matching.
- Automated vaccine reminders and recall notifications.
- Automated password resets.
- Automated account recovery.
- Automated creation and routing of support tickets.
- Self-service resolution of common account and access issues.
- Escalation of unresolved issues to authorized support staff.
- Automated retrieval of updated immunization records.

5.4 Notifications and Dependents

The solution should:

- Allow parents and guardians to manage dependents from a single account.
- Support linked family records.
- Allow authorized users to oversee notifications for multiple records.
- Support configurable email, SMS/text, and other approved notification mechanisms.
- Allow users to manage notification preferences.

5.5 Search and Record Access

The solution should:

- Provide secure search and retrieval of an individual's immunization record.
- Support configurable demographic matching criteria.



- Display current and historical immunization information.
- Display vaccination forecasts and recommendations.
- Display applicable titer/immunity information.
- Provide downloadable and printable documentation.

5.6 Reporting and Dashboards

The solution should provide real-time or near-real-time dashboards for:

- New registrations.
- Active users.
- Application usage.
- Login and authentication activity.
- Record matching success and failure rates.
- Customer support ticket volume.
- Support response times.
- Common support issues.
- Other configurable operational metrics.

5.7 Customer Support and Self-Service

The solution should provide:

- Configurable FAQ content that authorized DOH staff can maintain without vendor development.
- Chatbot or self-service functionality for common questions, where appropriate.
- Support ticket creation and routing.
- Ticket status tracking.
- Escalation workflows.
- Administrative tools for authorized staff to assist users with account and matching issues.

5.8 Content and Customization

The solution should support:

- Multiple languages.
- Washington State-specific content.
- DOH-configurable informational content.
- DOH event and service announcements.
- Configurable notification messages.
- Configurable help and FAQ content.
- State-specific CIS documentation and formatting.

6. School and Child Care Immunization Module Functional Requirements

6.1 Core Functionality

The solution must enable authorized school, district, and childcare users to:

1. Create and maintain organization-specific rosters.
2. Manage students by school, district, grade, and program.
3. View immunization summaries.
4. View detailed immunization histories.
5. Assess compliance against applicable Washington State requirements.
6. Identify compliant, at-risk, and non-compliant students.



7. Generate Certificates of Immunization Status (CIS).
8. Enter immunization records.
9. Document exemptions.
10. Document immunity by titer when supported by appropriate written parental/guardian consent and applicable requirements.
11. Support outbreak response activities.
12. Generate required annual and regulatory reports.

6.2 Immunization Data Entry

The solution must provide authorized users with the ability to:

- Enter immunization information.
- Update immunization records as permitted.
- Record exemptions.
- Record immunity by titer.
- View vaccine history.
- Support appropriate documentation and audit trails for changes.
- Apply applicable state requirements and validation rules.

6.3 Forecasting and Compliance

The platform should utilize Washington DOH/American Academy of Pediatrics (AAP) forecasting rules, as applicable, to:

- Determine vaccines that are due.
- Determine vaccines that are overdue.
- Identify recommended vaccines.
- Identify students requiring additional immunizations.
- Support school attendance compliance determinations.
- Support compliance monitoring.
- Identify students requiring follow-up.

Vendors should describe how forecasting rules are maintained, updated, tested, and implemented following changes recommendations.

6.4 Roster Management

The solution should provide centralized roster management that enables users to:

- Create school and district rosters.
- Add and remove students.
- Update enrollment information.
- Transfer students between schools.
- Support grade-level changes.
- Import or synchronize roster information.
- Minimize duplicate data entry.
- Identify duplicate student records.
- Maintain appropriate historical records.
- Support integration with school systems.



6.5 Workflow Automation

The solution should support automated workflows for:

- Roster management.
- Immunization status evaluation.
- Reminder and recall processes.
- Parent/guardian notifications.
- Compliance monitoring.
- Outbreak response.
- Follow-up of missing immunization information.
- Annual reporting.
- Account management and password recovery.

6.6 Parent and Guardian Communications

The current environment primarily supports postal mail.

The preferred solution should provide electronic communication capabilities, including:

- Email notifications.
- SMS/text notifications.
- Printable letters.
- Reminder and recall communications.
- Missing immunization notifications.
- Upcoming due-date notifications.
- Compliance notifications.
- Configurable communications by district and/or school.
- Notification history.
- Delivery status tracking where supported.
- Templates configurable by authorized users.

The solution should also describe its ability to integrate directly with school systems for parent communications.

6.7 User Management and Multi-Organization Access

The solution must provide role-based security controls for multiple user types, including, as applicable:

- School nurses.
- School administrators.
- District administrators.
- Childcare personnel.
- Public health staff.
- DOH staff.
- System administrators.

Permissions should be configurable to provide appropriate view, edit, administrative, and reporting capabilities based on role and jurisdiction.



The preferred solution should allow an authorized individual who works with multiple organizations to access multiple districts and/or school accounts using a single user identity and login, rather than requiring separate accounts for each organization.

The solution must ensure that users see only the organization-specific data, documentation, requirements, and functionality for which they are authorized.

6.8 Search

The solution should provide search capabilities to:

- Locate individual students.
- Search student immunization records.
- Manage school and district rosters.
- View immunization histories.
- View vaccine-level information.
- Identify students by compliance status.
- Identify exemptions.
- Locate students requiring follow-up.
- Generate compliance reports.

6.9 Reporting and Dashboards

The solution should provide configurable reports, including, at a minimum:

- Action Reports.
- At-Risk Reports.
- Student Compliance Reports.
- Roster Reports.
- CIS Status Reports.
- Reminder letters and labels.
- Annual immunization reports.
- Exemption reports.
- Outbreak-related reports.

The solution should also provide internal operational dashboards for monitoring:

- Support ticket volume.
- Support response times.
- Common user issues.
- System performance.
- Data quality issues.
- Application errors.
- Other configurable operational metrics.

6.10 Customization

The solution should support configuration by:

Grade/Program

- Preschool, approximately 19 months–3 years.
- Preschool/TK, approximately 4–5 years.



- Grades K–6.
- Grades 7–12.
- Childcare programs covering multiple age ranges.

Compliance Series

- HPV Dose 1.
- HPV Dose 2.
- Tdap.
- Meningococcal.
- HPV series.
- Other Washington State-defined compliance series.

Vendors should describe the process and timeline for updating state-specific compliance requirements.

7. Technical Requirements

7.1 Cloud Infrastructure

The proposed solution should:

- Support a minimum of 5 million users.
- Provide scalable compute and storage resources.
- Support increased transactional volumes without material degradation in performance.
- Provide high availability and fault tolerance.
- Support monitoring of capacity and system performance.

Vendors should describe their cloud architecture, hosting environment, scalability model, and service availability commitments.

7.2 Operating Systems and Browser Compatibility

The solution should:

- Support current versions of major desktop operating systems.
- Support current versions of major web browsers.
- Maintain compatibility through regular updates and testing.
- Clearly identify browser and operating system requirements.

7.3 Mobile Platform Support

The solution should provide a consistent user experience across:

- Desktop web browsers.
- Mobile web browsers.
- iOS devices.
- Android devices.

Vendors should identify whether mobile functionality is delivered through responsive web design, native applications, progressive web applications, or another approach.



8. Disaster Recovery and Business Continuity

The vendor must maintain documented disaster recovery and business continuity plans.

8.1 Recovery Objectives

DOH's target objectives are:

- Recovery Time Objective (RTO): Ideally no more than 24 hours.
- Recovery Point Objective (RPO): Ideally between 1 and 24 hours, with vendors encouraged to provide more stringent capabilities where available.

Vendors should state their committed RTO and RPO.

8.2 Disaster Recovery Phases

The vendor's plan should address:

Notification and Activation

- Detection of an incident.
- Assessment of impact.
- Notification of appropriate partners.
- Activation of the disaster recovery plan.

Recovery

- Restoration of temporary operations.
- Restoration of application services.
- Recovery of data and supporting infrastructure.
- Validation of restored services.

Reconstitution

- Restoration of normal operations.
- Validation of production systems.
- Closure of disaster recovery activities.
- Post-incident review.

9. Backup and Data Retention

If the vendor retains DOH data, the vendor must maintain a documented backup and retention strategy.

The preferred backup strategy includes:

- Hourly restore points for the current day.
- Daily restore points for the preceding 13 days.
- Additional retention periods as required by state policy or law.
- Documented backup schedules.
- Regular backup integrity testing.
- Periodic restoration testing.

Backups containing Protected Health Information (PHI) must be encrypted using appropriate secure methods consistent with applicable standards, including NIST guidance.



Off-site backup storage should be maintained in a physically secure location within the continental United States unless otherwise approved by DOH.

Access to backup systems must be restricted to authorized personnel.

10. Service Management and Issue Severity

The vendor should provide a formal incident management process.

10.1 Severity Levels

Severity 1 – Critical

A system or critical business function is unavailable or significantly impaired, resulting in a major impact on users' ability to conduct business.

- Target response: Within 2 hours
- Target resolution: Within 4 hours of acknowledgement

Severity 2 – High

A significant issue affects a user, group, or business function and critically impairs operations, but an inefficient workaround is available.

- Target response: Within 4 hours
- Target resolution: Within 8 hours of acknowledgement

Severity 3 – Moderate

An issue affects a limited number of users and an acceptable, although not optimal, workaround exists. There is no significant impairment of critical business operations.

- Target response: Next business day
- Target resolution: Within 5 business days of acknowledgement

Vendors should identify any differences between these requested targets and their standard SLAs.

10.2 Definitions

- Response Time: Elapsed time between incident submission and initial contact by a support representative.
- Resolution Time: Elapsed time between issue acknowledgement and resolution or implementation of an acceptable workaround.

11. Scalability and Performance

Vendors should describe:

- Maximum supported user population.
- Maximum concurrent users.
- Transaction-processing capacity.
- API transaction capacity.
- Data ingestion capacity.
- Expected performance at peak usage.



- Auto-scaling capabilities.
- Performance monitoring.
- Load testing methodology.
- Capacity planning process.

The solution must be capable of supporting projected growth in users, organizations, immunization records, transactions, and integrations.

12. Data Security and Privacy

The vendor must describe its approach to protecting sensitive health and personal information.

Responses should address:

- Data encryption at rest.
- Data encryption in transit.
- Encryption key management.
- Access controls.
- Role-Based Access Control (RBAC).
- Multi-Factor Authentication (MFA).
- Audit logging.
- Security monitoring.
- Vulnerability management.
- Penetration testing.
- Security incident response.
- Data retention and destruction.
- Data residency.
- Backup security.
- Third-party access.
- Administrative access.
- Privileged user monitoring.

13. Data Sharing and External Access

Vendors should describe:

- Data-sharing policies.
- Data-sharing agreements and controls.
- Authorized third-party access.
- External user authentication.
- Internal DOH user authentication.
- Role-based permissions.
- MFA options.
- Data access auditing.
- Controls for least-privilege access.
- Procedures for terminating access.
- Data-use monitoring.



The solution should support MFA methods including, where permitted:

- Email.
- SMS/text.
- Voice/telephone.
- Authenticator applications or other secure methods required by DOH.

Vendors should identify all available authentication methods and any associated limitations.

14. System Administration and Oversight

The solution should support separation of responsibilities between vendor and DOH administrators.

Vendors should describe:

- Vendor administrative capabilities.
- DOH administrative capabilities.
- Role-based administrative permissions.
- Auditability of administrative actions.
- Configuration management.
- Data monitoring.
- Troubleshooting capabilities.
- Tools for identifying and resolving unmatched records.
- Tools for monitoring data quality.
- System health monitoring.
- Administrative reporting.

15. DOH-Specific Requirements

- The solution must support State-specific configuration and business requirements.
- Vendors should describe their ability to support:
 - Washington State immunization schedules.
 - Washington DOH/AAP forecasting.
 - Washington State CIS forms.
 - Washington State compliance requirements.
 - Washington-specific reporting.
 - State-specific terminology and workflows.
 - Washington State data retention requirements.
 - Washington State integration requirements.
- The vendor should provide a copy or example of the CIS form currently supported by its solution (if available) and describe its process for implementing future Washington State CIS changes.

16. Integration Requirements

The solution should support integration with existing and future DOH systems.

Vendors must describe compatibility with:

16.1 Active Directory

Describe support for:

- Active Directory.
- Azure/Entra ID, if applicable.
- User provisioning.
- Group/role synchronization.
- Deprovisioning.

16.2 Single Sign-On

Describe support for:

- Single Sign-On (SSO).
- SAML 2.0.
- OpenID Connect (OIDC).
- OAuth 2.0.
- Other supported authentication standards.

16.3 HL7/FHIR

Describe support for:

- HL7 interfaces.
- FHIR APIs.
- Immunization-related FHIR resources.
- Bidirectional exchange.
- Data validation.
- Error handling.
- Interface monitoring.

16.4 APIs

Describe:

- Available APIs.
- API documentation.
- Authentication mechanisms.
- Rate limits.
- Data formats.
- API monitoring.
- Versioning.

16.5 School Systems

Describe the solution's ability to integrate with School Information Systems for:

- Student roster exchange.
- Enrollment updates.
- Parent/guardian contact information.
- School and district information.
- Parent communications.
- Compliance status.



17. Security and Compliance Requirements

The vendor must describe its security program and compliance framework.

17.1 Required Security Capabilities

The solution should provide:

- Encryption at rest.
- Encryption in transit.
- MFA.
- RBAC.
- Comprehensive audit logging.
- Vulnerability management.
- Secure software development practices.
- Penetration testing.
- Security monitoring.
- Incident response.
- Backup and recovery.
- Secure data destruction.

17.2 Compliance Standards

Vendors should identify applicable certifications, attestations, and compliance standards supported by the solution, including, as applicable:

- HIPAA.
- FERPA.
- NIST security frameworks.
- SOC 2 Type II.
- ISO 27001.
- Washington State security requirements.

For each certification or standard, vendors should provide the applicable scope and current status.

18. Implementation Requirements

Vendors should describe their implementation methodology and provide estimated timelines for a project of this size and complexity.

18.1 Implementation Timeline

Provide estimated durations for:

- Discovery.
- Requirements validation.
- Solution design.
- Configuration.
- Development/customization.
- Integration development.
- Data migration.
- Testing.
- User acceptance testing.
- Training.



- Production readiness.
- Go-live.
- Post-go-live stabilization.

18.2 Project Methodology

Describe the proposed project management methodology, such as:

- Agile.
- Scrum.
- Waterfall.
- Hybrid.
- Other.

Identify project governance, status reporting, risk management, issue management, and change control processes.

18.3 Client Responsibilities

Identify responsibilities expected of DOH, including:

- Subject matter expertise.
- Requirements validation.
- Data validation.
- User acceptance testing.
- Security review.
- Integration coordination.
- Training participation.
- Go-live approval.

18.4 Vendor Responsibilities

Identify vendor responsibilities, including:

- Project management.
- Solution configuration.
- Development.
- Testing.
- Documentation.
- Integration.
- Data migration.
- Training.
- Deployment.
- Go-live support.
- Post-go-live stabilization.

18.5 Data Migration

Describe the proposed approach for migrating data from the existing platform, including:

- Data extraction.
- Data mapping.
- Data cleansing.
- Transformation.
- Validation.
- Duplicate management.
- Reconciliation.
- Migration testing.
- Cutover.
- Rollback procedures.
- Post-migration validation.

18.6 Training and Documentation

The vendor should provide:

- Administrator training.
- End-user training.
- Train-the-trainer options.
- Technical documentation.
- User guides.
- System administration guides.
- Integration documentation.
- Configuration documentation.
- Frequently Asked Questions.
- Training recordings or self-service materials where available.

18.7 Go-Live Support

Describe:

- Go-live staffing.
- Extended support hours.
- On-site or remote support.
- Issue triage.
- Escalation procedures.
- Daily status reporting.
- Post-go-live stabilization period.

19. Support and Maintenance

19.1 Help Desk

Vendors should identify:

- Standard help desk hours.
- Extended support hours.
- 24x7 support availability.
- Holiday support.
- Emergency support.

19.2 Support Channels

Describe available support channels, including:

- Telephone.
- Email.
- Web-based ticketing.
- Chat.
- Self-service knowledge base.
- Emergency escalation channels.

19.3 Service Level Agreements

Vendors should provide proposed SLAs for:

- System availability.
- Severity 1 incidents.
- Severity 2 incidents.
- Severity 3 incidents.
- Security incidents.
- Data incidents.
- Interface failures.
- Customer support requests.

19.4 Escalation

Describe the escalation process for:

- Unresolved incidents.
- Repeated defects.
- Major system outages.
- Security incidents.
- Missed service commitments.
- Critical integration failures.

19.5 Application Updates

Vendors should describe:

- Release frequency.
- Planned maintenance windows.
- Emergency patches.
- Version management.
- Release notes.
- Regression testing.
- Customer notification.
- State-specific testing.
- Rollback capabilities.

20. Quality Assurance and Release Management

The vendor must describe its software quality assurance program.

The response should address:

- Unit testing.
- Integration testing.



- Regression testing.
- Performance testing.
- Security testing.
- Accessibility testing.
- User acceptance testing.
- Automated testing.
- Manual testing.
- Release readiness criteria.
- Defect tracking.
- Defect severity classification.
- Production monitoring.
- Post-release validation.

DOH's objective is to minimize the amount of internal DOH effort required to identify defects following vendor releases.

21. Issue, Bug, and Change Management

The vendor should provide tools and processes for:

- Reporting software defects.
- Tracking incidents.
- Tracking enhancement requests.
- Assigning severity.
- Prioritizing issues.
- Tracking resolution.
- Communicating status.
- Maintaining audit trails.
- Providing release notes.
- Reporting recurring issues.
- Identifying root causes.
- Conducting post-incident reviews for significant defects.

Vendors should describe their average resolution times for defects by severity.

22. Licensing and Pricing

Vendors should provide general pricing information and identify all anticipated costs.

Responses should address:

22.1 Licensing Model

- Subscription.
- Per-user licensing.
- Enterprise licensing.
- Organization-based licensing.
- Transaction-based licensing.
- Other models.

22.2 Subscription Options

Describe:

- Contract terms.
- Annual versus multi-year options.
- Renewal terms.
- Price escalation.
- Minimum commitments.

22.3 User-Based Pricing

Identify whether pricing is based on:

- Registered users.
- Active users.
- Concurrent users.
- Administrative users.
- School/district users.
- Public users.
- Other measures.

22.4 Additional Costs

Identify costs associated with:

- Implementation.
- Data migration.
- Training.
- Support.
- Hosting.
- Integrations.
- APIs.
- Customization.
- Configuration.
- Additional environments.
- Testing.
- Reporting.
- Future enhancements.
- Inactive users (data retention)

Vendors should identify any costs that are not included in standard licensing or subscription fees.

23. Product Roadmap and Future Capabilities

Vendors should provide a three-to-five-year product roadmap, where available.

The roadmap should identify:

- Planned enhancements.
- Major platform upgrades.
- Planned interoperability improvements.
- Future integrations.
- Mobile enhancements.



- Accessibility enhancements.
- Reporting and analytics improvements.
- AI capabilities.
- Automation capabilities.
- Customer support improvements.

23.1 Artificial Intelligence

Vendors should describe current or planned AI capabilities, including potential use cases such as:

- Customer support chatbots.
- Natural-language search.
- Automated ticket classification.
- Support-ticket summarization.
- Data-quality assistance.
- Record matching assistance.
- Predictive analytics.
- Administrative workflow automation.

Vendors must describe appropriate safeguards for AI capabilities involving protected or sensitive health information.

23.2 Product Lifecycle

Describe:

- Product lifecycle.
- Supported versions.
- End-of-life policy.
- Upgrade process.
- Backward compatibility.
- Major release frequency.
- Minor release frequency.
- Security patch frequency.

24. Vendor Information

Vendors should provide the following information:

24.1 Corporate Information

- Legal company name.
- Headquarters location.
- Years in business.
- Number of employees.
- Ownership structure.
- Parent company, if applicable.
- Subsidiaries, if applicable.
- Financial stability.
- Relevant mergers or acquisitions.



24.2 Relevant Experience

Describe experience providing:

- Immunization information systems.
- Public health technology.
- Health information systems.
- School health technology.
- Childcare systems.
- Public-sector SaaS solutions.
- Large-scale consumer-facing health applications.

24.3 Customer References

Provide relevant customer references, preferably including:

- State government agencies.
- Local government agencies.
- Public health organizations.
- School districts.
- Large healthcare organizations.
- Immunization information system clients.

For each reference, provide:

- Organization name.
- General scope of implementation.
- Approximate number of users.
- Implementation date.
- Contact information, if permitted.

25. Vendor Response Format

To facilitate consistent evaluation, vendors should organize their response according to the sections in this RFI.

For each functional or technical requirement, vendors should identify:

Response	Definition
Meets	Capability is currently available as standard functionality.
Configurable	Capability is available through configuration without custom software development.
Customization Required	Capability can be provided but requires software development or significant customization.
Planned	Capability is planned but is not currently available.
Does Not Meet	Capability is not currently available and is not planned.

For requirements identified as Customization Required or Planned, vendors should provide:

- Description of proposed approach.
- Estimated implementation timeline.
- Estimated cost.
- Dependencies.



- Risks.
- Ongoing maintenance implications.

26. Assumptions, Exceptions, and Dependencies

Vendors should clearly identify:

- Assumptions used in preparing the response.
- Required third-party products or services.
- Required DOH resources.
- Required integrations.
- Data dependencies.
- Licensing dependencies.
- Security dependencies.
- Features requiring customization.
- Features requiring third-party services.
- Limitations or exclusions.
- Any requirements the vendor believes require clarification.

27. Requested Vendor Attachments

Vendors should include, as applicable:

- Product overview.
- Solution architecture diagram.
- System architecture and hosting documentation.
- Security documentation.
- SOC 2 or equivalent report.
- HIPAA documentation or Business Associate Agreement information.
- Accessibility conformance documentation.
- Disaster recovery/business continuity summary.
- Sample SLA.
- Sample implementation plan.
- Sample project schedule.
- Data migration methodology.
- API documentation.
- HL7/FHIR interoperability documentation.
- Sample CIS form.
- Sample reports and dashboards.
- Sample user interfaces.
- Training materials.
- Support model.
- Product roadmap.
- Pricing schedule.
- Customer references.
- Other relevant supporting documentation.



28. Cost Information

Please provide detailed information for both off-the-shelf products and custom-built products you may include as a solution.

- **Off-the-Shelf Product:** If part of your solution is an Off-the-Shelf Product, please include detailed information for setting up, licensing, ongoing maintenance, and any ancillary services.
- **Custom-Built Solution:** Provide a detailed breakdown for each component, including:
 - IIS & school system integration
 - Mobile application portal development
 - API data pipeline development
 - Registry management and data integration
 - Data migration from existing registry
 - Reporting and analytics
 - Advanced patient matching algorithms (machine learning)