Can you print and deliver this to:

Crystal Hustead
State of West Virginia
2019 Washington St E
Charleston, WV 25305

Tiffany Tate
Chief Executive Officer
VAULT Technologies
P: 888-862-2920, Ext. 1
E: tiffany.tate@vaulttechinc.com
Pronouns: she/her

Our messages are encrypted to maintain confidentiality according to HIPAA requirements. As email communications are not guaranteed to be encrypted, it is our duty and policy not to exchange confidential information via this channel. Please do not include protected health information or any personal medical information in any emails you send to us. If you are not the intended recipient of this message, please notify the sender immediately.

VAULT
TECHNOLOGIES
THE FUTURE OF PUBLIC HEALTH IS HERE

Technical Proposal Cover Sheet

Proposal Type: **TECHNICAL PROPOSAL**

Solicitation Number: **CRFP 0506 MIS2600000001**

Solicitation Title: **REQUEST FOR PROPOSAL – IMMUNIZATION INFORMATION SYSTEM**

Vendor Name : **VAULT Technologies, LLC**

Contact Person: **Tiffany Tate**

Phone Number: **+1 888-862-2920 Ext. 1**

Email Address: **tiffany.tate@vaulttechinc.com**

Date of Submission: **03/24/26**

TECHNICAL PROPOSAL

Immunization Information System (IIS)

RFP No. CRFP MIS2600000001

Submitted To:

State of West Virginia
Department of Health
Bureau for Public Health

Submitted By:

VAULT Technologies, LLC
1 Reservoir Circle, Suite 101
Pikesville, MD 21208

Contact Information:

Contact Name: Tiffany Tate

Title: Chief Executive Officer

Telephone: 888-862-2920 Ext. 1

Fax Number: N/A

Email: tiffany.tate@vaulttechinc.com

Authorized Signature:

Signature

Tiffany Tate

Printed Name & Title

3 24 26

Date

TABLE OF CONTENTS

4.1 BACKGROUND AND CURRENT OPERATING ENVIRONMENT

Transforming West Virginia's Immunization Infrastructure into a Statewide Public Health Operating System

The State of West Virginia is at a pivotal moment in the evolution of its Immunization Information System (IIS).

Historically, IIS platforms have served as systems of record—repositories designed to collect, store, and report vaccination data. While these systems remain essential, the demands placed on public health infrastructure have fundamentally changed. Today, states are being asked not only to track immunizations, but to actively improve vaccination coverage, respond to emerging health threats, and deliver care to populations that are often difficult to reach—particularly in rural and underserved communities.

West Virginia faces these challenges acutely. Geographic dispersion, provider shortages, and barriers to access require more than a traditional registry. They require an infrastructure that can identify need, coordinate resources, deploy care, and measure outcomes in real time.

VAULT Technologies proposes a solution designed specifically for this moment.

Rather than delivering a standalone IIS, VAULT provides a modern, cloud-based immunization platform anchored by our IIS platform, OptimIIS, and powered by the broader PMEcosystem—a fully integrated suite of capabilities that enables West Virginia to manage immunization data and operationalize public health across the entire state.

At its core, OptimIIS serves as the authoritative, CDC-compliant immunization registry, supporting high-volume HL7 v2.5.1 and FHIR-based data exchange, real-time validation, and longitudinal patient records. However, what differentiates VAULT's approach is the seamless integration of operational, clinical, and community-based capabilities that extend far beyond traditional IIS functionality.

As OptimIIS functions as a centralized, secure registry, it is complemented by an integrated ecosystem of microservices, miniature, specialized programs that operate independently and together to provide users a flexible, semi-bespoke experience.

The Ecosystem is comprised of "bundles" that are nimble enough that they can be used for vaccinations and any other public health service, including:

- A powerful, rules-based interoperability module that streamlines and modernizes sharing among any modern health information systems
- A market-leading end-to-end scheduling and clinic management application
- An community outreach and community-based clinic planning automation bundle
- An emergency preparedness and disaster response engine
- A digital patient record

This ecosystem-based approach enables the State of West Virginia to move beyond a traditional, standalone IIS and adopt a modular, scalable public health platform. Functionality can be deployed incrementally, enhancements can be delivered without disruption, and system components can scale independently to meet evolving program needs.

Through this ecosystem, West Virginia gains the ability to:

- Identify unmet immunization needs at the population and community level using real-time data and analytics
- Enable users to deploy care into underserved areas, including rural communities, through coordinated mobile and community-based service delivery
- Streamline provider onboarding and participation, reducing barriers to data submission and improving completeness and timeliness
- Support clinical decision-making through real-time forecasting aligned with ACIP recommendations
- Equip users with a tool to capture and sustain funding through integrated billing and reimbursement capabilities
- Respond rapidly to public health emergencies with scalable infrastructure designed for surge events

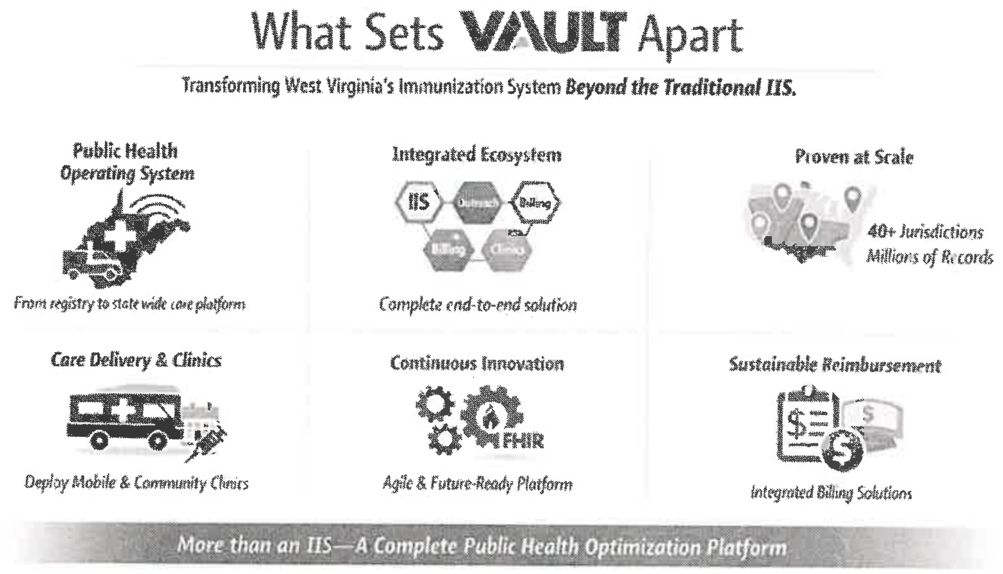
This approach directly aligns with the State's objectives for interoperability, data quality, performance, and long-term sustainability, while also supporting broader federal initiatives such as the CDC Data Modernization Initiative and North Star Architecture.

Importantly, VAULT's solution is not theoretical. The Ecosystem has been used in more than 40 jurisdictions and has supported tens of millions of immunization encounters, including large-scale, high-volume public health responses. This experience ensures that West Virginia receives a solution that is both innovative and proven, capable of delivering immediate value while supporting long-term transformation.

By implementing VAULT's solution, West Virginia will not simply modernize its IIS—it will establish a statewide public health operating system that enables more effective vaccination programs, improves access to care, and strengthens the State's ability to respond to both current and future public health needs.

What Sets VAULT Apart

VAULT Technologies' solution differs fundamentally from traditional IIS vendors in both scope and impact. While many systems focus primarily on data collection and reporting, VAULT delivers a comprehensive platform that enables West Virginia to actively improve immunization outcomes.



What Sets VAULT Apart

Transforming West Virginia's Immunization System *Beyond the Traditional IIS.*

Public Health *Operating System*

From registry to state wide care platform

Integrated Ecosystem

Complete end-to-end solution

Proven at Scale

40+ Jurisdictions
Millions of Records

Care Delivery & Clinics

Deploy Mobile & Community Clinics

Continuous Innovation

Agile & Future-Ready Platform

Sustainable Reimbursement

Integrated Billing Solutions

More than an IIS—A Complete Public Health Optimization Platform

1. From Registry to Public Health Operating System

Traditional IIS platforms function as systems of record.
VAULT provides a statewide operational platform that enables the State to identify need, deploy care, and measure outcomes in real time.

2. Integrated Ecosystem vs Standalone System

Most vendors deliver a single IIS application.
VAULT delivers a fully integrated ecosystem, including:

- OptimIIS (registry)
- IISConnex (interoperability)
- PrepMod (clinic operations)
- PMCommunity (outreach and workforce coordination)
- ReadiBilling (reimbursement)

This integration eliminates fragmentation and enables end-to-end public health operations.

3. Proven at Scale in Real-World Public Health Operations

VAULT's platform has supported:

- Over 40 jurisdictions
- Tens of millions of immunization records
- Large-scale emergency response efforts

This ensures that the solution is not theoretical, but proven under real-world conditions.

4. Ability to Deliver Care—Not Just Track It

Unlike traditional systems that document vaccinations after they occur, VAULT enables:

- Deployment of mobile and community-based clinics
- Rapid activation of vaccination events
- Coordination of workforce and resources

This directly addresses West Virginia's rural access challenges.

5. Built for Continuous Innovation Without Disruption

Legacy IIS platforms require large, disruptive upgrades.
VAULT's microservices architecture allows:

- Incremental enhancements
- Rapid adoption of new standards (FHIR, TEFCA)
- Continuous improvement without downtime

6. Financial Sustainability Through Integrated Billing

VAULT uniquely integrates reimbursement capabilities through ReadiBilling, enabling:

- Capture of billable services
- Reduced administrative burden
- Long-term sustainability of immunization programs

Summary

VAULT is not simply offering an IIS replacement.
VAULT is enabling West Virginia to transition from a data-centric system to a care delivery and public health optimization platform.

4.2 PROJECT GOALS AND MANDATORY REQUIREMENTS

VAULT Technologies proposes the implementation of the PrepModEcosystem, anchored by OptimIIS, as a comprehensive solution to meet the State of West Virginia's requirements for a modern Immunization Information System (IIS). This solution is designed to securely collect, store, manage, and exchange immunization data while supporting improved vaccination tracking, increased coverage, and data-driven public health decision-making.

Our methodology is grounded in delivering a fully integrated, modular, and scalable platform that addresses both current operational requirements and future public health needs. Unlike traditional IIS solutions that function as standalone registries, VAULT's approach provides an ecosystem-based model that connects immunization data, clinical workflows, interoperability, analytics, and community engagement into a unified platform.

At the core of this approach is OptimIIS, which serves as the authoritative system of record for immunization data. It is complemented by tightly integrated modules including IISConnex for interoperability, PrepMod for clinic and scheduling workflows, PMCommunity for outreach, and ReadiBilling for financial sustainability. This integrated architecture ensures that immunization data is not only captured and stored, but actively used to support clinical care, operational efficiency, and public health strategy.

VAULT's methodology is grounded in delivering a fully integrated, modular, and scalable platform that addresses both current operational requirements and future public health needs. This approach directly aligns with the State's objectives for interoperability, data quality, system performance, and long-term sustainability.

To improve immunization tracking and vaccination coverage, the platform incorporates advanced clinical decision support and analytics capabilities. The system evaluates patient immunization histories against ACIP recommendations and provides real-time forecasting, helping providers deliver appropriate care. In parallel, robust reporting and dashboard tools allow public health administrators to monitor coverage rates, identify gaps, and target outreach efforts to underserved populations.

VAULT also prioritizes data quality and integrity through automated validation, deduplication, and reconciliation processes. These capabilities ensure that the IIS maintains a single, accurate record for each patient and supports reliable reporting and analysis. These capabilities directly support the State's requirement to maintain accurate, complete, and reliable immunization records.

From an operational perspective, VAULT employs a phased, collaborative implementation methodology that minimizes risk and ensures alignment with State priorities. This includes structured project governance, iterative development cycles, and continuous stakeholder engagement. Our experience in jurisdictions such as Maryland and Washington demonstrates our ability to deliver systems that evolve in partnership with public health agencies, incorporating feedback and adapting to changing requirements over time.

A key differentiator of VAULT's approach is its ability to deliver continuous innovation without disruption. The platform's microservices-based architecture allows enhancements to be deployed incrementally, avoiding the large, disruptive upgrades often associated with legacy systems. This enables the State to respond quickly to emerging needs, such as new vaccination programs, policy changes, or public health emergencies.

Compared to traditional IIS implementations, which often require extensive customization and long deployment cycles, VAULT's approach provides a configurable, extensible solution that accelerates time to value. Features such as automated provider onboarding, scalable interoperability, and integrated reporting reduce administrative burden and improve system adoption. This phased approach aligns with the State's requirement for a structured, low-risk implementation with clear governance and stakeholder engagement.

In summary, VAULT's proposed solution offers a superior approach by combining:

- A unified ecosystem rather than a standalone registry
- Real-time interoperability aligned with national standards
- Advanced analytics and clinical decision support

- A scalable, cloud-based architecture
- A proven, collaborative implementation model

This approach ensures that West Virginia will not only meet the requirements outlined in this RFP, but will also establish a modern, future-ready IIS platform capable of supporting the State's public health mission for years to come.

4.2.1 CDC-BASED GOALS & OBJECTIVES

VAULT's approach to supporting the CDC IIS Functional Standards is centered on delivering a modern, interoperable, and high-performance Immunization Information System (IIS) that aligns directly with national standards while supporting the operational needs of West Virginia. Rather than treating CDC requirements as discrete compliance items, VAULT implements these standards as core system capabilities embedded throughout the platform, including data validation, interoperability, clinical decision support, reporting, and security. This ensures that CDC-aligned functionality is consistently applied across all workflows, data exchanges, and user interactions.

VAULT's solution is continuously maintained in alignment with:

- CDC IIS Functional Standards
- CDC HL7 v2.5.1 Implementation Guides and Message Mapping Guides (MMGs)
- National interoperability initiatives, including FHIR-based data exchange

The platform incorporates real-time validation, standardized data exchange, configurable business rules, and scalable reporting capabilities, enabling West Virginia to maintain high-quality immunization data, support clinical decision-making, and meet federal reporting requirements.

The following table provides a clear mapping of CDC functional areas to VAULT's capabilities and the resulting outcomes for the State.

CDC Functional Area	VAULT Capability	Outcome for West Virginia
Data Quality and Completeness	Real-time validation of inbound HL7 messages, code set enforcement (CVX, MVX, NDC), and deterministic/probabilistic deduplication	Accurate, complete, and reliable immunization records across the population
Interoperability and Data Exchange	HL7 v2.5.1 compliant interfaces, real-time ACK/NACK processing, and FHIR-based APIs for modern integration	Seamless, standards-based data exchange with EHRs, HIEs, pharmacies, and federal systems
Clinical Decision Support (Forecasting)	ACIP-aligned forecasting engine with configurable rules and real-time evaluation of patient immunization status	Improved clinical decision-making and increased vaccination compliance
Coverage Assessment and Reporting	Configurable reporting tools, population definition logic (numerator/denominator), and read-replica-based analytics	Timely, accurate reporting to support public health planning and federal requirements
Patient Identity and Record Management	Advanced patient matching using deterministic and probabilistic algorithms, with ongoing data quality monitoring	Reduced duplicate records and improved continuity of patient immunization histories
Security and Privacy	Role-based access control (RBAC), encryption in transit and at rest, audit logging, and compliance with security standards	Protection of sensitive health data and compliance with federal and State security requirements
Provider Participation	Automated onboarding workflows,	Increased provider participation and improved data submission quality

CDC Functional Area	VAULT Capability	Outcome for West Virginia
and Data Submission	interface validation tools, and provider support capabilities	
Data Access and Usability	Web-based interface, role-based dashboards, and support for external analytics via read replica and APIs	Efficient access to data for providers, administrators, and public health staff
Scalability and Performance	Cloud-based architecture with workload separation and high-volume processing capabilities	Reliable system performance under statewide usage and high data exchange volumes

PrepModEcosystem

4.2.1.1 ESTABLISH AND MAINTAIN A SECURE, CONFIDENTIAL IMMUNIZATION INFORMATION SYSTEM

Security is embedded into every layer of the PrepModEcosystem and is treated as a continuous operational discipline rather than a static feature. VAULT's approach ensures that the IIS meets federal and State requirements for protecting sensitive health information while maintaining system availability, performance, and scalability.

VAULT delivers a comprehensive, policy-driven, and technically enforced security framework that integrates governance, infrastructure, and user enablement to protect data across the entire system lifecycle—from capture and storage to processing and exchange.

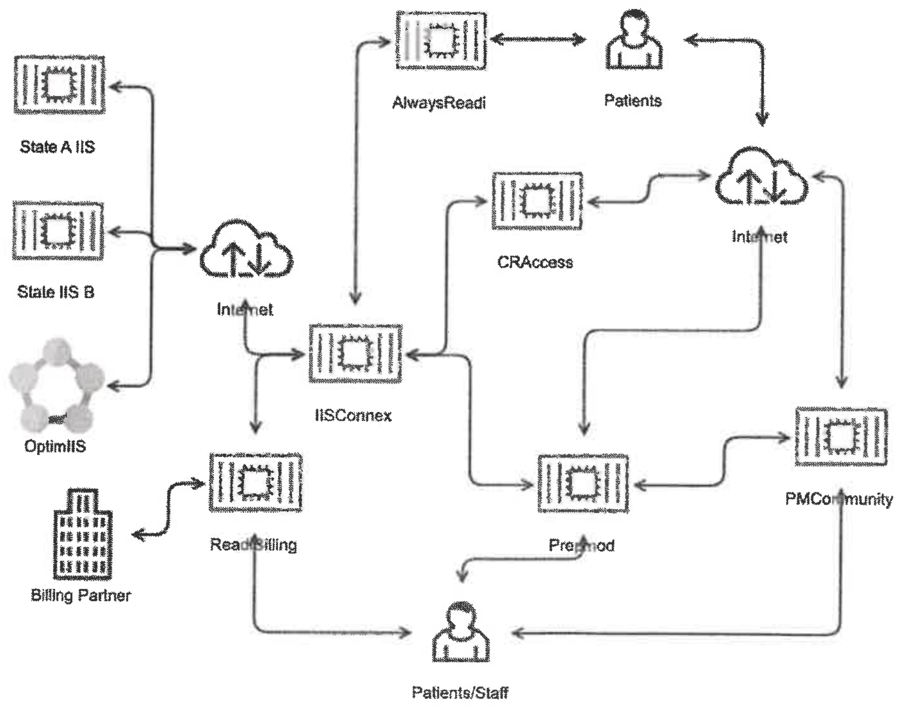
The platform aligns with established cybersecurity frameworks, including:

- NIST SP 800-53
- FedRAMP Moderate
- FIPS 140-2 encryption standards
- SOC 2 Type II practices

These frameworks guide the implementation of administrative, technical, and physical safeguards across infrastructure, application services, and data storage.

Access is governed through a robust role-based access control (RBAC) model, ensuring users can only access data necessary for their responsibilities. Multi-factor authentication (MFA) is supported for privileged and configurable roles, and session management controls prevent unauthorized access.

All data is encrypted both in transit and at rest using industry-standard protocols. Continuous monitoring provides real-time visibility into system activity, while comprehensive audit logs capture user interactions, data access events, and system changes—supporting compliance, forensic analysis, and operational oversight.



VAULT maintains a proactive security posture through:

- Regular vulnerability scanning and automated remediation workflows
- hird-party penetration testing with findings tracked in our incident management system
- Continuous monitoring and threat detection with real-time alerting routed to on-call SRE teams for immediate response

Security patches and updates are applied through controlled change management processes, ensuring protection against evolving threats while maintaining system stability.

Importantly, security policies and procedures are not only documented—they are operationalized within the system through configurable controls, role-based enforcement, and user training. This ensures consistent application of security requirements across all users and workflows.

Together, these capabilities create a layered, resilient security model that enables West Virginia's IIS to operate as a secure, compliant, and high-performing platform capable of supporting both routine operations and large-scale public health response efforts.

What Sets VAULT Apart

Unlike traditional IIS solutions that treat security policies, infrastructure, and user behavior as separate components, VAULT delivers a fully integrated and operationalized security model.

In VAULT's approach:

- Security policies are embedded directly into system functionality, ensuring consistent, system-enforced compliance rather than reliance on manual processes
- Access control, onboarding, and training are interconnected, enabling the State to enforce readiness and compliance before users interact with sensitive data
- Security is designed for real-world public health operations, ensuring protections remain effective during high-volume events, provider onboarding, and emergency response scenarios
- This modern technology foundation — powered by automated testing (RSpec, Capybara, Webmock, Jest) and Tailwind 3.x/4.x for responsive user experiences — enables rapid, secure enhancements without disruption.

This integration of governance, technology, and user enablement reflects VAULT's philosophy of building systems that are not only secure, but operationally effective under real-world conditions.

As a result, West Virginia gains a system that is not only compliant, but enforceable, scalable, and resilient—capable of supporting statewide immunization programs today while adapting to future public health and federal requirements.

4.2.1.1.1 PHYSICAL AND DIGITAL SECURITY

VAULT meets this requirement by implementing a comprehensive, policy-driven approach to both physical and digital security, ensuring that all IIS data and system components are protected in accordance with federal and State requirements for protected health information (PHI), security, and encryption.

The PrepModEcosystem is supported by secure, U.S.-based cloud infrastructure that incorporates physical security controls at the data center level, Physical controls include 24/7 monitored facilities with biometric access, video surveillance, environmental protections, and redundant power/cooling systems, including controlled facility access, environmental protections, and redundancy. These controls are complemented by robust digital security measures embedded throughout the platform.

These technical controls are implemented in alignment with established standards, including NIST, HIPAA, and FIPS encryption requirements, and are reinforced through documented policies and procedures that govern system access, data handling, and operational use.

Together, these capabilities ensure that PHI is protected from unauthorized access, disclosure, and misuse, while remaining securely accessible to authorized users for clinical and public health purposes.

4.2.1.1.1.1 POLICIES AND PROCEDURES

VAULT's PrepModEcosystem is architected for continuous operation through redundant layers across multiple availability zones, automated load balancing, and real-time monitoring.

Comprehensive DR and business continuity plans with defined RTO/RPO, encrypted backups, and routine testing ensure rapid recovery.

Policy Framework and Governance

VAULT maintains documented policies and procedures that address all key aspects of IIS operations, including:

- System access and user management
- Data handling, use, and disclosure
- Security and privacy protections for protected health information (PHI)
- Operational workflows and system usage
- Audit, monitoring, and compliance requirements

These policies are designed to support the full set of IIS functions and capabilities in alignment with CDC IIS Functional Standards and applicable federal and State regulations, including HIPAA.

Policy Management and Continuous Updates

Policies and procedures are:

- Formally documented and version-controlled
- Regularly reviewed and updated to reflect evolving regulatory requirements, security standards, and program needs
- Adaptable to jurisdiction-specific requirements, allowing the State to define and refine policies over time

System-Enforced Policy Implementation

VAULT's platform is designed to operationalize policies through system configuration and controls, ensuring that:

- Access rules are enforced through role-based permissions
- Data handling requirements are embedded in workflows
- Security policies are applied consistently across all system components

Administrative Oversight and State Control

The system provides tools that enable authorized State administrators to manage and enforce policies, including:

- Configuring access rules and user roles
- Monitoring compliance through audit logs and reporting
- Updating policies without requiring system redesign or vendor intervention

Summary

VAULT's approach ensures that IIS policies and procedures are:

- Comprehensive and aligned with industry and public health standards
- Actively maintained and updated
- Embedded within system functionality
- Enforceable and auditable

This provides West Virginia with a governed, compliant, and adaptable policy framework for managing its IIS.

4.2.1.1.1.2 TECHNICAL INFRASTRUCTURE FOR SECURE DATA MANAGEMENT

VAULT meets this requirement by providing a secure, scalable, and policy-aligned technical infrastructure that supports the capture, storage, and processing of patient demographic and immunization data in accordance with established policies and procedures.

Secure Cloud-Based Infrastructure

The system is hosted in a secure, U.S.-based cloud environment that incorporates industry-standard protections, including:

- Network isolation and segmentation, protecting system components and sensitive data
- Continuous monitoring and intrusion detection, identifying and responding to potential threats
- Automated security patching and updates, ensuring infrastructure remains current and protected
- High availability and redundancy, supporting uninterrupted system operations
- Built on a modern Ruby on Rails 8 architecture with Stimulus-driven interfaces, AWS Aurora for data integrity, and Sidekiq 8 for reliable background processing, AWS Lambda

functions for microservices. The entire platform is hosted on AWS using ECR, RDS, OpenSearch, and Secrets Manager, fully orchestrated via ArgoCD and Terraform for zero-downtime, automated deployments and consistent security controls.

Secure Data Capture, Storage, and Processing

The platform is designed to securely manage the full data lifecycle:

- Data capture through validated interfaces (e.g., HL7, FHIR, and web-based entry), with real-time validation to ensure accuracy and completeness
- Secure data storage, with encryption at rest and controlled access based on role and policy
- Data processing and exchange, including real-time updates, deduplication, and integration with external systems

These processes ensure that immunization data is handled securely and consistently across all system functions.

Alignment with Policies and Standards

The infrastructure is designed to operate in accordance with:

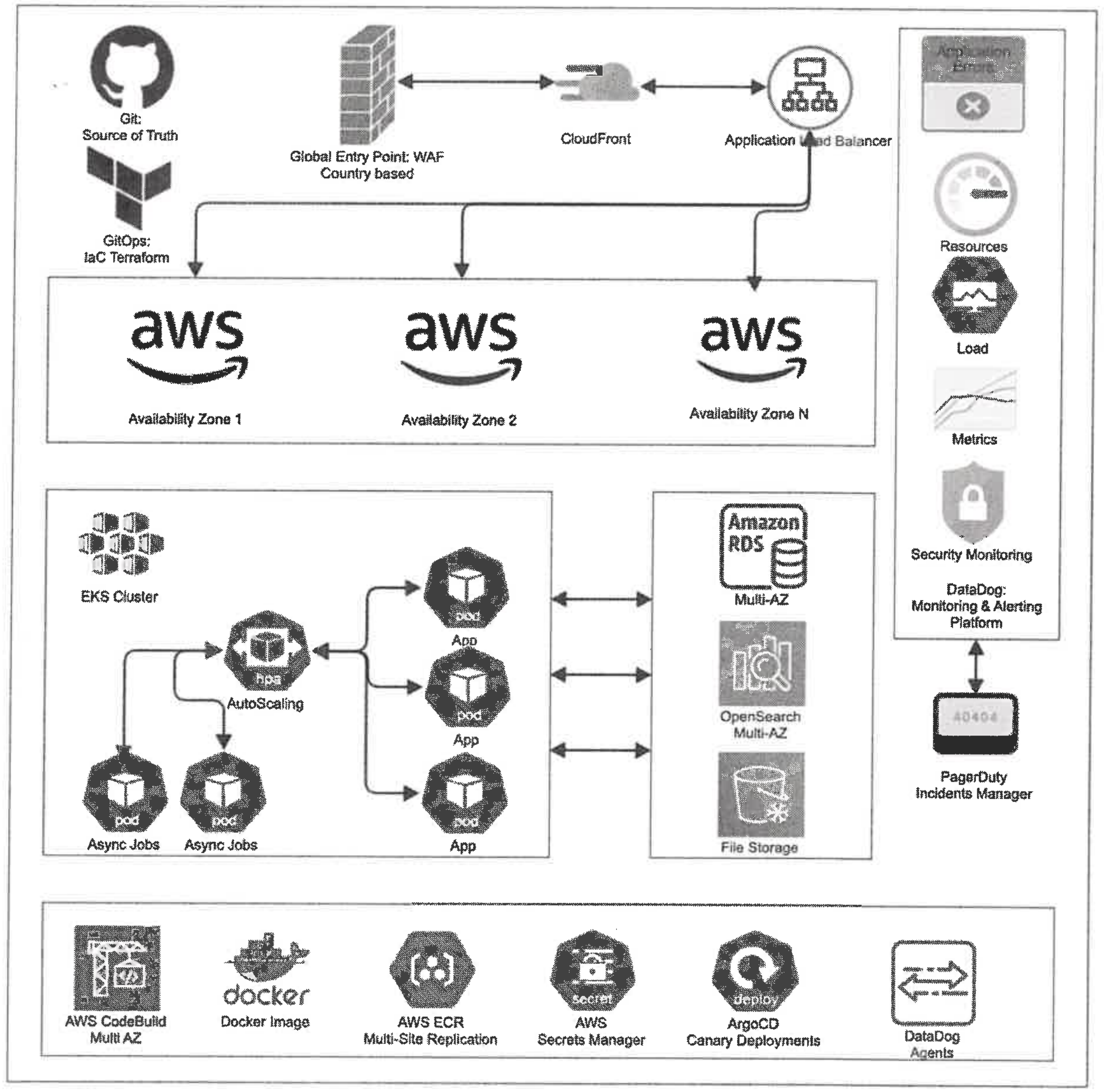
- Documented system policies and procedures, ensuring that data handling and processing align with defined governance
- Industry security standards, including HIPAA and NIST-aligned controls
- CDC IIS Functional Standards, supporting interoperability, data quality, and reporting requirements

Scalability and Performance

The system is engineered to support:

- High-volume data processing, including large-scale vaccination events and routine operations
- Rapid onboarding of providers and partners, without degradation in performance
- Elastic scalability, allowing infrastructure to expand based on demand

Infrastructure Diagram



Summary

VAULT's technical infrastructure ensures that:

- Data is securely captured, stored, and processed throughout its lifecycle
- System operations are aligned with established policies and procedures
- Security controls are applied consistently across all infrastructure layers
- The platform remains scalable, resilient, and capable of supporting statewide operations

This provides West Virginia with a secure, reliable, and future-ready infrastructure for managing immunization data.

4.2.1.1.1.3 USER TRAINING AND SECURITY AWARENESS

VAULT meets this requirement by providing comprehensive, role-based training and ongoing security awareness programs to ensure that all users understand their responsibilities related to data security, privacy, and compliance.

Role-Based Training and Onboarding

The system supports structured, role-based training that is aligned with user responsibilities, including:

- Security and privacy requirements for protected health information (PHI)
- Proper data entry, handling, and reporting procedures
- System usage aligned with defined policies and workflows

As part of the onboarding process, the system supports policy-driven access activation, allowing the State to require completion of applicable training prior to granting system access.

Ongoing Training and Reinforcement

VAULT supports continuous user education through:

- Periodic refresher training, ensuring users remain current on policies and procedures
- Updated training materials, reflecting changes in system functionality, regulations, or State policies
- On-demand documentation and guidance, accessible within the system

This ensures that training is not a one-time activity, but an ongoing component of system use.

Alignment with Policies and Compliance

Training is directly aligned with system policies and procedures, ensuring that:

- Users understand and adhere to access control and data use policies
- Data handling practices are consistent across all user types
- Compliance with regulatory and State requirements is maintained

Monitoring and Accountability

The system supports oversight of training and compliance by enabling:

- Tracking of training completion, where required by the State
- Alignment of user access with training status, reinforcing policy enforcement
- Auditability of user activity, ensuring accountability for data access and use

Summary

VAULT's approach ensures that:

- Users are trained prior to and throughout system use
- Training is aligned with roles, policies, and system functionality
- Security and privacy responsibilities are clearly understood and reinforced
- Compliance is supported through training, access control, and auditability

This provides West Virginia with a sustainable and enforceable approach to user training and security awareness.

4.2.1.1.2 DISASTER AVOIDANCE AND RECOVERY

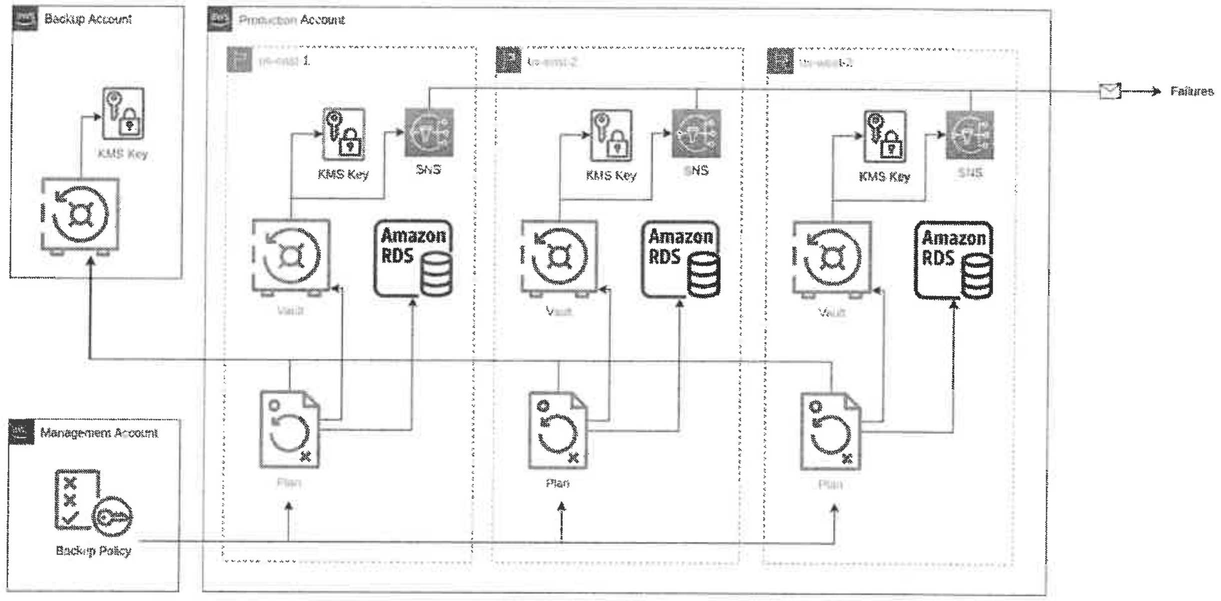
VAULT meets this requirement by providing a highly available, fault-tolerant, and resilient infrastructure designed to prevent service disruptions, minimize downtime, and ensure rapid recovery in alignment with industry standards for disaster avoidance, mitigation, and recovery.

Our internal Site Reliability Engineering (SRE) practices drive this resilience through regular chaos engineering exercises, automated disaster-recovery drills, documented runbooks for every failure mode, and clearly defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that are tested quarterly.

The PrepModEcosystem is architected to support continuous system operation through:

- Redundant application and database layers, deployed across multiple availability zones to eliminate single points of failure
- Automated load balancing and elastic scaling, maintaining performance during peak demand and large-scale public health events
- Continuous system monitoring and real-time alerting, enabling early detection and mitigation of potential issues

To support disaster recovery and downtime mitigation, VAULT maintains comprehensive, actively tested disaster recovery (DR) and business continuity plans that include defined RTO/RPO, automated encrypted backups, rapid failover, and routine testing — all governed by our SRE playbook.



4.2.1.1.2.1 INFRASTRUCTURE FOR DISASTER AVOIDANCE

VAULT meets this requirement by providing a highly available, fault-tolerant infrastructure designed to prevent service disruptions and ensure continuous system operation, in alignment with industry standards for disaster avoidance and system resilience.

The platform is architected to proactively mitigate the risk of outages through:

- Redundant application and database layers, deployed across multiple availability zones to eliminate single points of failure
- Automated load balancing, distributing traffic to prevent system overload and maintain performance during peak demand
- Continuous system health monitoring, with real-time alerting to detect and address potential issues before they impact operations

- Proactive, elastic scaling, enabling the system to automatically adjust capacity in response to spikes in usage, including large-scale vaccination campaigns and emergency response scenarios

These capabilities are supported by a cloud-based infrastructure aligned with NIST and FedRAMP Moderate principles, ensuring that disaster avoidance is built into the core system architecture.

In addition, infrastructure design and operations are aligned with established system policies and procedures, ensuring that resilience and availability requirements are consistently applied and maintained.

These capabilities have been proven in real-world conditions. During large-scale vaccination efforts, the system successfully supported high transaction volumes without degradation in performance, demonstrating its ability to maintain availability under significant load.

4.2.1.1.2.2 RECOVERY PLANNING AND TESTING

VAULT meets this requirement by establishing and maintaining comprehensive, actively tested disaster recovery (DR) and business continuity plans designed to minimize system downtime and ensure rapid restoration of services in the event of disruption.

Disaster Recovery Planning and Capabilities

The platform incorporates a structured disaster recovery framework that includes:

- Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) aligned with public health operational and service-level requirements
- Automated, encrypted data backups, stored in secure, geographically distributed environments
- Rapid failover capabilities, enabling transition to secondary environments in the event of primary system failure
- High availability architecture, reducing the likelihood of full system disruption

Testing and Continuous Readiness

VAULT ensures ongoing readiness through:

- Routine disaster recovery testing and drills, validating system recovery processes and ensuring staff preparedness
- Continuous monitoring and alerting, enabling rapid detection of issues and initiation of recovery procedures
- Regular review and refinement of DR plans, incorporating lessons learned from testing and real-world system performance

Alignment with Policies and Service Expectations

Disaster recovery and business continuity processes are aligned with:

- Established system policies and procedures, ensuring consistent application of recovery protocols
- Service-level expectations (SLAs), supporting system availability and uninterrupted data access
- Industry standards for resilience and recovery, including NIST-aligned practices

Summary

VAULT's disaster recovery approach ensures that:

- System disruptions are rapidly detected and addressed
- Downtime is minimized through failover and high availability design
- Data integrity is preserved through secure, redundant backups
- Recovery processes are continuously tested and improved

This provides West Virginia with a resilient, well-governed, and continuously validated recovery framework capable of maintaining system availability under a wide range of conditions.

4.2.1.1.3 SERVICE EXPECTATIONS AND SERVICE-LEVEL AGREEMENTS

VAULT meets this requirement by implementing clearly defined, measurable, and enforceable service-level agreements (SLAs) supported by a highly available infrastructure and coordinated operational model designed to ensure continuous system availability and uninterrupted data flows.

The PrepModEcosystem integrates performance standards, real-time monitoring, and responsive support processes to maintain system reliability across all conditions. SLAs define expectations for uptime, response, and resolution, while infrastructure and operations are purpose-built to consistently meet these targets.

Our Site Reliability Engineering (SRE) practices drive these commitments through:

- Service Level Objectives (SLOs) of 99.99 % availability for production environments and 99.9 % for staging deployments, tracked in Datadog for every service
- Error-budget tracking with automated alerts sent to dedicated Slack channels when budgets are at risk of being burned
- Continuous monitoring of latency, traffic, saturation, and error rates using Datadog APM and infrastructure metrics
- Forecast monitoring to anticipate capacity needs and prevent performance degradation
- Monthly capacity reviews that assess CPU/memory usage, traffic patterns, and upcoming events to proactively adjust resources

These practices ensure SLA commitments are not only established, but actively measured, reported, and continuously improved.

Key capabilities include:

- Defined and measurable SLA performance criteria, including uptime, response times, and resolution targets
- Continuous system monitoring and real-time alerting with automated incident creation and on-call paging
- Scalable, redundant infrastructure supporting high availability and sustained performance under varying demand
- Dedicated SRE-led incident management processes, including classification, escalation, root-cause analysis, blameless post-mortems, and corrective actions
- Ongoing performance reporting and transparency, providing the State with visibility into system availability, error budgets, SLO compliance, and service outcomes

4.2.1.1.3.1 SERVICE-LEVEL AGREEMENTS (SLAS)

SLA performance is actively managed and enforced through:

- Continuous system monitoring and real-time alerting, enabling rapid identification of SLA-impacting events
- Regular performance reporting, including system availability metrics, error budgets, incident response times, and resolution outcomes

- Transparent communication with Agency stakeholders, ensuring that service disruptions and performance issues are promptly reported and addressed

Collaboration and Continuous Improvement

SLAs are established collaboratively with the Agency to align with operational priorities and public health needs. VAULT continuously refines SLA targets and performance based on:

- System performance trends and error-budget consumption
- Incident analysis, root-cause evaluation, and blameless post-mortems
- Monthly capacity reviews and forecast monitoring
- Evolving State requirements and program priorities

Summary

VAULT's SLA approach ensures that system performance expectations are clearly defined and measurable, service levels are continuously monitored and enforced, issues are rapidly identified, escalated, and resolved, and the State has full visibility into system performance and accountability. This provides West Virginia with a reliable, transparent, and performance-driven service model that supports continuous system availability and uninterrupted data flow.

4.2.1.1.3.2 INFRASTRUCTURE AND OPERATIONAL SUPPORT FOR SLA COMPLIANCE

VAULT meets this requirement by maintaining a highly available, scalable infrastructure and coordinated operational model specifically designed to fulfill and sustain defined service-level agreements (SLAs) for system availability, performance, and responsiveness.

Infrastructure Supporting SLA Fulfillment

The platform leverages a secure, cloud-based architecture that enables consistent SLA performance through:

- Scalable, elastic infrastructure, supporting high availability and sustained performance under varying load conditions
- Redundant system architecture, minimizing the impact of component failures and ensuring continuity of operations
- Continuous monitoring of system performance, availability, and data exchange processes, ensuring real-time visibility into SLA adherence

- Automated alerting and incident detection, enabling rapid response to potential SLA-impacting events

These capabilities ensure that infrastructure performance directly supports SLA commitments for uptime and data availability.

Operational Processes and SLA Execution

SLA performance is reinforced through structured operational processes, including:

- Dedicated support and operations teams, responsible for system monitoring, incident response, and issue resolution
- Formal incident management processes, including classification, escalation, root cause analysis, and corrective actions
- Preventive maintenance and controlled system updates, ensuring ongoing stability and performance

This coordinated approach ensures that operational activities are aligned with SLA targets and continuously support system reliability.

Continuous Improvement and Real-World Validation

VAULT continuously refines its infrastructure and operational processes based on:

- Performance monitoring and SLA reporting
- Incident trends and root cause analysis
- Lessons learned from high-volume public health deployments

These capabilities have been validated in real-world conditions, including large-scale vaccination efforts where the system maintained performance and availability under significant demand.

Summary

VAULT's approach ensures that:

- Infrastructure and operations are directly aligned with SLA requirements
- System availability and performance are continuously monitored and maintained
- Issues are rapidly detected, addressed, and resolved

- SLA performance improves over time through continuous evaluation and refinement

This provides West Virginia with a reliable, scalable, and performance-driven operational model that ensures consistent fulfillment of service-level expectations.

4.2.1.2 CONTINUOUSLY IMPROVE IIS DATA QUALITY

VAULT meets the requirements of this section by delivering a comprehensive, policy-aligned framework for managing, monitoring, and continuously improving data quality across the IIS.

The PrepModEcosystem is designed to ensure that immunization data is accurate, complete, timely, and reliable, supporting both clinical decision-making and public health operations. This is achieved through an integrated approach that combines real-time validation, advanced matching and deduplication, standardized data capture, continuous monitoring, and structured provider engagement.

Data quality is managed across the full data lifecycle—from initial entry and ingestion to ongoing monitoring and reporting—ensuring that issues are not only identified, but proactively prevented and resolved. The system supports the creation and maintenance of a single, longitudinal patient record, reducing fragmentation and improving continuity of care.

Through configurable dashboards, analytics, and reporting tools, the State is provided with real-time visibility into data quality performance at the system, organization, and provider levels. These insights enable targeted interventions, training, and outreach to improve data quality at the source.

All data quality processes are aligned with CDC IIS Functional Standards and jurisdictional policies and procedures, ensuring consistency, compliance, and adaptability to evolving federal and State requirements.

Together, these capabilities create a closed-loop data quality model in which data is continuously validated, monitored, corrected, and improved—ensuring that the IIS serves as a trusted, high-quality, and actionable source of immunization data.

Data Quality Framework Overview:

- Inbound validation (HL7/FHIR)

- Deduplication (deterministic + probabilistic)

- Address standardization

- Continuous monitoring dashboards

- Provider feedback loop

What Sets VAULT Apart

Unlike traditional IIS platforms that focus primarily on data collection and retrospective reporting, VAULT provides a proactive, system-driven data quality and improvement model that operates continuously across the data lifecycle.

In VAULT's approach:

- Data quality is enforced at the point of entry, through real-time validation, standardization, and matching—reducing errors before they enter the system
- Monitoring is continuous and actionable, with dashboards, alerts, and performance metrics that provide real-time visibility into data quality at the provider, organizational, and system levels
- Providers are actively engaged through structured feedback and training, enabling targeted improvements at the source rather than relying solely on downstream correction
- Data quality processes are embedded within system workflows, ensuring consistent alignment with policies and procedures without requiring manual intervention

This integrated model transforms the IIS from a passive repository into an active data quality engine, where data is continuously validated, improved, and operationalized.

Because VAULT's platform is designed by public health practitioners and proven in high-volume, real-world environments, it supports not only data integrity, but effective public health execution—including accurate reporting, targeted outreach, and informed decision-making.

As a result, West Virginia gains a system that not only meets data quality requirements, but continuously improves the quality, usability, and impact of its immunization data over time.

4.2.1.2.1 VALIDATION OF PATIENT DEMOGRAPHIC AND VACCINATION DATA

VAULT meets the requirements of this subsection by integrating advanced matching, real-time validation, continuous monitoring, and provider engagement to prevent, detect, and resolve data quality issues across the full data lifecycle.

The PrepModEcosystem integrates advanced matching algorithms, real-time validation, continuous monitoring, and structured provider engagement to both prevent and resolve data quality issues. These capabilities support the creation and maintenance of a single, longitudinal patient record, while reducing duplication, standardizing data inputs, and improving consistency across multiple reporting sources.

Data quality is continuously evaluated through system-level analytics, dashboards, and reporting tools, providing visibility into key performance metrics such as completeness, timeliness, and accuracy at the system, organizational, and provider levels. Automated alerts and exception reporting enable early identification of issues, while integrated feedback and training mechanisms support corrective action at the source.

All data quality processes are aligned with CDC IIS Functional Standards and jurisdictional policies and procedures, ensuring consistent application of validation rules, monitoring practices, and reporting requirements. This alignment enables the State to maintain compliance with federal guidance while adapting to evolving program needs.

Together, these capabilities establish a closed-loop data quality model in which data is continuously validated, monitored, corrected, and improved. This approach ensures that West Virginia's IIS functions as a trusted, accurate, and actionable source of immunization data to support clinical care, public health reporting, and program decision-making.

4.2.1.2.1.1 DUPLICATE AND FRAGMENTED RECORD MANAGEMENT

VAULT meets this requirement by providing a comprehensive, policy-aligned approach to the identification, prevention, and resolution of duplicate and fragmented patient records, ensuring the integrity and continuity of IIS data.

Advanced Matching and Record Reconciliation

The system employs a combination of deterministic and probabilistic matching algorithms to continuously identify and reconcile duplicate or fragmented records submitted from multiple providers and systems.

This process:

- Operates in real time and continuously, ensuring ongoing data quality
- Consolidates records into a single, longitudinal patient profile
- Supports accurate clinical decision-making and reporting across the IIS

Prevention and Data Quality Controls

In addition to resolving duplicates, the system actively supports prevention of duplicate record creation through:

- Real-time validation and matching at the point of data entry and ingestion
- Standardized data capture workflows, reducing variability across reporting sources
- Configurable matching thresholds and rules, aligned with jurisdictional policies and procedures

These capabilities reduce the likelihood of duplicate records entering the system and improve overall data quality.

User-Assisted Review and Policy Alignment

The system supports user-assisted review workflows, enabling authorized jurisdictional staff to:

- Review potential matches and conflicts
- Apply policy-defined rules to resolve complex cases
- Maintain data integrity in high-volume and multi-source environments

All matching and resolution processes are aligned with established policies and procedures, ensuring consistency, transparency, and auditability.

Summary

VAULT's approach ensures that:

- Duplicate and fragmented records are continuously identified and resolved
- Duplicate record creation is proactively prevented
- Longitudinal patient records are accurately maintained
- Data quality processes are aligned with jurisdictional policies and procedures

This provides West Virginia with a reliable, scalable, and policy-driven approach to maintaining high-quality patient data across the IIS.

4.2.1.2.1.2 DATA QUALITY MONITORING

VAULT meets this requirement by providing continuous, policy-aligned data quality monitoring capabilities that evaluate and improve the completeness, timeliness, and consistency of IIS data.

System-Level Monitoring and Analytics

The platform utilizes real-time analytics and data quality monitoring tools to assess data across key dimensions, including:

- Completeness, ensuring required demographic and vaccination fields are populated
- Timeliness, tracking data submission and reporting latency
- Consistency and validity, identifying discrepancies, formatting issues, and outliers

These metrics are presented through configurable dashboards and reports, providing visibility into data quality at the system, organization, and provider levels.

Alerting and Issue Identification

The system supports automated alerts and exception reporting, enabling the State to:

- Identify data quality issues as they occur
- Detect trends or recurring issues across providers or regions
- Prioritize remediation based on severity and impact

This ensures that data quality issues are detected early, before they affect downstream reporting and analysis.

Policy Alignment and Governance

Data quality monitoring is aligned with established policies and procedures, ensuring that:

- Data quality thresholds and validation rules reflect jurisdictional standards
- Monitoring processes support compliance with federal and State requirements
- Data quality expectations are consistently applied across all reporting entities

Action and Continuous Improvement

The platform supports a closed-loop data quality improvement process, enabling:

- Identification of issues through monitoring and analytics
- Targeted follow-up and correction at the provider or system level
- Ongoing tracking of improvements over time

This proactive approach reduces downstream impacts on reporting, forecasting, and program operations.

Summary

VAULT's data quality monitoring approach ensures that:

- Data quality is continuously evaluated across key dimensions
- Issues are identified early through automated monitoring and alerting
- Monitoring is aligned with policies and procedures
- Data quality improves over time through actionable insights and feedback

This provides West Virginia with a transparent, proactive, and continuously improving data quality framework.

4.2.1.2.1.3 ADDRESS STANDARDIZATION AND VALIDATION

VAULT meets this requirement by providing automated address standardization and validation capabilities, supported by both integrated third-party services and internal data quality processes, to ensure accuracy and consistency of geographic data within the IIS.

Address Validation and Standardization Tools

The system leverages industry-leading address validation services, including SmartyStreets, to:

- Standardize address formats in accordance with postal and geographic reference standards
- Validate addresses in real time, ensuring accuracy at the point of data entry and ingestion
- Correct and normalize address data, reducing variability across multiple reporting sources

These capabilities ensure that address data is consistently formatted and aligned with recognized standards.

Integrated Data Quality Processes

Address validation is embedded within system workflows, including:

- Real-time validation during data entry, preventing incorrect or incomplete address submission
- Batch validation and correction processes, improving data quality for existing records
- Alignment with jurisdictional policies and procedures, ensuring consistent application of address standards

Support for Public Health and Geographic Analysis

Accurate address data enables the State to:

- Conduct reliable geographic and population-based reporting
- Identify regional disparities and gaps in coverage
- Support targeted outreach and intervention strategies
- Ensure reporting aligns with correct jurisdictional boundaries

Summary

VAULT's approach ensures that:

- Address data is standardized and validated using trusted tools and processes
- Data quality is maintained at both the point of entry and across existing records
- Address validation is aligned with policies and procedures
- Geographic reporting and population analysis are accurate and reliable

This provides West Virginia with a high-quality, location-aware data foundation to support public health decision-making.

4.2.1.2.1.4 PROVIDER FEEDBACK AND TRAINING

VAULT meets this requirement by providing a structured, system-supported feedback and training model that improves data quality at the source through continuous engagement with IIS partners and providers.

Automated Feedback and Performance Visibility

The system delivers timely, actionable feedback to providers through:

- Real-time validation feedback, alerting users to errors or inconsistencies at the point of data entry
- Data quality reports and dashboards, providing visibility into completeness, timeliness, and accuracy at the provider level
- Exception and error reporting, enabling providers to identify and correct issues quickly

This ensures that providers are aware of data quality issues as they occur and can take immediate corrective action.

Training and Ongoing Education

VAULT supports data quality improvement through role-based training and continuous education, including:

- Initial onboarding and training, ensuring providers understand data submission requirements and best practices
- Ongoing training and guidance, aligned with system updates, policy changes, and identified data quality issues
- Targeted training interventions, based on provider-specific performance and data quality trends

All training and feedback processes are aligned with established policies and procedures, ensuring consistent expectations across all reporting entities.

Collaborative and Continuous Improvement Model

VAULT works in partnership with the State to support:

- Ongoing provider engagement and communication
- Identification of systemic data quality issues
- Continuous improvement initiatives based on performance metrics and trends

This approach has been successfully applied in prior implementations, including Maryland, where sustained engagement with providers contributed to measurable improvements in data completeness and timeliness.

Summary

VAULT's approach ensures that:

- Providers receive timely, actionable feedback on data quality
- Training is continuous, targeted, and aligned with system policies
- Data quality improves at the point of entry
- Improvements are sustained over time through ongoing engagement and monitoring

This provides West Virginia with a proactive and scalable model for improving data quality across all IIS partners.

4.2.1.2.1.5 COMPLIANCE WITH FEDERAL AND JURISDICTIONAL METRICS

VAULT meets this requirement by supporting the measurement, monitoring, and continuous improvement of federal and jurisdictional data quality metrics, in alignment with CDC IIS Functional Standards.

Data Quality Metrics and Monitoring

The system tracks and reports on key data quality indicators, including:

- Completeness, ensuring required demographic and vaccination fields are populated
- Timeliness, measuring the speed of data submission and reporting
- Accuracy and validity, identifying inconsistencies, errors, and outliers in submitted data

These metrics are accessible through configurable dashboards and reporting tools, providing visibility at the system, organization, and provider levels.

Alignment with CDC and Jurisdictional Requirements

The platform is designed to support compliance with:

- CDC IIS Functional Standards and data quality benchmarks
- Jurisdiction-specific reporting requirements and performance targets

- Evolving federal guidance, ensuring ongoing alignment with national initiatives

VAULT supports the State in generating required reports and monitoring compliance with these standards.

Actionable Insights and Continuous Improvement

Data quality metrics are integrated into a continuous improvement framework, enabling the State to:

- Identify gaps and trends in data quality across providers and regions
- Target interventions, training, and outreach based on performance
- Monitor improvements over time and adjust strategies accordingly

This ensures that data quality monitoring translates into measurable improvements.

Summary

VAULT's approach ensures that:

- Data quality metrics are clearly defined, measurable, and visible
- Monitoring is aligned with CDC and State requirements
- Data quality issues are identified and addressed proactively
- Continuous improvement is supported through actionable insights

This provides West Virginia with a transparent, standards-aligned, and continuously improving data quality framework, ensuring that the IIS remains a trusted and authoritative source of immunization data.

4.2.1.3 PROMOTE ELECTRONIC DATA EXCHANGE BETWEEN THE IIS AND ITS PARTNERS AND PROVIDERS

Overview

VAULT meets the requirements of this section by delivering a standards-based, scalable, and operationally integrated interoperability framework that enables secure, reliable, and efficient electronic data exchange across IIS partners, providers, and external systems.

The PrepModEcosystem supports end-to-end interoperability, including:

- Standards-compliant data exchange, leveraging HL7 v2.5.1, FHIR APIs, and CDC implementation guides
- Rapid onboarding and integration of partners and providers, supporting diverse systems and technical capabilities
- Continuous, real-time monitoring of data exchange, providing visibility into interface performance, data quality, and participation
- Structured error detection and resolution workflows, ensuring timely correction of issues and sustained data integrity

These capabilities are supported through IISConnex, which provides a centralized platform for ingesting, validating, transforming, routing, and managing immunization data across all interfaces.

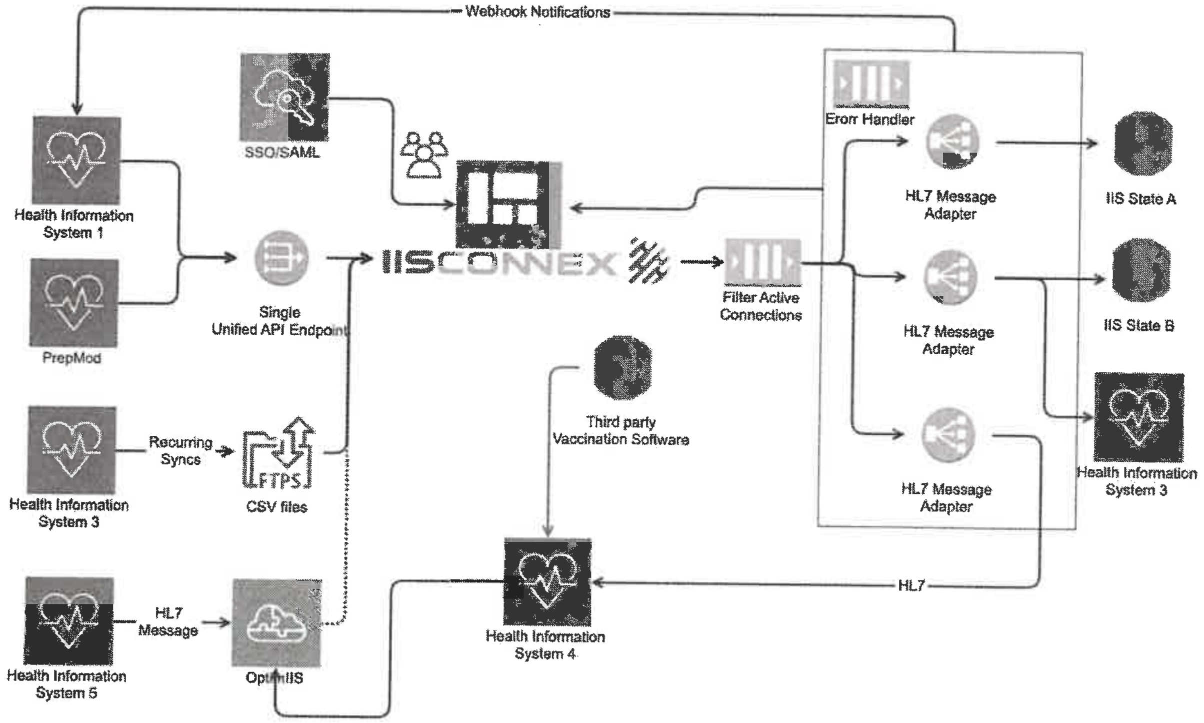
All interoperability processes are aligned with federal standards and jurisdictional policies, ensuring compliance while maintaining flexibility to adapt to evolving requirements.

Together, these capabilities enable West Virginia to maintain reliable, high-quality, and scalable data exchange, supporting both routine operations and high-demand public health scenarios.

What Sets VAULT Apart

Unlike traditional IIS platforms that treat interoperability as a set of interfaces, VAULT delivers a fully operational and policy-driven data exchange model.

In VAULT's approach:


Webhook Notifications
SSO/SAML
Health Information System 1
PrepMod
Single Unified API Endpoint
IISCONNEX
Filter Active Connections
Erorr Handler
HL7 Message Adapter
HL7 Message Adapter
HL7 Message Adapter
IIS State A
IIS State B
Health Information System 3
Third party Vaccination Software
Health Information System 3
Recurring Syncs
FTPS
CSV files
Health Information System 5
HL7 Message
OptimIIS
Health Information System 4
HL7

- Interoperability is managed as a continuous operational lifecycle, integrating onboarding, monitoring, and resolution into a single coordinated system
- Data exchange is governed by configurable, State-controlled policies, enabling the State to define what data is shared, with whom, and under what conditions
- Interoperability is actively monitored and managed in real time, ensuring visibility, accountability, and rapid response to issues
- The system supports real-world public health operations, including high-volume data exchange and dynamic data sharing needs during emergencies

This integrated model transforms interoperability from a technical capability into a strategic operational asset, enabling the State to not only exchange data, but to control, optimize, and adapt data sharing across its public health ecosystem.

As a result, West Virginia gains a solution that is not only standards-compliant, but flexible, scalable, and operationally effective, capable of supporting evolving data exchange needs and future public health initiatives.

4.2.1.3.1 ELECTRONIC DATA EXCHANGE AND INTEROPERABILITY MANAGEMENT

VAULT meets the requirements of this subsection by providing a comprehensive, standards-based, and operationally integrated approach to electronic data exchange, enabling the State to efficiently connect, manage, and optimize data sharing across IIS partners and providers.

The PrepModEcosystem supports the full lifecycle of interoperability, including:

- Standards-based data exchange, using HL7 v2.5.1, FHIR APIs, and CDC-aligned implementation guides
- Structured onboarding and integration workflows, enabling rapid enrollment and activation of providers and partner systems
- Continuous, real-time monitoring of data exchange, providing visibility into interface performance, data quality, and provider participation
- System-supported error identification and resolution, ensuring timely correction of issues and ongoing data integrity

These capabilities are supported through IISConnex, which provides a centralized and coordinated platform for ingesting, validating, transforming, routing, and managing immunization data across all interfaces.

In addition, VAULT enables policy-driven, State-controlled data exchange, allowing jurisdictions to define what data is shared, with whom, and under what conditions. This flexibility is particularly valuable in dynamic environments, including public health emergencies, where data sharing requirements may evolve rapidly.

Together, these capabilities create a closed-loop interoperability model in which data exchange is continuously monitored, managed, and improved—ensuring reliability, scalability, and compliance with federal and jurisdictional standards.

This approach provides West Virginia with a modern, flexible, and operationally effective interoperability framework that supports both routine data exchange and high-demand public health scenarios.

4.2.1.3.1.1 INTEROPERABILITY STANDARDS AND DATA EXCHANGE

VAULT meets this requirement by supporting standards-based, flexible, and policy-driven data exchange in alignment with CDC-endorsed interoperability standards for message content, format, and transport.

Standards-Based Interoperability

The system supports data exchange using:

- HL7 v2.5.1 immunization messaging, compliant with CDC Implementation Guides and Message Mapping Guides (MMGs)
- FHIR-based APIs, enabling modern, real-time interoperability with external systems
- Standards-based transport protocols, supporting secure, reliable message exchange

All incoming and outgoing messages are validated against applicable standards to ensure data quality, consistency, and compliance.

Flexible and Future-Ready Architecture

VAULT's architecture supports the parallel use of HL7 and FHIR, enabling the State to:

- Maintain existing integrations while adopting modern interoperability approaches
- Expand real-time data exchange capabilities over time
- Participate in national data exchange frameworks and initiatives

Policy-Driven and Configurable Data Exchange

Unlike traditional IIS platforms, VAULT enables State-controlled, policy-driven data exchange, allowing jurisdictions to define:

- What data is shared (e.g., vaccine type, demographic elements, or other attributes)
- With whom data is shared (e.g., specific providers, systems, or partner jurisdictions)

- Under what conditions data is exchanged, based on jurisdictional policies and program requirements

This capability is particularly valuable during public health emergencies, where States may need to rapidly adjust data sharing rules to support coordinated response efforts while maintaining control over sensitive information.

Summary

VAULT's approach ensures that:

- Data exchange is fully compliant with CDC-endorsed interoperability standards
- The system supports both current and emerging interoperability frameworks
- Data sharing is flexible, configurable, and aligned with jurisdictional policies
- The State maintains control over how and when data is exchanged

This provides West Virginia with a modern, standards-compliant, and highly adaptable interoperability framework.

4.2.1.3.1.2 PARTNER AND PROVIDER ONBOARDING FOR DATA EXCHANGE

VAULT meets this requirement by providing a structured, scalable, and system-supported onboarding model that enables the efficient recruitment, enrollment, and activation of IIS partners and providers for electronic data exchange.

End-to-End Onboarding Lifecycle

The PrepModEcosystem supports the full lifecycle of partner onboarding—from initial engagement through production data exchange—through a standardized and repeatable process, including:

- Provider and partner enrollment, capturing required organizational and technical information
- Interface configuration and connectivity setup, supporting HL7 and FHIR-based integrations
- Validation and testing of data submissions, ensuring compliance with CDC and jurisdictional standards
- Approval and activation, enabling providers to begin live data exchange

These workflows are supported within the system, ensuring consistency and reducing onboarding time.

System-Supported Workflow and Visibility

The platform provides tools to manage and track onboarding activities, including:

- Centralized tracking of onboarding status, allowing the State to monitor progress across all partners
- Standardized templates and testing protocols, ensuring consistent implementation
- Validation tools and feedback mechanisms, enabling providers to resolve issues prior to production

This provides the State with visibility and control over onboarding activities at scale.

Scalability and Real-World Experience

VAULT's onboarding model is designed for scalability and rapid deployment, supporting:

- Onboarding of diverse provider types, including hospitals, pharmacies, and community-based organizations
- Expansion of electronic data exchange during routine operations and public health emergencies

In prior implementations, including Maryland, VAULT worked closely with public health teams to onboard a wide range of providers, demonstrating the ability to scale onboarding efforts efficiently across complex environments.

Policy Alignment and Consistency

All onboarding processes are aligned with State-defined policies and procedures, ensuring that:

- Providers meet participation and data exchange requirements prior to activation
- Data submissions are validated and compliant with applicable standards
- Onboarding is consistent across all partner types and organizations

Summary

VAULT's onboarding approach ensures that:

- Partners and providers are efficiently recruited, enrolled, and activated
- Onboarding processes are structured, repeatable, and scalable
- Integration is completed accurately and in compliance with standards
- The State has visibility and control over onboarding activities

This provides West Virginia with a highly efficient and scalable model for expanding electronic data exchange across the IIS ecosystem.

4.2.1.3.1.3 MONITORING AND EVALUATION OF DATA EXCHANGE

VAULT meets this requirement by providing continuous, real-time monitoring of electronic data exchange, enabling the State to assess performance, ensure data quality, and maintain effective participation across all IIS partners and providers.

Real-Time Monitoring and Visibility

The system provides comprehensive monitoring of all electronic interfaces, including:

- Message volume and submission frequency, tracking provider participation and data flow activity
- Interface performance and transmission status, identifying delays, failures, or disruptions in data exchange
- Data quality indicators, including completeness, timeliness, and validity of submitted data

These metrics are available through configurable dashboards and reporting tools, providing visibility at the system, organization, and provider levels.

Automated Alerts and Issue Identification

The platform supports automated alerts and exception reporting, enabling the State to:

- Detect interface issues and data anomalies in real time
- Identify providers with inconsistent or incomplete submissions
- Prioritize follow-up actions based on severity and impact

This ensures that issues are identified early, before they affect reporting or program operations.

Provider Performance and Accountability

Monitoring capabilities support ongoing evaluation of provider participation and performance, enabling the State to:

- Assess compliance with reporting requirements
- Identify gaps in data submission across regions or provider types
- Track improvements over time

Integration with Data Quality and Operational Workflows

Electronic data exchange monitoring is integrated with broader system capabilities, including:

- Data quality monitoring and improvement processes
- Provider feedback and training workflows
- Incident management and issue resolution processes

This creates a closed-loop operational model, ensuring that identified issues are not only detected, but addressed and resolved.

Summary

VAULT's approach ensures that:

- Electronic data exchange is continuously monitored in real time
- The State has visibility into interface performance and provider participation
- Issues are identified early through automated alerts and analytics
- Monitoring is integrated with data quality and operational workflows

This provides West Virginia with a proactive, transparent, and actionable approach to managing electronic data exchange across the IIS ecosystem.

4.2.1.3.1.4 INVESTIGATION AND RESOLUTION OF DATA EXCHANGE ISSUES

VAULT meets this requirement by providing a structured, system-supported process for identifying, investigating, resolving, and preventing data exchange errors, ensuring reliable and uninterrupted interoperability across IIS partners and providers.

Automated Error Detection and Routing

Through IISConnex, the system automatically:

- Validates incoming and outgoing messages against CDC and jurisdictional standards
- Identifies errors and anomalies in real time
- Routes failed messages to structured error queues, where they are categorized by error type and severity

This enables rapid identification and prioritization of issues.

Centralized Error Management and Visibility

The platform provides clear visibility into error conditions, including:

- Affected records and message details
- Error types and root causes
- Provider-specific and system-level trends

These capabilities allow the State and support teams to efficiently investigate and address issues.

Resolution Workflows and Partner Engagement

VAULT supports coordinated resolution workflows, including:

- Structured triage and resolution processes, ensuring timely handling of errors
- Collaboration with providers, EHR vendors, and partners, providing guidance and technical support
- Ongoing communication and follow-up, ensuring issues are fully resolved

Prevention and Continuous Improvement

Error resolution is integrated into a continuous improvement model, enabling:

- Identification of recurring issues and root causes

- Updates to validation rules, workflows, and training
- Reduction of future errors through system and process improvements

This ensures that issues are not only resolved, but systematically prevented from recurring.

Policy Alignment and Operational Continuity

All error management processes are aligned with State-defined policies and procedures, ensuring:

- Consistent handling of errors across all partners
- Compliance with interoperability and data quality standards
- Minimal disruption to reporting and public health operations

Summary

VAULT's approach ensures that:

- Data exchange errors are identified and routed in real time
- Issues are efficiently investigated and resolved through structured workflows
- Providers and partners are supported throughout the resolution process
- Recurring issues are reduced through continuous improvement

This provides West Virginia with a reliable, transparent, and continuously improving error management framework that supports consistent and high-quality data exchange.4.2.1.4 Ensure the delivery of immunization services reflects current ACIP recommendations.

4.2.1.4 ENSURE THE DELIVERY OF IMMUNIZATION SERVICES REFLECT CURRENT ACIP RECOMMENDATIONS

VAULT meets CDC Functional Standard 4.2.1.4 by delivering a real-time, rules-driven Clinical Decision Support (CDS) framework aligned with ACIP recommendations and CDC CDSi resources. This framework evaluates patient-specific immunization histories, determines dose validity, and generates accurate, actionable forecasts at the point of care and across public health workflows.

VAULT's approach goes beyond simply displaying vaccine schedules. It operationalizes ACIP recommendations through a maintained CDS framework that is integrated into the core workflow of the IIS and connected public health operations.

What Sets VAULT Apart

VAULT differentiates its approach to ACIP-aligned CDS by:

- Delivering real-time, patient-specific forecasting rather than static schedule reference
- Centralizing rule execution to ensure consistent recommendations across all providers
- Maintaining CDSi alignment through governed, validated release processes
- Supporting complex and catch-up scenarios, including invalid dose recognition
- Integrating CDS outputs into operational workflows such as reminder/recall, reporting, and outreach
- Leveraging a modern, scalable architecture (ICE + Docker + AWS ECS) for performance and maintainability

This approach ensures that CDS is not limited to point-of-care reference but actively drives immunization program performance across the State.This means VAULT does not merely meet the functional standard at the point of care. It extends ACIP-aligned decision support across the broader immunization program, improving consistency, reducing missed opportunities, and supporting stronger vaccination coverage outcomes.

Operational Workflow

1. Provider submits or views patient immunization record

2. System evaluates patient age, history, dose intervals, and sequence

3. ICE engine executes CDSi-aligned rules in real time

4. System determines dose validity and forecast status (due, overdue, complete, invalid)

5. Forecast is immediately displayed within clinical workflows and made available for reporting and outreach

For West Virginia, this ensures consistent, statewide forecasting across a diverse provider network, reduces missed vaccination opportunities, and supports improved coverage outcomes across rural and underserved populations.

4.2.1.4.1 IMMUNIZATION FORECASTING ACROSS POPULATIONS

VAULT supports immunization forecasting across pediatric, adolescent, and adult populations by applying age-appropriate and vaccine-specific forecasting logic to each patient's immunization record. The system does not treat forecasting as a one-size-fits-all schedule; instead, it evaluates each patient in context and applies the rule set appropriate to that person's age group, vaccine history, and timing.

For pediatric patients, the system evaluates early childhood and school-age immunization schedules, including dose spacing, minimum intervals, minimum ages, series completion, and catch-up logic. For adolescent patients, the system evaluates routine adolescent schedules and timing-sensitive recommendations. For adults, the system applies adult forecasting rules, including age-based and risk-based recommendations where the required data elements are available and supported within the workflow.

Forecasting is generated by analyzing the validity and sequence of prior doses, identifying whether previous doses satisfy schedule requirements, and then determining what is currently due or when the next valid dose should occur. This allows the IIS to support:

- routine forecasting for standard immunization schedules
- catch-up forecasting when patients are behind schedule
- recognition of invalid or non-counting doses based on timing or sequence
- determination of next-dose timing when additional doses are required
- consistent forecasting across provider sites and user roles

Because the forecasting logic is centralized within the platform, providers across the jurisdiction receive consistent recommendations rather than site-specific interpretations. This improves standardization, reduces missed opportunities, and supports statewide quality and coverage goals.

4.2.1.4.1.1 CLINICAL DECISION SUPPORT FUNCTIONALITY

VAULT meets this requirement by embedding rules-driven forecasting into the core IIS transaction and workflow model to establish and maintain CDS functionality consistent with ACIP recommendations.

Structured Data Capture and Organization

The system captures and organizes all data elements required for accurate forecasting, including patient demographics, administered vaccines with standardized identification, administration dates, historical doses where available, and related clinical context needed to determine dose validity and schedule progression.

Immunization History Evaluation for Validity

Before any recommendation is generated, the system evaluates prior doses to determine whether they count toward a series. This includes assessment of timing, intervals, age at administration, sequence, and all applicable ACIP rule logic so that invalid or extra doses are distinguished and the forecast is based on clinically meaningful history.

Real-Time Rules Execution

When a user opens a patient record, enters a new vaccination, performs clinical review, or triggers any forecast-relevant workflow, the CDS engine immediately evaluates the patient's current state and produces updated recommendations. This real-time execution is powered by the CDC-endorsed Immunization Calculation Engine (ICE) running in a secure Docker container on ECS, with requests securely proxied through AWS API Gateway and supporting AWS Lambda functions for scalable, low-latency processing.

Workflow-Integrated Forecast Outputs

Recommendations are surfaced directly in the places where they are most operationally useful, including patient record views, vaccination workflows, assessment screens, and other clinical decision points. Providers can immediately see what is due, overdue, complete, invalid, or upcoming, eliminating the need for separate manual schedule review.

Governed Updates to Forecast Logic

VAULT maintains CDS logic through a controlled configuration and release process. When ACIP recommendations change, the ICE rules are reviewed, updated, validated, and deployed through formal release management so that the system remains current without requiring jurisdictions to manually rebuild logic.

Operational Use Beyond the Patient Screen

Forecast status is fully integrated into platform workflows, enabling use in reminder and recall campaigns, coverage gap identification, outreach planning, and reporting. This transforms ACIP alignment from a simple display feature into a true operational capability across the entire IIS.

Summary

This structured, real-time, governed, and workflow-integrated approach — leveraging the CDC-endorsed ICE engine in a modern Docker/ECS architecture — ensures that VAULT delivers and maintains CDS functionality that is fully consistent with ACIP recommendations while supporting both clinical and public health operations.

4.2.1.4.1.2 ALIGNMENT WITH CDC CDSI RESOURCES

VAULT meets this requirement by maintaining forecasting logic in accordance with published CDC decision support guidance and incorporating those updates through a formal governance and release process.

Monitoring of CDC CDSi Resources

VAULT continuously reviews relevant CDC-published CDSi artifacts and related ACIP schedule updates as part of its clinical and product governance process.

Analysis of Rule Impact

When CDC guidance changes, the impact is evaluated against forecast rules, dose validity logic, series completion logic, catch-up scheduling, and related recommendation outputs.

Controlled Rule Updates

Required changes are incorporated into the ICE rule set through formal change control, with full testing and validation performed before any release to ensure accuracy and prevent unintended effects on other scenarios.

Structured Release and Deployment

Updated logic is deployed centrally through structured release management rather than local manual configuration, ensuring the jurisdiction remains aligned with CDC guidance consistently across all users and sites.

Operational Integration of Updated Logic

Once deployed, revised forecasts are immediately reflected in point-of-care displays, assessments, reminder and recall workflows, and reporting where forecast status is used.

Summary

This repeatable, governed process — built around the CDC-endorsed ICE engine — ensures that alignment with CDC CDSi resources is not a one-time setup but an actively maintained capability, keeping CDS current, consistent, and statewide in its application. The ICE engine implements CDC CDSi logic directly, ensuring alignment with published CDSi artifacts without requiring custom rule translation or reinterpretation.

4.2.1.5 ENSURE APPROPRIATE USER ACCESS TO DATA

Overview

VAULT meets the requirements of this section by delivering a comprehensive, policy-driven framework for managing and enforcing appropriate access to IIS data, ensuring that access is secure, role-based, and aligned with both public health operations and consumer needs.

The PrepModEcosystem supports a dual access model, enabling:

- Authorized internal users and IIS partners to access data appropriate to their roles and responsibilities
- Individuals, parents, and guardians to securely access their own immunization records

This approach ensures that access to data is both controlled and purpose-driven across all user types.

For internal users, the system provides:

- Role-based and granular access control, enabling precise definition of data access and functionality
- Full user lifecycle management, including provisioning, role assignment, modification, and deactivation
- Policy-driven access enforcement, ensuring alignment with State-defined legal, regulatory, and operational requirements

- Training and onboarding requirements, ensuring users are prepared and compliant prior to accessing sensitive data
- Auditability and reporting, providing full visibility into access activity and supporting compliance oversight

The system supports diverse IIS partners, including providers, schools, health plans, and community-based organizations, ensuring that each user type has appropriate access to support clinical care, compliance, reporting, and population health activities.

For consumers, the system provides secure, user-friendly access to immunization records, enabling individuals to retrieve official documentation for school, employment, travel, and healthcare purposes, while maintaining strict privacy and authentication controls.

All access controls are configurable and managed directly by the State, enabling West Virginia to adapt access rules as policies, programs, and public health needs evolve.

Together, these capabilities ensure that access to IIS data is not only secure, but appropriately governed, user-centered, and aligned with real-world public health and consumer use cases.

What Sets VAULT Apart

Unlike traditional IIS platforms that treat user access as a static configuration or limit access models to internal users, VAULT delivers a dynamic, policy-driven access governance framework that spans both public health professionals and consumers.

In VAULT's approach:

- Access is managed as a continuous lifecycle, from onboarding and training to monitoring, modification, and deactivation, ensuring that permissions remain aligned with current roles and authorization status
- Policies are embedded directly into system functionality, enabling consistent, system-enforced access control rather than reliance on manual processes or external governance
- The State maintains full administrative control, including the ability to define roles, configure permissions, enforce policies, and manage users at scale through bulk and automated controls

- Access is tailored to real-world public health ecosystems, supporting diverse partners such as providers, schools, health plans, and community-based organizations within a single, unified platform
- Consumer access is fully integrated into the access model, enabling individuals to securely retrieve their immunization records while maintaining strict privacy, authentication, and policy alignment
- Training, monitoring, and auditability are built into the access framework, ensuring that users are not only authorized, but prepared, accountable, and compliant

This integrated approach transforms user access from a static technical feature into a continuously governed, user-centered, and operationally aligned system, where access is actively managed to support both security and public health outcomes.

As a result, West Virginia gains a solution that not only protects sensitive data, but ensures that access is appropriate, controlled, and optimized across all users—from public health professionals to the individuals they serve.

4.2.1.5.1 USER ACCESS GOVERNANCE AND CONTROL

VAULT meets the requirements of this subsection by providing a comprehensive, policy-driven framework for managing, controlling, and enforcing user access to IIS data, ensuring that access is appropriate, secure, and aligned with user roles and responsibilities across all system users.

The PrepModEcosystem integrates confidentiality policies, role-based access control, account lifecycle management, and structured training to ensure that access to sensitive data is not only authorized, but properly governed and continuously maintained over time.

User access is managed across the full lifecycle—from onboarding and role assignment to ongoing monitoring and deactivation—ensuring that permissions remain aligned with current roles, organizational relationships, and State-defined policies. Configurable controls enable the State to define and enforce access rules across functional, organizational, and geographic dimensions, while administrative tools provide direct control over user provisioning, updates, and deactivation without vendor dependency.

The system also supports appropriate access for a diverse range of IIS partners, including providers, schools, health plans, and community-based organizations, ensuring that each user type can access the data necessary to support clinical care and public health activities while maintaining strict privacy protections.

Access governance is reinforced through training, auditability, and automated controls, including policy-driven access activation, inactivity-based deactivation, and comprehensive reporting. These capabilities ensure that access remains appropriate, compliant, and transparent at all times.

Together, these capabilities create a controlled and adaptive access model, in which user access is continuously aligned with policies, monitored for compliance, and adjusted as roles and conditions evolve.

This approach provides West Virginia with a secure, scalable, and fully governed framework for managing appropriate access to IIS data across all users and use cases.

4.2.1.5.1.1 CONFIDENTIALITY AND PRIVACY PROTECTIONS

VAULT meets this requirement by implementing comprehensive confidentiality policies and procedures designed to protect the privacy of individuals while ensuring that access to data is appropriate, controlled, and aligned with user roles, in accordance with federal and State regulations, including HIPAA and applicable jurisdictional privacy requirements.

Policy Framework and Governance

VAULT maintains documented confidentiality and privacy policies that govern:

- Access to protected health information (PHI)
- Permitted use and disclosure of data
- User responsibilities and acceptable use
- Data handling, storage, and transmission practices

These policies are regularly reviewed and updated to reflect evolving regulatory requirements and best practices.

Technical and Administrative Safeguards

Confidentiality policies are enforced through a combination of technical and administrative controls, including:

- Role-based access control (RBAC), ensuring users can only access data necessary for their role

- Encryption of data at rest and in transit, protecting sensitive information from unauthorized access
- Comprehensive audit logging, capturing all access to and interaction with sensitive data
- Secure authentication mechanisms, including multi-factor authentication (MFA)

Monitoring, Enforcement, and Accountability

All access to sensitive data is:

- Tracked and auditable, enabling the State to monitor usage and detect unauthorized activity
- Subject to review and oversight, supporting compliance enforcement and risk mitigation
- Traceable to individual users, ensuring accountability for all system interactions

Workforce Training and Compliance

VAULT supports confidentiality through role-based training and user education, ensuring that all system users understand:

- Privacy requirements and responsibilities
- Appropriate access and use of sensitive data
- Compliance with applicable laws and policies

This reinforces a culture of privacy and appropriate data access across all user groups.

Summary

VAULT's confidentiality framework ensures that:

- Privacy policies are clearly defined and consistently enforced
- Access to sensitive data is appropriate, controlled, and role-based
- All data access is monitored, auditable, and accountable
- Users are trained to uphold privacy and data protection requirements

This approach provides West Virginia with a secure, compliant, and well-governed environment for protecting individual privacy while enabling appropriate access to immunization data.

4.2.1.5.1.2 ACCOUNT MANAGEMENT POLICIES AND CONTROL

VAULT meets this requirement by implementing comprehensive account management policies and controls aligned with industry security standards, including NIST guidance and best practices for identity and access management, ensuring that user access remains appropriate, controlled, and aligned with roles over time.

User Lifecycle Management

The system supports full user lifecycle management to ensure that access is appropriate and continuously aligned with user responsibilities:

- User provisioning, including account creation and role assignment based on defined responsibilities
- Role-based access control (RBAC), enforcing the principle of least privilege
- Location-based access controls, enabling restriction of access by region or service venue during statewide or emergency responses
- Periodic access reviews, allowing the State to validate and adjust permissions over time
- Account modification and deactivation, ensuring access is updated or revoked promptly when roles change

In addition, the system provides advanced lifecycle controls, including:

- Bulk deactivation and reactivation, enabling efficient management of large user groups
- Configurable inactivity-based deactivation, automatically disabling accounts after a user-defined period
- User status management tools, providing visibility into active, inactive, and deactivated accounts

Authentication and Access Controls

Account management policies are enforced through:

- Secure authentication, including support for multi-factor authentication (MFA)
- Configurable password and session policies, aligned with security best practices
- Administrative controls, enabling centralized management of accounts, roles, and permissions

Administrative Oversight and State Control

The system provides robust administrative tools that enable the State to directly manage user access without vendor dependency, including:

- User onboarding and provisioning
- Role assignment and modification
- Bulk account updates
- Account deactivation and reactivation

This ensures that West Virginia maintains full control over user access and can enforce jurisdiction-specific policies efficiently.

Auditability, Monitoring, and Reporting

All account management activities are:

- Tracked and auditable, including account creation, modification, role changes, and deactivation
- Traceable to individual users, ensuring accountability
- Available through reporting tools, enabling exportable reports on access, account status, inactivity, and administrative actions

These capabilities support compliance monitoring, audit readiness, and ongoing governance.

Summary

VAULT's account management approach ensures that:

- User access is securely managed across the entire lifecycle
- Permissions remain aligned with roles and least privilege principles
- The State retains full administrative control, including bulk and automated account management
- All account activities are auditable, reportable, and transparent

This provides West Virginia with a secure, flexible, and fully governed account management framework that maintains appropriate access to data at all times.

4.2.1.5.1.3 TECHNICAL CONTROLS FOR ROLES AND PERMISSIONS

VAULT meets this requirement by providing robust, configurable technical capabilities for defining, managing, and enforcing user roles and permissions, ensuring that access to data is precise, appropriate, and aligned with user responsibilities.

Role Definition and Configuration

The PrepModEcosystem enables authorized State administrators to:

- Create and configure custom user roles, allowing the State to define new user types as operational needs evolve
- Define and modify permissions associated with each role, without requiring vendor intervention
- Assign roles across diverse user types, including providers, school personnel, public health staff, administrators, and partner organizations
- Leverage role templates and reusable configurations, supporting consistent and efficient role setup

This flexibility allows West Virginia to adapt role structures and permissions over time as workflows, programs, and policies change.

Granular Permission Management

The system supports fine-grained permission assignment, enabling control at multiple levels, including:

- Functional access, such as data entry, reporting, and administration
- Data-level access, ensuring users can only view or interact with authorized records
- Organizational and geographic scope, restricting access by site, region, or jurisdiction

These controls allow users to perform required functions while maintaining strict control over sensitive data.

Enforcement and Access Control Mechanisms

Permissions are system-enforced at all levels, ensuring that:

- Users are restricted to authorized actions and data
- Access controls are consistently applied across all system components
- Unauthorized access attempts are prevented and logged

This ensures that role and permission configurations are actively enforced—not just defined.

Administrative Management and Usability

The system provides intuitive administrative tools that allow authorized State personnel to:

- Create, modify, and assign roles
- Update permissions in real time
- Apply changes across individual users or groups efficiently

This enables rapid adaptation to changing operational needs without reliance on vendor support.

Summary

VAULT's approach to role and permission management ensures that:

- The State can independently define and manage user roles
- Permissions are granular, precise, and enforceable
- Access is controlled across functional, organizational, and geographic dimensions
- The system remains flexible and adaptable over time

This provides West Virginia with a secure, scalable, and State-controlled framework that ensures appropriate access to data across all users and use cases.

4.2.1.5.1.4 POLICY-BASED ACCESS ENFORCEMENT

VAULT meets this requirement by ensuring that all user access is governed, configured, and enforced in accordance with jurisdiction-defined policies and procedures, using a combination of role-based access control, system-level enforcement, and administrative oversight.

Policy-Driven Access Control

User access is aligned with State policies through:

- Role-based access control (RBAC), where permissions are assigned based on defined user roles and responsibilities

- Configurable access rules, allowing the State to define and enforce policies related to data access, user roles, and system functionality
- Granular permission settings, ensuring that users can only access the data and functions permitted under applicable policies

This ensures that access is consistently aligned with legal, regulatory, and operational requirements.

System-Enforced Policy Compliance

The system enforces access policies at all levels by:

- Restricting users to authorized data based on role, organization, and geographic scope
- Preventing unauthorized actions through system-level controls
- Applying access rules consistently across all system components and workflows

This reduces the risk of unauthorized access and ensures that policies are not only defined, but actively enforced.

Administrative Control and Policy Enforcement

Authorized State administrators can:

- Configure and update access rules to reflect evolving policies and procedures
- Create and modify user roles and permissions without vendor intervention
- Apply policy changes in real time across the system

In addition, the system supports policy-driven access activation, allowing the State to require completion of role-based training or other onboarding requirements prior to granting system access.

This ensures that users are not only authorized, but also properly trained before accessing sensitive data or system functionality, reinforcing compliance with privacy, security, and operational policies.

Auditability and Oversight

All user access and policy enforcement activities are:

- Tracked and auditable, including access attempts and data interactions

- Available for reporting and review, supporting compliance monitoring
- Linked to individual users, ensuring accountability

Summary

VAULT's approach ensures that:

- User access is fully aligned with State-defined policies and procedures
- Access controls are enforced consistently across the system
- The State retains control over policy configuration and updates
- Access can be conditioned on completion of required training
- All access activity is auditable and compliant

This provides West Virginia with a policy-driven, enforceable, and adaptable access control framework.

4.2.1.5.1.5 ACCESS FOR PARTNERS AND PROVIDERS

VAULT meets this requirement by providing role-based, policy-driven access controls that ensure IIS partners and providers have appropriate access to data for public and population health purposes, while maintaining strict privacy protections.

Role-Based Access by Partner Type

The system supports differentiated access for a wide range of IIS partners, including:

- Childcare facilities and schools, with access to student immunization records for school-entry compliance and reporting
- Colleges and universities, with access to student vaccination status and compliance tracking
- Health plans, with access to population-level and member-specific data for quality reporting and care coordination
- Clinics and providers, with access to patient-level records for clinical decision-making and vaccine administration

Access for each partner type is defined through configurable roles and permissions, ensuring users can only view and manage data relevant to their responsibilities.

Granular and Scoped Data Access

The system enforces appropriate access through:

- Role-based access control (RBAC) aligned with partner responsibilities
- Organizational and site-level restrictions, limiting access to patients associated with a specific provider, school, or organization
- Geographic and jurisdictional controls, ensuring access aligns with State-defined boundaries
- Minimum necessary access principles, ensuring users only see the data required for their role

Policy Enforcement and Privacy Protection

All partner access is governed by State-defined policies and enforced through system controls that:

- Restrict unauthorized data access
- Ensure compliance with privacy and regulatory requirements
- Apply access rules consistently across all users and workflows

Support for Public and Population Health Use Cases

This structured access model enables partners to effectively support key public health activities, including:

- School-entry compliance tracking and reporting
- Population health analysis and coverage monitoring
- Care coordination across providers and organizations
- Identification of gaps in vaccination coverage

Proven Experience Supporting Diverse Partner Types

VAULT has extensive experience supporting a diverse range of IIS partners, including schools, childcare facilities, health systems, pharmacies, and public health organizations across multiple jurisdictions.

The flexibility of the PrepModEcosystem enables these varied user groups to operate within a single, unified platform while maintaining appropriate, role-based access to data.

This experience demonstrates that VAULT's approach is not only configurable, but **proven in real-world environments**, reducing implementation risk and supporting effective adoption across all partner types.

Summary

VAULT's approach ensures that:

- IIS partners and providers have appropriate, role-based access to data
- Access is tailored to partner type, organization, and use case
- Privacy and security requirements are consistently enforced
- The system supports both clinical and population health objectives
- The approach is proven across diverse, real-world partner environments

This provides West Virginia with a secure, flexible, and purpose-driven access model for all IIS stakeholders.

4.2.1.5.1.6 TRAINING ON DATA ACCESS

VAULT meets this requirement by providing structured, role-based training programs that ensure users understand how to appropriately access, interpret, and use patient demographic and vaccination data in accordance with State policies and privacy requirements.

Role-Based Training and User Education

Training is tailored to specific user roles and responsibilities, ensuring that each user group receives relevant guidance on:

- Accessing patient demographic and vaccination data
- Appropriate use of system functionality based on role
- Privacy, confidentiality, and compliance requirements
- Data handling best practices

This ensures that users are equipped to use the system effectively while maintaining compliance with applicable policies.

Training as a Prerequisite for Access

The system supports policy-driven access activation, enabling the State to require completion of training prior to granting access to sensitive data or system functionality.

This ensures that users are not only authorized, but also prepared and compliant before interacting with the system.

Ongoing Training and Reinforcement

VAULT provides ongoing training and support to ensure that users remain aligned with:

- System updates and enhancements
- Changes to policies and procedures
- Identified data quality or access-related issues

This continuous education model helps reinforce proper system use over time.

Summary

VAULT's approach ensures that:

- Users are trained based on their roles and responsibilities
- Access to data is supported by proper understanding and compliance
- Training can be required prior to access activation
- Users remain informed and aligned with policies over time

This provides West Virginia with a well-governed and sustainable approach to ensuring appropriate access and use of IIS data.

4.2.1.5.1.7 ACCOUNT DEACTIVATION AND LIFECYCLE MANAGEMENT

VAULT meets this requirement by providing comprehensive, policy-driven mechanisms for the identification, inactivation, and management of user and site accounts, ensuring that access remains current, appropriate, and aligned with authorization status.

Automated and Administrative Inactivation Controls

The system supports both automated and administrator-driven processes to manage account status, including:

- Manual deactivation and reactivation of users and sites, allowing administrators to promptly update access based on changes in roles or authorization
- Bulk deactivation and reactivation capabilities, enabling efficient management of large groups of users or sites
- Configurable inactivity-based deactivation, allowing the State to automatically disable accounts after a user-defined period of inactivity

These capabilities ensure that inactive or unauthorized accounts are promptly identified and removed from active access.

Policy Alignment and Lifecycle Management

Account inactivation is integrated into the broader user lifecycle management framework, ensuring that:

- Access is continuously aligned with current roles and responsibilities
- Deactivation processes reflect State-defined policies and procedures
- Accounts are reactivated only when appropriate authorization is restored

Monitoring, Reporting, and Oversight

The system provides reporting and visibility into account status and activity, enabling the State to:

- Generate reports on active, inactive, and deactivated users and sites
- Monitor inactivity trends and identify accounts requiring action
- Support audit, compliance, and security oversight

Summary

VAULT's approach ensures that:

- User and site access is continuously evaluated and updated
- Inactive or unauthorized accounts are promptly deactivated
- Bulk and automated processes support efficient account management
- The State has full visibility and control over account status

This provides West Virginia with a secure, efficient, and policy-driven framework for managing user and site inactivation across the IIS.

4.2.1.5.2 PUBLIC ACCESS TO IMMUNIZATION RECORDS

VAULT meets the requirements of this subsection by providing secure, policy-aligned, and user-friendly access for individuals to retrieve their immunization records, ensuring that consumer access is both accessible and appropriately controlled.

The PrepModEcosystem enables individuals, parents, and guardians to access immunization records through secure, web-based interfaces, designed to support common real-world needs such as school enrollment, employment verification, travel, and healthcare coordination.

All consumer access is governed by State-defined policies and procedures, ensuring that:

- Access is restricted to authorized individuals or their legal representatives
- Identity verification and authentication controls are enforced
- Data is accessed in accordance with privacy and security requirements

The system is designed to provide a simple and intuitive user experience, allowing individuals to easily locate, view, and retrieve official immunization records without requiring technical expertise.

All access and interactions are logged and auditable, supporting transparency, compliance, and oversight.

This capability enhances patient engagement, reduces administrative burden on public health staff, and improves access to critical health information across the population.

4.2.1.5.2.1 CONSUMER ACCESS

VAULT meets this requirement by providing secure, user-friendly access for individuals to view and retrieve their immunization records, in alignment with State policies and privacy requirements.

Secure Consumer Access

The PrepModEcosystem enables consumers to access their immunization records through secure, web-based interfaces, allowing individuals to:

- View their immunization history
- Retrieve official immunization records
- Access documentation for use in school, employment, travel, or healthcare settings

Access is protected through secure authentication and identity verification processes, ensuring that only authorized individuals can access their personal health information.

User-Friendly Experience

The system is designed to provide a simple and intuitive user experience, enabling individuals to:

- Easily locate and access their records
- Navigate information without requiring technical expertise
- Quickly retrieve documentation when needed

This improves accessibility and supports broader public engagement with immunization data.

Privacy and Policy Alignment

All consumer access is governed by State-defined policies and procedures, ensuring that:

- Access complies with applicable privacy and security requirements
- Data is only accessible to the appropriate individual or authorized representative
- Consumer access aligns with jurisdictional guidelines for data sharing

Summary

VAULT's approach ensures that:

- Individuals have secure, direct access to their immunization records
- Access is user-friendly and aligned with real-world needs
- Privacy and security protections are consistently enforced
- Consumer access supports public health and individual decision-making

This provides West Virginia with a secure, accessible, and policy-aligned solution for enabling consumer access to immunization data.

4.2.1.6 SUPPORT THE GENERATION AND USE OF IIS DATA THROUGH VARIOUS CHANNELS AND FORMATS

Overview

VAULT meets the requirements of this section by delivering a comprehensive, multi-channel framework for generating, accessing, analyzing, and using IIS data, enabling the State to transform immunization data into actionable public health intelligence.

The PrepModEcosystem supports the full lifecycle of data use, including:

- Standard and ad hoc reporting, aligned with CDC and jurisdictional requirements
- Direct data access and querying, enabling advanced analysis and data extraction
- Interactive dashboards and visualization tools, supporting real-time insight and communication
- Coverage reporting and compliance monitoring, enabling identification of gaps and vulnerable populations
- Adverse event investigation and reporting, supporting vaccine safety and regulatory compliance
- Reminder and recall capabilities, enabling targeted outreach to improve vaccination coverage

These capabilities are accessible through user-driven, configurable tools, allowing authorized users to generate reports, conduct analysis, and initiate outreach activities without reliance on IIS technical staff.

All data access and use are governed by role-based permissions and State-defined policies, ensuring that flexibility in data use is balanced with privacy, security, and compliance requirements.

Together, these capabilities enable West Virginia to leverage IIS data across multiple channels and use cases, supporting operational management, program evaluation, population health analysis, and public health response.

What Sets VAULT Apart

Unlike traditional IIS platforms that focus primarily on static reporting, VAULT delivers a fully integrated public health intelligence and action platform, where data is not only collected and reported, but actively used to drive decision-making and improve outcomes.

In VAULT's approach:

- Data is accessible across multiple channels, including reports, dashboards, queries, and outreach tools, enabling users to interact with data in ways that support their specific roles
- Reporting, analytics, and outreach are fully integrated, allowing users to move seamlessly from identifying gaps to taking action through reminder and recall campaigns
- The State maintains full control over data access and configuration, enabling flexible, user-driven reporting and analysis without vendor dependency
- Data is transformed into actionable insights, supporting real-time decision-making, resource allocation, and targeted public health interventions
- The platform supports end-to-end public health workflows, including coverage monitoring, compliance tracking, vaccine safety investigation, and population outreach

This integrated model transforms IIS data from a passive repository into an active, operational asset, enabling West Virginia to not only monitor immunization programs, but to continuously improve them.

As a result, the State gains a solution that is scalable, flexible, and outcome-driven, capable of supporting evolving public health needs and maximizing the impact of immunization programs.

4.2.1.6.1 SUPPORT FOR FEDERAL AND JURISDICTIONAL REPORTING

VAULT meets the requirements of this subsection by providing a comprehensive, configurable reporting framework that supports both federal and jurisdictional immunization program needs.

The PrepModEcosystem enables the generation of standardized reports aligned with CDC requirements, as well as flexible, ad hoc reporting to support evolving State priorities and operational needs. Reporting capabilities are designed to provide timely, accurate, and actionable insights, enabling the State to monitor program performance, assess coverage, and respond to emerging public health challenges.

All reporting functions are user-driven and configurable, allowing authorized users to generate and customize reports without technical assistance, ensuring that reporting remains adaptable to changing requirements.

This approach ensures that West Virginia has a reliable, scalable, and responsive reporting capability that supports both compliance and data-driven decision-making.

4.2.1.6.1 REPORTING FOR FEDERAL AND JURISDICTIONAL PROGRAMS

VAULT meets this requirement by providing a comprehensive, configurable reporting framework that supports both standardized and ad hoc reporting needs for federal and jurisdictional immunization programs.

Standard Reporting Capabilities

The system includes a robust library of predefined reports aligned with CDC requirements and jurisdictional priorities, including:

- Immunization coverage rates
- Vaccine utilization and inventory trends
- Provider participation and performance metrics
- Compliance and program reporting indicators
- De-identified data reports for research, analysis, and secure sharing with authorized external partners

These reports are designed to support federal reporting requirements while enabling consistent monitoring of program performance.

Ad Hoc and Configurable Reporting

Authorized users can generate ad hoc reports without technical assistance, using flexible configuration options that allow reports to be tailored by:

- Population characteristics (e.g., age, risk group)
- Geographic region or jurisdiction
- Provider, organization, or site
- Vaccine type, manufacturer, or administration details

This enables the State to quickly respond to emerging needs, policy changes, or public health events.

Operational and Real-Time Use

Reporting is designed to support real-time decision-making and program management, enabling the State to:

- Monitor vaccination coverage and identify gaps
- Evaluate provider performance and participation
- Support targeted outreach and intervention strategies
- Respond to public health emergencies and changing demand

Self-Service and State Control

All reporting capabilities are user-driven and configurable, allowing authorized State users to create, modify, and run reports independently, without reliance on vendor support.

4.2.1.6.1.1 STANDARD AND AD HOC REPORTING

VAULT complies with this requirement.

The IIS provides both standard and ad hoc reporting capabilities to meet federal and jurisdictional reporting requirements. The PrepModEcosystem includes a comprehensive library of predefined reports aligned with CDC reporting standards and jurisdictional program needs, enabling consistent and compliant reporting across required use cases.

In addition to standard reports, the system supports flexible, user-driven ad hoc reporting. Authorized users can generate customized reports by configuring parameters such as population demographics, geographic regions, providers, and vaccine-specific data elements. This allows the State to respond quickly to emerging public health needs, policy changes, and reporting requests.

Reporting capabilities are designed to deliver timely, accurate, and actionable data, supporting both routine federal reporting and jurisdiction-specific analysis. All reports can be generated without reliance on vendor technical staff, ensuring that the State maintains full control over reporting and data access.

These capabilities ensure that West Virginia can efficiently meet all required reporting obligations while leveraging IIS data to support ongoing program management and decision-making.

4.2.1.6.2 AD HOC QUERIES AND DATA ACCESS

VAULT meets the requirements of this subsection by providing secure, flexible, and user-driven access to IIS data, enabling authorized users to query, analyze, and visualize data to support public health decision-making.

The PrepModEcosystem enables direct access to IIS data for advanced users, allowing for ad hoc querying and data extraction in accordance with role-based permissions and State-defined policies. These capabilities support in-depth analysis, program evaluation, and data-driven planning.

In addition, the system provides interactive dashboards and visualization tools that transform IIS data into clear, actionable insights. Users can monitor trends, assess performance, and identify gaps through configurable visualizations tailored to their specific needs.

All data access and visualization capabilities are fully integrated and governed, ensuring that flexibility in analysis is balanced with strict privacy, security, and policy compliance.

Together, these capabilities provide West Virginia with a powerful, scalable, and user-driven framework for accessing, analyzing, and interpreting IIS data, supporting both operational and strategic public health initiatives.

4.2.1.6.2.1 DIRECT DATA ACCESS

VAULT meets this requirement by providing secure, role-based direct access to IIS data for authorized internal users, enabling advanced querying, analysis, and data extraction in accordance with State policies and procedures.

Secure and Governed Data Access

Access to IIS data is controlled through role-based permissions and policy-driven access controls, ensuring that:

- Only authorized users can access data for analysis and reporting
- Access is aligned with user roles, responsibilities, and jurisdictional policies
- Data use complies with privacy and security requirements

Flexible Query and Data Access Capabilities

The system enables authorized users to:

- Perform ad hoc queries on patient demographic and vaccination data
- Access data for custom analysis and reporting
- Extract datasets for approved public health use cases

These capabilities support advanced users in conducting deeper analysis without requiring vendor support.

Multiple Access Channels

Data access is supported through multiple channels, including:

- User interface–based query tools, enabling non-technical users to retrieve data
- Export capabilities, allowing users to securely extract datasets for further analysis
- Controlled access pathways, ensuring that all data access is governed and auditable

Operational and Analytical Use

Direct access to IIS data enables the State to:

- Conduct in-depth analysis of immunization coverage and trends
- Support program evaluation and performance monitoring
- Respond to emerging public health needs with timely data insights

4.2.1.6.2.2 DATA VISUALIZATION AND ANALYSIS

VAULT meets this requirement by providing interactive dashboards and visualization tools that enable users to analyze, interpret, and present IIS data in meaningful and actionable formats.

Interactive Dashboards and Visual Analytics

The system includes configurable dashboards that allow users to:

- Visualize immunization coverage, trends, and gaps across populations
- Monitor provider performance and participation
- Track vaccine utilization and program metrics
- Analyze data across geographic regions, demographics, and time periods

These dashboards present complex data through intuitive visual formats, including charts, graphs, and summary indicators.

Configurable and User-Driven Analysis

Authorized users can customize dashboards and visualizations to meet specific needs, including:

- Selecting data elements and metrics
- Filtering by population, provider, geography, or vaccine type
- Adjusting timeframes and comparison views

This enables the State to tailor data views for operational, programmatic, and strategic analysis without vendor support.

Support for Decision-Making and Communication

Visualization tools are designed to support:

- Real-time decision-making, including identification of coverage gaps and emerging trends
- Program management and performance monitoring
- Communication of insights to stakeholders, including leadership, partners, and the public

Integration with Reporting and Data Access

Visualization capabilities are fully integrated with the system's reporting and query tools, allowing users to:

- Transition from dashboards to detailed reports or data extracts
- Validate and explore underlying data
- Use visual insights to guide further analysis

Summary

VAULT's approach ensures that:

- IIS data is presented in clear, actionable formats
- Dashboards support real-time analysis and decision-making
- Visualizations are configurable and user-driven
- Data insights can be effectively communicated across stakeholders

This provides West Virginia with a powerful and flexible visualization capability that transforms IIS data into actionable public health intelligence.

4.2.1.6.3 INVESTIGATION AND REPORTING OF VACCINE ADVERSE EVENTS

VAULT meets the requirements of this subsection by providing structured tools, workflows, and resources to support the identification, investigation, and reporting of vaccine adverse events, ensuring alignment with clinical and public health safety practices.

The PrepModEcosystem enables users to capture and document adverse events, access complete patient and vaccination histories, and utilize analytical tools to support case review and investigation. Integrated query and reporting capabilities allow users to identify patterns, assess potential safety signals, and support coordinated public health response efforts.

In addition, the system provides embedded guidance and access to external reporting resources, including support for federal reporting requirements such as VAERS. Users are equipped with the information and tools needed to accurately document and report adverse events in accordance with established policies and procedures.

Together, these capabilities provide West Virginia with a comprehensive, data-driven framework for monitoring vaccine safety, supporting investigation workflows, and ensuring compliant reporting of adverse events.

4.2.1.6.3.1 IDENTIFICATION AND INVESTIGATION OF ADVERSE EVENTS

VAULT meets this requirement by providing structured tools and workflows to identify, document, and investigate vaccine adverse events, ensuring that users have access to the data and context needed to support clinical review and public health response.

Adverse Event Capture and Documentation

The system enables authorized users to:

- Document adverse events associated with vaccine administration
- Capture relevant details, including patient demographics, vaccination history, timing, and reported symptoms
- Associate adverse events with specific vaccines, providers, and administration events

This ensures that adverse events are consistently and accurately recorded within the IIS.

Integrated Data Access for Investigation

Users can access comprehensive patient and vaccination data within the system to support investigation, including:

- Complete immunization history
- Demographic and clinical context
- Provider and administration details

This allows investigators to evaluate adverse events using a longitudinal view of the patient record.

Analytical and Review Capabilities

The system supports investigation through:

- Search and query tools, enabling identification of similar cases or patterns
- Reporting and analysis capabilities, supporting trend identification and case review
- Visualization tools, helping users assess patterns and potential signals

Workflow Support for Public Health Response

These capabilities support:

- Clinical review and follow-up
- Identification of potential safety signals
- Coordination of investigation activities across public health teams

Summary

VAULT's approach ensures that:

- Adverse events are consistently captured and documented
- Investigators have access to complete and relevant data
- Analysis tools support identification of patterns and trends
- The system supports structured public health investigation workflows

This provides West Virginia with a comprehensive and data-driven approach to adverse event identification and investigation.

4.2.1.6.3.2 ADVERSE EVENT DOCUMENTATION

VAULT meets this requirement by providing integrated resources, guidance, and system capabilities to support proper documentation and reporting of vaccine adverse events in accordance with federal and State requirements.

Guidance and Reference Materials

The system provides users with access to:

- Embedded guidance and reference materials, supporting proper adverse event documentation
- Links and references to federal reporting systems, including the Vaccine Adverse Event Reporting System (VAERS)
- Role-based instructions to ensure users understand reporting requirements and processes

Support for Reporting Workflows

The platform supports adverse event reporting by enabling users to:

- Compile required information from existing patient and vaccination records
- Access relevant data needed for reporting without duplicative entry
- Generate supporting documentation for submission to external reporting systems

Training and User Support

VAULT supports users through:

- Role-based training, ensuring understanding of adverse event reporting requirements
- Ongoing support and guidance for proper documentation and reporting practices

Policy Alignment and Compliance

All adverse event reporting support is aligned with:

- Federal reporting requirements, including VAERS
- State policies and procedures, ensuring consistent and compliant reporting

Summary

VAULT's approach ensures that:

- Users have access to guidance and resources for proper reporting
- Reporting workflows are supported and streamlined
- Required data is readily available within the system
- Reporting practices are aligned with federal and State requirements

This provides West Virginia with a supported, compliant, and efficient framework for adverse event reporting.

4.2.1.6.4 COVERAGE REPORTING AND SELF-SERVICE ACCESS

VAULT meets the requirements of this subsection by providing comprehensive, user-driven coverage reporting and compliance monitoring capabilities that support identification of vulnerable populations, tracking of vaccination status, and enforcement of immunization requirements.

The PrepModEcosystem enables users to independently generate coverage reports, analyze trends, and assess performance across populations, providers, and geographic regions. Integrated tools support patient status tracking, compliance monitoring, and data-driven decision-making, while role-based training ensures that users can effectively interpret and act on insights.

Together, these capabilities provide West Virginia with a powerful and accessible framework for monitoring immunization coverage, identifying gaps, and supporting public health interventions and compliance efforts.

4.2.1.6.4.1 COVERAGE ANALYSIS AND IDENTIFICATION OF VULNERABLE POPULATIONS

VAULT meets this requirement by providing robust, user-driven access to coverage data and analytics, enabling the State to assess vaccination coverage and identify under-vaccinated and vulnerable populations.

The system enables users to:

- Generate coverage reports across demographic groups, geographic regions, and provider sites
- Analyze vaccination rates by age, risk group, and population segment
- Identify gaps in coverage and populations at increased risk

These capabilities support targeted outreach, intervention planning, and public health response efforts, ensuring that resources are directed where they are most needed.

4.2.1.6.4.2 PATIENT STATUS MANAGEMENT ACROSS LEVELS

VAULT meets this requirement by enabling tracking and management of patient vaccination status across provider, site, and jurisdictional levels, supporting both operational and program-level oversight.

The system allows users to:

- Assess patient vaccination status at the individual, provider, and jurisdiction levels
- Monitor completion of vaccine series and identify overdue or missing doses
- Aggregate data to support provider performance monitoring and jurisdiction-wide analysis

This provides a comprehensive view of immunization status, supporting both clinical workflows and public health program management.

4.2.1.6.4.3 TRAINING FOR REPORTING AND INTERPRETATION

VAULT meets this requirement by providing role-based training and support to ensure that users can effectively access, generate, and interpret IIS reports.

Training includes:

- Guidance on generating standard and ad hoc reports
- Instruction on interpreting coverage data, trends, and performance metrics
- Best practices for using data to support decision-making and program improvement

This ensures that users are not only able to generate reports, but can translate data into actionable insights.

4.2.1.6.4.4 SUPPORT FOR COMPLIANCE IN EDUCATIONAL SETTINGS

VAULT meets this requirement by supporting compliance monitoring for immunization requirements across childcare, school, and college settings.

The system enables:

- Tracking of immunization compliance for enrolled populations
- Identification of individuals who are non-compliant or overdue for required vaccinations
- Generation of reports to support school-entry compliance and regulatory reporting

These capabilities enable the State and partner organizations to monitor compliance, identify gaps, and support enforcement of immunization requirements.

4.2.1.6.5 REMINDER AND RECALL ACTIVITIES

VAULT meets this requirement by providing fully configurable, user-driven reminder and recall capabilities that enable authorized users to conduct outreach activities independently, without reliance on IIS technical staff.

Identification of Due and Overdue Populations

The system enables users to identify individuals who are:

- Due for upcoming vaccinations
- Overdue for required doses
- Incomplete in vaccine series

These lists are generated using clinical decision support (CDS) and current immunization schedules, ensuring accuracy and alignment with public health guidelines.

User-Driven Campaign Management

Authorized users can independently:

- Generate targeted reminder and recall lists
- Define criteria based on age, vaccine type, geography, provider, or population group
- Initiate outreach campaigns without vendor or IIS staff support

This supports rapid response to coverage gaps and emerging public health needs.

Multi-Channel Outreach Capabilities

The system supports multiple communication methods, including:

- Email notifications
- SMS/text messaging (where enabled)
- Printable letters or outreach lists

This flexibility allows the State and partners to tailor outreach strategies to specific populations and communication preferences.

Integration with Reporting and Clinical Decision Support

Reminder and recall functionality is integrated with:

- Clinical decision support (CDS), ensuring outreach is based on accurate vaccine forecasting
- Reporting and analytics tools, enabling users to monitor campaign effectiveness and coverage improvements

Support for Public Health Outcomes

These capabilities enable the State to:

- Improve vaccination coverage rates
- Reduce missed opportunities for vaccination
- Target underserved or high-risk populations

- Support large-scale outreach campaigns during public health initiatives

Summary

VAULT's approach ensures that:

- Reminder and recall activities can be conducted independently by authorized users
- Outreach is targeted, configurable, and data-driven
- Multiple communication channels are supported
- Campaigns are based on accurate and up-to-date clinical guidance

This provides West Virginia with a powerful, scalable, and user-driven framework for improving vaccination coverage through effective outreach.

4.2.1.6.5.1 INDEPENDENT REMINDER/RECALL CAPABILITY

VAULT complies with this requirement.

The IIS enables authorized users to conduct reminder and recall activities independently, without assistance from IIS technical staff. All functionality required to identify target populations, configure outreach criteria, generate communication lists, and initiate campaigns is available through user-accessible tools within the system.

Users can create and execute reminder and recall activities using configurable parameters such as age, vaccine status, geography, provider, and other relevant criteria. These activities are supported by integrated clinical decision support, ensuring that outreach is based on accurate and current immunization schedules.

The system is designed to be intuitive and user-driven, allowing public health staff and authorized partners to manage outreach efforts directly. This ensures that reminder and recall activities can be performed efficiently, scaled as needed, and adapted quickly to changing public health priorities without reliance on vendor or IIS staff intervention.

4.2.1.7 SUPPORT FEDERAL AND JURISDICTIONAL VACCINE PROGRAM REQUIREMENTS

VAULT supports federal and jurisdictional vaccine program requirements through a comprehensive, integrated framework that combines program management, inventory control, supply chain operations, and federal system integration within a single platform. The PrepModEcosystem enables the State to manage all aspects of vaccine programs—from eligibility and compliance to distribution and reporting—with real-time visibility, configurability, and auditability.

The system provides configurable tools to define and enforce program procedures aligned with federal and State policies, including strong support for programs such as Vaccines for Children (VFC). Dose-level eligibility tracking ensures that each administered vaccine is accurately associated with the appropriate funding source. Integrated quality assurance capabilities enable rapid identification of non-viable doses and recalled vaccine lots.

VAULT also delivers robust, real-time vaccine inventory and supply chain management across provider and jurisdictional levels, including automated decrementing, reconciliation, tracking of returns/transfers/wastage, and integrated ordering workflows. Secure, standards-based integration with federal systems such as the CDC's Vaccine Tracking System (VTrckS) via ExIS ensures automated, compliant data exchange and the ability to adapt to evolving federal specifications without disruption.

What Sets VAULT Apart

VAULT delivers federal and jurisdictional vaccine program management as a unified, operational capability—enabling the State to maintain compliance, visibility, and control across all aspects of vaccine program administration.

Key differentiators include:

- **Unified Program and Operational Platform** – Integrates program management, inventory, ordering, administration, and reporting within a single system, eliminating manual reconciliation between disparate tools.

- **Embedded Compliance and Eligibility Tracking** – Dose-level tracking and configurable rules ensure compliance with federal and State programs (e.g., VFC) is maintained as part of routine operations rather than an added burden.
- **Real-Time Inventory and Supply Chain Visibility** – Centralized tracking of stock levels, lots, expiration dates, and utilization supports equitable allocation, proactive management, and audit readiness.
- **Integrated Federal System Alignment (VTrckS / ExIS)** – Automated, standards-based integration with federal systems ensures timely data exchange and quick adaptation to changing requirements.
- **Configurable and Future-Ready Architecture** – Flexible design enables the State to adapt to evolving policies and priorities through configuration instead of system redesign.

4.2.1.7.1 PROGRAM MANAGEMENT AND QUALITY ASSURANCE

VAULT meets the requirements of this subsection by providing configurable tools and workflows to support vaccine program management, compliance, and quality assurance in alignment with federal and jurisdictional requirements.

The PrepModEcosystem enables the State to define and enforce program procedures, track eligibility at the dose level, and monitor vaccine administration for compliance with funding and safety requirements. Integrated reporting capabilities support the identification of non-viable vaccine administration and recalled lots, enabling rapid response and corrective action.

These capabilities provide West Virginia with a comprehensive framework for ensuring program integrity, supporting compliance, and maintaining high standards for vaccine administration and safety across all provider sites.

4.2.1.7.1.1 PROGRAM PROCEDURES ALIGNED WITH POLICY

VAULT meets this requirement by enabling the State to define, configure, and enforce vaccine program procedures in alignment with federal and jurisdictional policies.

The system provides configurable tools that allow administrators to:

- Define program rules, eligibility criteria, and operational workflows
- Align system behavior with federal programs (e.g., VFC) and State-specific requirements
- Update policies dynamically as guidance evolves, without requiring system redesign

These capabilities ensure that program procedures are consistently applied across all users and provider sites, supporting compliance and operational consistency.

4.2.1.7.1.2 DOSE-LEVEL ELIGIBILITY TRACKING

VAULT meets this requirement by supporting eligibility tracking at the dose level for publicly purchased vaccines, ensuring accurate program participation and compliance.

The system enables:

- Capture and tracking of eligibility status at the time of vaccine administration
- Association of each administered dose with the appropriate funding source
- Validation of eligibility against program rules and criteria

This ensures that the State can accurately determine whether administered vaccines are associated with publicly funded programs and supports reporting, auditing, and compliance with federal requirements.

4.2.1.7.1.3 IDENTIFICATION OF NON-VIABLE VACCINE ADMINISTRATION

VAULT meets this requirement by enabling the State to identify and report patients who may have received non-viable vaccines, supporting rapid response and patient safety.

The system supports:

- Identification of doses administered outside of viability parameters (e.g., expired or improperly handled vaccines)
- Generation of reports listing affected patients
- Access to patient and administration details to support follow-up and remediation

These capabilities enable timely intervention and ensure that affected individuals can be appropriately notified and managed.

4.2.1.7.1.4 IDENTIFICATION OF RECALLED VACCINE LOTS

VAULT meets this requirement by providing tools to identify and report provider sites and patients associated with recalled vaccine lots, enabling rapid response to safety events.

The system enables:

- Tracking of vaccine lot numbers at the dose and administration level
- Identification of providers and patients associated with recalled lots
- Generation of reports to support outreach, notification, and corrective action

This ensures that the State can respond quickly to manufacturer recalls and maintain the integrity of immunization programs.

4.2.1.7.2 VACCINE INVENTORY MANAGEMENT AND RECONCILIATION

VAULT meets the requirements of this subsection by providing a fully integrated vaccine inventory, ordering, and supply chain management framework that supports real-time tracking, reconciliation, reporting, and federal system integration.

The PrepModEcosystem enables the State to manage vaccine inventory across provider and jurisdictional levels with centralized, real-time visibility into stock levels, lot numbers, expiration dates, and distribution. Administered doses are automatically decremented from active inventory, reconciliation processes identify and resolve discrepancies, and tracking of returns, transfers, and wastage ensures full accountability and audit readiness for programs including VFC. Integrated ordering workflows allow providers to request vaccines while the State maintains oversight of allocation and distribution.

4.2.1.7.2.1 INVENTORY MANAGEMENT, TRACKING, AND RECONCILIATION

AULT meets this requirement by providing comprehensive, real-time inventory management and reconciliation capabilities at both the jurisdictional and provider site levels, ensuring accurate tracking, accountability, and compliance with federal and State vaccine program requirements.

Real-time inventory tracking captures doses received, administered, transferred, and wasted along with lot numbers and expiration dates. The platform provides visibility to monitor stock levels across all sites, identify shortages or excess inventory, and support equitable distribution. Structured reconciliation processes enable comparison of administered doses against available inventory, resolution of discrepancies, and reporting of wastage and returns.

These capabilities have been successfully implemented in Maryland, where VAULT supports vaccine distribution and tracking across a diverse provider network, enabling effective supply management, reduced wastage, and compliance with federal reporting requirements.

Real-Time Inventory Tracking

The system tracks vaccine inventory at the provider level, including:

- Doses received, administered, transferred, and wasted
- Lot numbers and expiration dates
- Distribution of inventory across provider sites and jurisdictions

Inventory is updated in real time, with administered doses automatically decremented from active inventory, ensuring that inventory data remains accurate and up to date without manual intervention.

Visibility and Oversight

The platform provides real-time visibility into inventory levels and utilization, enabling the State to:

- Monitor stock levels across all provider sites
- Identify shortages or excess inventory
- Support equitable distribution of vaccines

This visibility supports both operational management and strategic planning.

Inventory Reconciliation and Accountability

The system supports structured reconciliation processes that enable:

- Comparison of administered doses against available inventory
- Identification and resolution of discrepancies
- Reporting of vaccine wastage and returns

These capabilities support program audits, compliance monitoring, and accountability for publicly funded vaccines.

Proven Implementation

These capabilities have been successfully implemented in Maryland, where VAULT supports vaccine distribution and tracking across a diverse provider network, enabling effective supply management, reduced wastage, and compliance with federal reporting requirements.

Summary

VAULT's inventory management approach ensures accurate real-time tracking, full visibility into supply and utilization, reconciliation processes that support compliance and accountability, and data that informs both operational and strategic decision-making. This provides West Virginia with a robust, scalable, and compliant inventory management framework.

4.2.1.7.2.2 VACCINE ORDERING AND ORDER MANAGEMENT

VAULT meets this requirement by providing integrated tools for creating, managing, and tracking vaccine orders, enabling efficient coordination between providers and the State.

Order Creation and Submission

The system enables providers to:

- Create and submit vaccine orders directly within the platform

- Request inventory based on current needs and usage patterns

Order Tracking and Status Monitoring

Providers and administrators can:

- Track order status throughout the fulfillment process
- Monitor approval, processing, and distribution stages
- Maintain visibility into expected deliveries

State Oversight and Coordination

The system provides the State with the ability to:

- Review and manage incoming orders
- Monitor distribution across providers and regions
- Ensure alignment with program priorities and inventory availability

Integration with Inventory Management

Order management is fully integrated with inventory tracking, ensuring that:

- Inventory levels are updated as orders are fulfilled
- Distribution is aligned with real-time supply and demand
- The State maintains accurate, end-to-end visibility across the supply chain

Summary

VAULT's approach ensures that vaccine ordering is efficient and user-driven, order status is transparent and trackable, the State maintains control over distribution and allocation, and ordering and inventory management are fully integrated. This provides West Virginia with a streamlined, transparent, and coordinated vaccine ordering and distribution process.

4.2.1.7.2.3 VACCINE RETURNS AND WASTAGE REPORTING

VAULT meets this requirement by providing comprehensive tracking and reporting of vaccine returns and wastage, enabling the State to monitor utilization and minimize loss.

The system enables providers and administrators to record and categorize returned and wasted doses, track reasons for wastage (e.g., expiration, storage issues, damage), and generate reports at provider, site, and jurisdiction levels. These capabilities support program accountability, audit readiness, and continuous improvement in inventory management practices.

4.2.1.7.2.4 AUTOMATIC INVENTORY DECREMENT

VAULT meets this requirement by automatically decrementing administered doses from active inventory in real time, ensuring accuracy and eliminating manual reconciliation.

Each vaccine administration event:

- Updates inventory levels immediately
- Maintains alignment between clinical activity and inventory records
- Reduces risk of discrepancies and manual errors

This ensures that inventory data remains accurate, timely, and operationally reliable.

4.2.1.7.3 INTEGRATION WITH VACCINE TRACKING SYSTEMS (VTRCKS)

The PrepModEcosystem supports integration with the CDC's Vaccine Tracking System (VTrckS) in accordance with External Information System (ExIS) specifications. This integration enables the State to exchange data with federal systems to support vaccine ordering, distribution, and accountability.

VAULT's interoperability framework ensures that data exchange with VTrckS is secure, automated, and aligned with current CDC standards. The system is designed to accommodate updates to ExIS specifications, allowing the State to remain compliant as federal requirements evolve.

Automated data exchange processes reduce the need for manual data entry and improve the timeliness and accuracy of reporting. This supports efficient program operations and ensures that the State can meet federal reporting obligations.

Summary

VAULT's solution provides a comprehensive framework for supporting federal and jurisdictional vaccine program requirements. By combining configurable program management tools, real-time inventory tracking, and seamless integration with federal systems such as VTrckS, the system enables the State to manage vaccine programs effectively and maintain compliance with all applicable standards.

This approach ensures that West Virginia can confidently administer, track, and report on vaccine programs while maintaining high levels of accuracy, transparency, and operational efficiency.

4.2.1.7.3.1 — EXIS-COMPLIANT DATA EXCHANGE

VAULT establishes and maintains data exchange with the CDC's Vaccine Tracking System (VTrckS) in accordance with External Information System (ExIS) specifications. The PrepModEcosystem's interoperability framework supports standardized data exchange protocols required for vaccine ordering, shipment tracking, and inventory reporting.

The system is designed to align with CDC-defined data formats and workflows, ensuring that all exchanges with VTrckS meet current federal requirements and support accurate, timely transmission of vaccine-related data.

4.2.1.7.3.2 — UPDATES TO EXIS FUNCTIONALITY

VAULT is designed to accommodate updates to ExIS functionality following the publication of new or revised CDC specifications. The system's modular interoperability framework allows for efficient updates to data exchange components without disruption to core system operations.

VAULT maintains alignment with evolving federal standards through ongoing monitoring of CDC guidance and structured update processes, ensuring that the State remains compliant with current ExIS requirements.

4.2.1.7.3.3 — AUTOMATED DATA EXCHANGE WITH VTRCKS

VAULT establishes automated data exchange with VTrckS to support efficient and timely communication between the IIS and federal systems. Automated processes eliminate the need for manual data entry, reducing administrative burden while improving data accuracy and timeliness.

These automated exchanges support key program functions, including vaccine ordering, distribution tracking, and reporting, ensuring that the State can meet federal reporting obligations and maintain accurate, up-to-date records.

Summary

VAULT's solution provides a comprehensive framework for supporting federal and jurisdictional vaccine program requirements. By combining configurable program management tools, real-time inventory tracking, and seamless integration with federal systems such as VTrckS, the system enables the State to manage vaccine programs effectively and maintain compliance with all applicable standards.

This approach ensures that West Virginia can confidently administer, track, and report on vaccine programs while maintaining high levels of accuracy, transparency, and operational efficiency.

4.2.1.8 SUPPORT THE RESPONSE EFFORTS FOR VACCINE-PREVENTABLE DISEASE OUTBREAKS AND OTHER PUBLIC HEALTH EMERGENCIES

VAULT enables West Virginia to rapidly establish, scale, and operate vaccination efforts during public health emergencies through a fully integrated, field-ready platform. The PrepModEcosystem supports the complete lifecycle of emergency response—preparedness, activation, onboarding, execution, and reporting—within a single unified system.

Configurable workflows, rapid onboarding tools, real-time coordination, and high-volume vaccination capabilities allow providers, public health teams, and partners to activate quickly and operate efficiently. Built-in offline functionality ensures uninterrupted registration, documentation, and vaccine administration in mobile, pop-up, and rural settings. Integrated reporting delivers immediate visibility into activity, coverage, and performance for decision-making and federal submissions.

Proven in large-scale real-world responses, including statewide COVID-19 vaccination initiatives, VAULT has repeatedly demonstrated fast provider onboarding, reliable operations under pressure, and accurate data capture across diverse environments.

What Sets VAULT Apart

VAULT delivers emergency response as a cohesive, end-to-end capability—enabling the State to move from preparedness to full execution rapidly, reliably, and at scale.

Key differentiators include:

- Unified Platform – Integrates onboarding, scheduling, clinical workflows, communication, and reporting in one system, eliminating fragmented tools.
- Rapid Activation – Template-based setups and configurable workflows allow providers and sites to go live within hours.
- Robust Offline Capability – Full vaccine administration continues seamlessly in low- or no-connectivity environments.
- High-Volume Scalability – Handles surge demand with integrated scheduling, throughput management, and real-time coordination.

- Proven Performance – Successfully powered statewide emergency campaigns with fast deployment and continuous operational visibility.

4.2.1.8.1 PROVIDER ONBOARDING AND EMERGENCY RESPONSE COORDINATION

VAULT provides a comprehensive, end-to-end capability that enables West Virginia to rapidly activate, coordinate, and sustain vaccination efforts during public health emergencies. Through integrated onboarding, training, offline functionality, scheduling, and real-time reporting, the platform supports the full response lifecycle—from initial activation through sustained operations and performance monitoring.

4.2.1.8.1.1 EXECUTES EMERGENCY PREPAREDNESS PLANS

VAULT meets this requirement by operationalizing the full lifecycle of emergency response—preparedness, activation, coordination, and execution—within a single unified platform aligned with federal and jurisdictional policies..

Preparedness and Planning

Preparedness features include configurable workflows, template-based clinic setups, defined roles, and training tools that turn plans into immediately activatable system configurations. During active response, the platform enables real-time coordination of workforce, volunteers, sites, and partners; scalable high-volume operations; and offline functionality for continuity.

This includes:

- Pre-configured and customizable workflows for vaccination campaigns, outbreak response, and emergency scenarios
- Template-based clinic setup, including registration, consent, and documentation processes
- Defined user roles and permissions aligned with emergency response responsibilities
- Training and simulation support to prepare providers and staff prior to activation

These capabilities ensure that emergency response plans are not static documents, but are fully operationalized within the system and ready for immediate activation.

Coordination of Emergency Response

During an active response, VAULT enables real-time coordination across providers, sites, and public health teams within a single system.

The platform supports:

- Coordination of workforce, volunteers, and partner organizations, including mobile units and community-based providers
- Scheduling, site management, and operational coordination of vaccination events
- Real-time data exchange across providers, EHRs, and public health systems

This unified approach reduces fragmentation, improves communication, and ensures that all participating entities operate within a coordinated framework.

Execution of Emergency Operations

VAULT supports the execution of emergency response activities through scalable, high-performance infrastructure designed for surge scenarios.

This includes:

- Rapid deployment of vaccination sites and workflows, enabling new clinics to be activated quickly
- High-volume registration, check-in, and vaccine administration workflows to support mass vaccination efforts
- Real-time data capture and reporting, providing immediate visibility into vaccination activity and coverage

- Offline functionality, enabling continued operations in environments with limited or no connectivity

These capabilities ensure that emergency operations can be executed reliably, even under high demand and constrained conditions.

Alignment with Federal and Jurisdictional Policy

VAULT is designed to align with federal standards and jurisdiction-specific requirements through:

- Support for CDC IIS Functional Standards and HL7 v2.5.1 messaging
- Configurable workflows and data elements that allow the State to implement jurisdiction-specific policies without custom development
- Integration with federal systems and reporting requirements, including real-time data submission

This ensures that all emergency response activities remain compliant with applicable policies and standards.

Proven Emergency Response Capability

VAULT has successfully supported large-scale emergency response efforts, including statewide COVID-19 vaccination campaigns. In these scenarios, the platform enabled rapid onboarding of providers, deployment of vaccination sites, and real-time data reporting across diverse environments.

This experience demonstrates VAULT's ability to operationalize and execute emergency preparedness plans effectively in real-world conditions.

Summary

VAULT transforms emergency preparedness from a planning exercise into an executable, system-driven capability.

By enabling the State to establish, coordinate, and execute emergency response activities within a unified platform, VAULT ensures that West Virginia can respond rapidly, operate efficiently, and maintain compliance during public health emergencies.

4.2.1.8.1.2 EXPEDITED COMMUNICATION AND DATA CAPTURE

VAULT meets this requirement by delivering a rapid, role-based training model specifically designed for emergency response scenarios, enabling newly onboarded partners to begin using the system quickly and effectively.

During vaccine-preventable disease outbreaks and public health emergencies, VAULT implements an accelerated onboarding and training approach that includes:

- **Rapid deployment training sessions**, delivered virtually and available on-demand, allowing partners to be trained within compressed timeframes
- **Role-based training tracks**, tailored to providers, clinic staff, public health personnel, and non-traditional partners (e.g., schools, mobile clinics, community organizations)
- **Simplified, workflow-driven training materials**, focused on essential tasks such as registration, vaccine administration, and data reporting
- **Just-in-time guidance and support**, ensuring that users can access help at the point of need during live operations
- **Hands-on, scenario-based training**, enabling users to practice critical workflows prior to or during activation

This approach is supported by the platform's intuitive, browser-based design, which minimizes training requirements and allows even first-time users to quickly become effective in high-volume or high-pressure environments.

VAULT's rapid training model is designed to ensure that newly onboarded partners can begin administering vaccines and reporting data within hours, depending on the scale and urgency of the response, while maintaining data quality and compliance.

VAULT has successfully implemented this approach in real-world emergency scenarios. For example, in Maryland, VAULT conducted rapid onboarding and training for newly participating providers during large-scale vaccination efforts, enabling them to begin administering vaccines and reporting data within compressed timelines. This ensured consistent system usage, minimized delays, and supported continuity of operations during peak demand periods.

4.2.1.8.1.3 TRAINING AND SUPPORT FOR EMERGENCY OPERATIONS

VAULT meets this requirement by delivering a rapid, role-based training model designed specifically for emergency response scenarios, enabling newly onboarded partners to begin using the system quickly and effectively.

During vaccine-preventable disease outbreaks and public health emergencies, VAULT implements an accelerated training approach that supports immediate readiness and operational continuity.

Rapid, Role-Based Training Model

VAULT provides targeted training aligned to user roles and emergency workflows, ensuring that all participants are prepared to perform their responsibilities effectively.

This includes:

- Rapid deployment training sessions, delivered virtually and available on-demand, enabling training within compressed timeframes
- Role-based training tracks tailored to providers, clinic staff, public health personnel, and non-traditional partners (e.g., schools, mobile clinics, community organizations)
- Simplified, workflow-driven training materials focused on critical tasks such as registration, vaccine administration, and data reporting
- Hands-on, scenario-based training that allows users to practice essential workflows prior to or during activation

Just-in-Time Training and Support

VAULT supports users during live operations through embedded guidance and accessible support resources.

This includes:

- Just-in-time guidance to assist users at the point of need during active response operations
- Contextual support aligned with system workflows, reducing reliance on external documentation
- Streamlined user experience supported by an intuitive, browser-based interface that minimizes training requirements

These capabilities ensure that even first-time users can quickly become effective in high-volume, high-pressure environments.

Rapid Readiness and Deployment

VAULT's training model is designed to support rapid activation of newly onboarded partners, enabling them to begin administering vaccines and reporting data within hours, depending on the scale and urgency of the response.

This approach ensures that speed does not come at the expense of data quality, compliance, or operational consistency.

Proven Emergency Training Execution

VAULT has successfully implemented this rapid training approach in real-world emergency scenarios. In Maryland, VAULT conducted accelerated onboarding and training for newly participating providers during large-scale vaccination efforts, enabling them to begin administering vaccines and reporting data within compressed timelines.

This ensured consistent system usage, minimized delays, and supported continuity of operations during peak demand periods.

Summary

VAULT ensures that West Virginia can rapidly prepare and enable partners to participate in emergency response efforts through a structured, scalable, and role-based training approach.

By combining rapid deployment training, intuitive system design, and real-time support, VAULT enables partners to become operational quickly while maintaining accuracy, compliance, and efficiency during public health emergencies.

4.2.1.8.1.4 VACCINE ADMINISTRATION AND OFFLINE CAPABILITIES

VAULT meets this requirement by providing robust, fully integrated offline capabilities that enable vaccine administration workflows to continue uninterrupted in environments with limited or no connectivity.

The PrepModEcosystem supports offline operation across all core applications, ensuring that registration, check-in, vaccine administration, and documentation can be performed reliably in field-based and emergency settings.

Offline Data Capture and Workflow Continuity

VAULT enables providers to perform all critical vaccination workflows without requiring continuous network connectivity.

This includes:

- Offline registration, check-in, and vaccine administration documentation
- Capture of patient demographic and vaccination data at the point of care
- Support for high-throughput workflows in mobile, pop-up, and temporary clinic environments
- Consistent user experience across online and offline modes, minimizing disruption for staff

These capabilities ensure that vaccination operations can continue without interruption, regardless of connectivity conditions.

Secure Data Storage and Synchronization

Data captured offline is securely stored within the system and automatically synchronized once connectivity is restored.

This includes:

- Secure local data storage during offline operation
- Automated synchronization of all captured data to the IIS and integrated systems
- Conflict resolution and validation processes to ensure data integrity and prevent duplication
- Alignment of synchronized data with real-time reporting and inventory management processes

This approach ensures that all administered doses are accurately recorded and integrated into the system of record.

Reliability in Emergency and Field Environments

VAULT's offline capabilities are designed specifically for use in dynamic and resource-constrained environments, including:

- Mobile clinics operating in rural or remote areas
- Pop-up vaccination sites with inconsistent connectivity
- Emergency response settings where network infrastructure may be unavailable or degraded

By enabling uninterrupted operations in these environments, VAULT ensures continuity of care and data capture during critical response efforts.

Proven Field Performance

VAULT has successfully demonstrated offline functionality in real-world emergency and field-based scenarios. In Maryland, the platform supported mobile and pop-up clinics operating under variable connectivity conditions, allowing providers to continue vaccination activities without interruption and synchronize data once connectivity was restored.

This ensured complete and accurate data capture while maintaining operational efficiency in diverse environments.

Summary

VAULT ensures that West Virginia can maintain uninterrupted vaccination operations and complete data capture regardless of connectivity conditions.

By providing fully integrated offline capabilities across all core workflows, VAULT enables reliable, field-ready operations and ensures that all vaccination activity is ultimately captured, synchronized, and available for reporting and decision-making.

4.2.1.8.1.5 INTEGRATION WITH SCHEDULING AND OPERATIONAL TOOLS

VAULT meets this requirement by providing fully integrated, high-volume scheduling capabilities that support the coordination and execution of vaccination appointments and clinic operations during emergency response scenarios.

The PrepModEcosystem enables the State to manage scheduling as part of a unified operational workflow, integrating appointment management with registration, check-in, vaccine administration, and reporting.

High-Volume Appointment Scheduling

VAULT supports large-scale scheduling required for emergency response efforts, including:

- Creation and management of high-volume vaccination appointment slots across multiple sites
- Support for mass scheduling events, including public registration and targeted outreach
- Real-time appointment availability and capacity management
- Configurable scheduling rules based on eligibility, location, and priority groups

These capabilities enable jurisdictions to rapidly scale appointment availability and manage demand during surge scenarios.

Clinic Throughput and Resource Management

Scheduling is tightly integrated with clinic operations to support efficient patient flow and resource utilization.

This includes:

- Alignment of appointment scheduling with staffing levels, vaccine supply, and site capacity
- Support for walk-in and appointment-based workflows within the same system
- Real-time visibility into appointment volumes, check-in status, and clinic throughput
- Tools to optimize patient flow and reduce bottlenecks at high-volume sites

This ensures that scheduling is not isolated, but directly supports efficient clinic operations.

Integrated Operational Workflow

VAULT integrates scheduling with all downstream workflows, ensuring seamless execution from appointment to reporting.

This includes:

- Automated transition from scheduling to registration and check-in workflows
- Integration with vaccine administration and documentation processes
- Real-time data capture and reporting tied directly to scheduled appointments
- Synchronization with inventory and supply management to align demand with available resources

This end-to-end integration improves operational efficiency and reduces administrative burden.

Proven High-Volume Scheduling Performance

VAULT has demonstrated these capabilities in real-world emergency response scenarios. In Maryland, the platform supported large-scale scheduling and clinic coordination efforts, enabling efficient management of high-volume vaccination events and optimization of patient flow and staffing across sites.

This ensured that vaccination operations could scale rapidly while maintaining efficiency and a positive patient experience.

Summary

VAULT enables West Virginia to efficiently schedule, coordinate, and manage high-volume vaccination operations during public health emergencies.

By integrating scheduling with clinic operations, resource management, and real-time reporting, VAULT ensures that the State can scale vaccination efforts quickly while maintaining efficiency, visibility, and control.

4.2.1.8.1.6 PUBLIC HEALTH REPORTING DURING EMERGENCIES

VAULT meets this requirement by providing real-time, integrated reporting capabilities that support timely, accurate data submission to federal and jurisdictional authorities during emergency response efforts.

The PrepModEcosystem ensures that all vaccination activity is captured, aggregated, and made available for reporting without delay, enabling continuous visibility into program performance and public health impact.

Real-Time Reporting and Data Availability

VAULT enables immediate access to vaccination data across all participating providers, sites, and jurisdictions.

This includes:

- Real-time visibility into vaccination activity, coverage rates, and operational performance
- Continuous data availability for both standard reporting and ad hoc analysis
- Immediate access to data at the State, regional, and provider levels

These capabilities ensure that public health leadership can monitor progress and respond quickly as conditions evolve.

Integrated Reporting to IIS and Federal Systems

Reporting is fully integrated with system workflows, ensuring that data is captured once and made available across all required reporting channels.

This includes:

- Automated data submission to the IIS and federal systems in accordance with established standards
- Alignment with HL7 and other required reporting formats
- Integration with federal reporting requirements, including support for real-time data exchange where applicable
- Elimination of manual reporting processes through automated data flow

This ensures accurate, consistent, and timely reporting across all required systems.

Analytics and Decision Support

VAULT supports data-driven decision-making during emergency response through advanced reporting and analytics capabilities.

This includes:

- Monitoring of vaccine uptake and coverage trends across populations and geographies
- Identification of underserved or under-vaccinated populations
- Support for targeted outreach and resource allocation strategies
- Real-time dashboards and reporting tools to inform operational and strategic decisions

These capabilities enable jurisdictions to adapt response strategies based on current data and emerging needs.

Proven Emergency Reporting Capability

VAULT has demonstrated these capabilities in real-world emergency response scenarios. In Maryland, the platform enabled public health leadership to monitor vaccination progress across jurisdictions, identify disparities in coverage, and implement targeted outreach strategies during critical phases of the response.

This ensured that response efforts were data-driven, responsive, and effective.

Summary

VAULT ensures that West Virginia has continuous, real-time visibility into vaccination activity, program performance, and population coverage during public health emergencies.
By integrating data capture, reporting, and analytics within a unified platform, VAULT enables accurate, timely reporting to federal and jurisdictional authorities while supporting informed decision-making and adaptive response strategies.

4.2.1.9 PARTICIPATE IN AND PRIORITIZE EMERGING TECHNOLOGIES AND STANDARDS

VAULT enables West Virginia to adopt and advance emerging technologies and standards through a modern, interoperable platform purpose-built for the future of public health data exchange.

The PrepModEcosystem features a flexible, standards-based architecture supporting both current and emerging interoperability frameworks, including HL7 v2.5.1 messaging and FHIR-based APIs. This foundation allows seamless integration with healthcare providers, public health agencies, and federal partners while preparing for the continued evolution of national standards.

VAULT approaches modernization through coordinated planning, phased implementation, and ongoing stakeholder collaboration. This ensures enhancements are practical, scalable, and aligned with State and federal priorities.

VAULT also actively participates in national initiatives that shape IIS and public health technology. Engagement with organizations such as AIRA and AIM — along with solutions like IISConnex — allows the platform to contribute to standards development and demonstrate emerging capabilities in live production environments.

What Sets VAULT Apart

VAULT distinguishes itself by delivering modernization as a coordinated, strategic capability rather than isolated upgrades. This enables the State to adopt new technologies in a structured, scalable, and sustainable manner.

Key differentiators include:

- Modernization as a Coordinated System Capability – A centralized platform and collaborative model that aligns stakeholders and eliminates fragmentation.
- Flexible Standards-Based Architecture – Native support for HL7 v2.5.1 and FHIR allows adoption of emerging standards without disruptive overhauls.
- Disciplined Planning and Phased Implementation – Structured prioritization and incremental delivery aligned with State priorities and operational needs.
- Active National Engagement – Direct participation with AIRA, AIM, and interoperability initiatives to influence and stay ahead of evolving standards.
- Proven Operationalization – IISConnex demonstrates the ability to turn national standards into production-ready capabilities across jurisdictions.
- The platform's modular design and continuous delivery pipeline (ArgoCD + Terraform) allow us to adopt emerging standards via API-first changes and automated regression suites, without rip-and-replace overhauls.

4.2.1.9.1 PARTICIPATION IN MODERNIZATION INITIATIVES

VAULT delivers a structured, end-to-end approach to modernization that enables coordinated planning and execution of system enhancements in alignment with national standards and State priorities. Through centralized capabilities and continuous collaboration, the platform ensures modernization is efficient, consistent, and sustainable.

The platform supports disciplined planning and prioritization of enhancements aligned with federal initiatives and emerging standards, while its modular architecture enables phased, low-disruption implementation. In addition, VAULT actively participates in national interoperability and standards development initiatives, including engagement with organizations such as AIRA and AIM, ensuring alignment with evolving best practices and contributing to the advancement of the IIS ecosystem.

By combining coordination, strategic planning, and active participation in modernization efforts, VAULT ensures that West Virginia can implement enhancements efficiently, remain compliant with evolving requirements, and adopt new capabilities in a structured and sustainable manner.

4.2.1.9.1.1 COORDINATION OF MODERNIZATION EFFORTS

VAULT meets this requirement through a centralized platform and collaborative delivery model that unifies stakeholders, systems, and workflows.

Structured collaboration includes regular engagement with State leadership, joint priority setting, backlog management, and iterative delivery of enhancements. A unified platform standardizes processes and provides role-based access to support consistent execution across the public health ecosystem.

In practice, this model has enabled weekly alignment sessions, ongoing prioritization, and smooth implementation of new capabilities without disrupting daily operations.

Centralized Platform for Coordination

VAULT enables coordination of modernization efforts through a shared platform that aligns stakeholders and standardizes workflows.

This includes:

- A unified system for data capture, workflow execution, and reporting across all participating entities
- Standardized processes that promote consistency across providers and jurisdictions
- Role-based configuration that supports coordination across diverse user groups

These capabilities reduce fragmentation and ensure that modernization efforts are implemented within a cohesive operational framework.

Continuous and Iterative Modernization

VAULT supports ongoing coordination of modernization efforts through a continuous development model.

In Maryland, VAULT has implemented a structured approach that includes weekly collaboration sessions with State leadership, ongoing backlog prioritization, and iterative delivery of enhancements. This model ensures that modernization initiatives remain aligned with evolving priorities and can be implemented efficiently without disrupting ongoing operations.

Summary

VAULT enables West Virginia to coordinate modernization efforts through a combination of structured collaboration, a centralized platform, and a continuous delivery model.
By aligning stakeholders, standardizing workflows, and supporting iterative enhancement, VAULT ensures that modernization initiatives are executed effectively, efficiently, and in alignment with State priorities.

4.2.1.9.1.2 ALIGNMENT WITH MODERNIZATION PRIORITIES

VAULT aligns system enhancements with both national direction and jurisdiction-specific needs through disciplined planning and a modular enhancement approach.
This includes support for emerging standards such as FHIR alongside continued HL7 v2.5.1 capabilities, interoperability improvements, and alignment with federal IIS initiatives.
Enhancements are prioritized through joint planning sessions and managed via a transparent backlog process. Phased implementation strategies allow new capabilities to be introduced incrementally with minimal operational impact.
A proactive roadmap ensures ongoing alignment with evolving federal requirements and emerging technologies.

Alignment with National and Jurisdictional Priorities

VAULT aligns system enhancements with federal guidance and jurisdiction-specific priorities, ensuring that modernization efforts support both compliance and program objectives.
This includes:

- Adoption and support of emerging standards such as HL7 FHIR and continued support for HL7 v2.5.1 messaging

- Enhancement of interoperability capabilities to support data exchange across public health and healthcare systems
- Alignment of system capabilities with federal initiatives and evolving IIS Functional Standards

These capabilities ensure that the State's modernization efforts remain aligned with broader national direction while addressing local needs.

Structured Planning and Prioritization

VAULT supports disciplined planning and prioritization of modernization initiatives through a collaborative and transparent process.

This includes:

- Joint planning with State stakeholders to define modernization priorities and timelines
- Backlog management aligned with program goals, regulatory requirements, and operational needs
- Phased implementation strategies that allow for incremental adoption of new capabilities

This structured approach ensures that modernization efforts are executed efficiently and in alignment with State priorities.

Modular and Scalable Enhancement Model

VAULT's modular architecture enables targeted system enhancements without requiring large-scale system overhauls.

This includes:

- Incremental delivery of new capabilities through modular system components
- Ability to introduce enhancements with minimal disruption to ongoing operations
- Scalable infrastructure that supports growth across programs and users

This approach allows jurisdictions to adopt new capabilities in a controlled and sustainable manner.

Proactive Roadmap and Continuous Alignment

VAULT maintains ongoing awareness of evolving federal requirements and emerging technologies, incorporating these into a forward-looking system roadmap.
This includes:

- Continuous monitoring of federal guidance and modernization initiatives
- Proactive incorporation of new standards and capabilities into the platform
- Regular updates to ensure ongoing compliance and readiness for future requirements

This ensures that the State remains prepared for future initiatives without requiring reactive or disruptive changes.

Summary

VAULT enables West Virginia to plan and execute modernization efforts in a structured, strategic, and forward-looking manner.
By aligning enhancements with national standards, State priorities, and a proactive roadmap, VAULT ensures that modernization initiatives are implemented efficiently, sustainably, and in support of long-term public health goals.

4.2.1.9.1.3 PARTICIPATION IN STANDARDS DEVELOPMENT AND INNOVATION

VAULT actively engages in national initiatives to advance standards and interoperability within the IIS community. The platform maintains strong relationships with the American Immunization Registry Association (AIRA), the Association of Immunization Managers (AIM), Health ISAC, and other key working groups.
This participation informs platform direction while allowing VAULT to contribute practical insights back to the community. Through IISConnex, VAULT has successfully operationalized both HL7 and FHIR-based interoperability across multiple states, turning emerging standards into scalable, real-time data exchange solutions.

The platform also incorporates ongoing innovation in areas such as data quality automation, analytics, and user experience — all delivered in a way that benefits the entire client community.

This combination of national engagement and proven implementation capability positions West Virginia to not only adopt emerging technologies, but to help shape their practical application in public health.

Active Participation in National Initiatives

VAULT participates in initiatives that promote interoperability, standardization, and modernization across the IIS ecosystem.

This includes:

- Engagement with AIRA, AIM, Health ISC and national working groups focused on IIS modernization and interoperability
- Contribution to best practices and alignment with emerging standards and implementation guidance
- Collaboration with public health agencies, technology partners, and stakeholders to advance shared capabilities

These efforts ensure that VAULT remains aligned with national priorities and contributes to the broader evolution of public health technology.

Operationalizing Emerging Standards

VAULT not only adopts emerging standards but operationalizes them in real-world environments.

Through solutions such as IISConnex, VAULT has developed scalable interoperability capabilities that support both HL7 and FHIR-based data exchange across multiple jurisdictions. These implementations demonstrate VAULT's ability to translate emerging standards into practical, production-ready solutions that support real-time data exchange and cross-system coordination.

Innovation and Continuous Capability Advancement

VAULT continuously evaluates and incorporates new technologies that enhance system functionality and support evolving public health needs.

This includes:

- Automation of data validation and quality assurance processes
- Enhanced analytics and reporting capabilities to support decision-making
- Ongoing improvements to user experience and workflow efficiency

These innovations are incorporated into the platform in a way that benefits all clients, ensuring continuous advancement without requiring significant reinvestment by the State.

Summary

VAULT enables West Virginia to participate in and benefit from national modernization efforts through active engagement, practical implementation of emerging standards, and continuous innovation.

By combining participation in national initiatives with the ability to operationalize new capabilities, VAULT ensures that the State remains aligned with evolving standards while adopting new technologies in a structured, reliable, and future-ready manner.

4.2.2 WEST VIRGINIA SPECIFIC GOALS AND OBJECTIVES

VAULT meets the West Virginia-specific goals and objectives by delivering a configurable, operationally focused IIS platform designed to address the State's unique environment, including its rural provider network, high-volume data exchange requirements, and need for real-time, actionable public health data.

Unlike a one-size-fits-all implementation, VAULT's approach is tailored to West Virginia's existing workflows, data volumes, and operational priorities, ensuring a seamless transition from the current system while enabling measurable improvements in performance, data quality, and usability.

Understanding West Virginia's Environment

The State currently manages:

- Approximately 2.9 million patient records
- Over 31 million vaccination records
- A diverse network of providers, including rural clinics, pharmacies, and public health entities

This environment presents specific challenges, including:

- Variability in provider technical capabilities
- High reliance on HL7-based data exchange
- Need for accurate, real-time reporting for public health decision-making
- Requirement for scalable infrastructure to support both routine operations and emergency response

VAULT's solution is designed specifically to address these conditions.

Operational Approach for West Virginia

VAULT's approach focuses on how the system functions in daily operations, including:

Provider Data Submission and Validation

- Providers submit data via HL7 or web entry
- Messages are validated in real time (structure, code sets, completeness)
- Errors are routed to structured hold queues for resolution

HL7 Error and Hold Queue Management

- OEPS staff can view, categorize, and resolve HL7 errors
- Errors are tracked, assigned, and corrected through workflow tools
- Providers receive feedback to prevent recurring issues

Data Quality and Patient Record Management

- Duplicate and fragmented records are automatically identified and resolved
- A single, longitudinal patient record is maintained
- Data quality is continuously monitored and improved

Clinical Decision Support and Forecasting

- ACIP-aligned forecasts are generated in real time
- Providers receive consistent recommendations across all sites
- Forecast data is used for reporting, outreach, and reminder/recall

Reporting and Public Health Analytics

- OEPS staff can generate reports using defined numerator/denominator logic
- Reports can be filtered by geography, provider, or population group
- Real-time dashboards support identification of coverage gaps

Why VAULT's Approach is Superior for West Virginia

Traditional IIS implementations focus primarily on data storage and reporting.

VAULT's approach differs by:

- Providing operational workflows, not just data repositories
- Enabling real-time data validation and correction, reducing downstream errors
- Supporting rural provider onboarding and participation, improving data completeness
- Delivering actionable insights, not just static reports
- Enabling the State to actively manage and improve immunization outcomes

Outcome for West Virginia

By implementing VAULT's solution, the State will:

- Improve data quality, completeness, and timeliness
- Reduce administrative burden on OEPS staff and providers
- Increase provider participation and engagement
- Enable faster, more accurate public health decision-making
- Strengthen its ability to respond to public health needs and emergencies

4.2.2.1 SYSTEM OPTIMIZATION, INNOVATION, AND INTEROPERABILITY

VAULT meets this requirement by providing a structured, transparent, and continuously operating framework for system optimization and enhancement delivery, ensuring that West Virginia's IIS evolves in alignment with operational needs, user feedback, and emerging public health requirements.

Rather than treating enhancements as isolated or one-time efforts, VAULT delivers a continuous improvement model that evaluates, prioritizes, develops, and deploys enhancements in a repeatable and governed manner.

VAULT's approach is specifically designed to support West Virginia's rural and geographically dispersed population by enabling scalable, community-based service delivery and real-time visibility into immunization coverage across counties, districts, and underserved regions.

How VAULT Meets This Requirement

1. Enhancement Identification and Evaluation

Enhancements are identified through:

- OEPS feedback and operational needs
- System analytics (e.g., HL7 error trends, data quality metrics)
- Provider feedback and support interactions
- Federal and industry requirements (CDC, interoperability standards)

Each enhancement is evaluated based on:

- Applicability across jurisdictions
- Impact on system performance, data quality, or usability
- Alignment with CDC and State priorities

2. Structured Release Process and Timeline

Enhancements are delivered through a controlled release process:

- Prioritized enhancements are developed within Agile release cycles

- Functionality is tested in staging environments
- Validated changes are deployed through scheduled production releases
- Release timelines are communicated in advance to the State

This ensures predictable delivery while maintaining system stability.

3. Governance and Communication

VAULT maintains a structured governance model that includes:

- Regular user group meetings with participating jurisdictions
- Formal communication of upcoming enhancements and changes
- Release notes, documentation, and training materials for each update

West Virginia will have direct input into enhancement prioritization and visibility into the product roadmap.

4. Operational Impact in West Virginia

For West Virginia, this approach enables continuous improvement in key operational areas, including:

- **HL7 error and hold queue management**, where recurring issues can be identified and addressed through targeted enhancements
- **Provider onboarding workflows**, improving participation and reducing submission errors
- **Reporting and analytics**, enabling refinement of numerator/denominator logic and coverage calculations
- **User experience improvements**, reducing administrative burden for OEPS staff and providers

Enhancements are not theoretical—they are driven by real operational needs and applied directly to improve system performance.

What Sets VAULT Apart

VAULT distinguishes its approach through a shared innovation model that delivers continuous, system-wide improvement:

- **Shared Enhancement Model:**
  Enhancements developed for one jurisdiction are evaluated and incorporated into the core platform when broadly applicable, reducing duplication and accelerating innovation
- **Data-Driven Optimization:**
  Enhancements are informed by system metrics such as error rates, performance indicators, and user behavior—not just feature requests
- **Continuous Delivery Model:**
  Frequent, controlled releases ensure rapid time-to-value without disrupting system operations
- **Integrated Adoption Support:**
  Training, release communication, and in-application guidance ensure that enhancements are quickly understood and adopted
- **Standards-Based Interoperability:**
  Ongoing support for HL7, FHIR, and emerging standards ensures long-term sustainability and integration flexibility

Proven Enhancement Delivery

VAULT has demonstrated the ability to translate jurisdiction-specific needs into scalable platform improvements.

For example:

- Enhancements to HL7 validation and error handling workflows have been implemented to reduce data submission errors
- Reporting enhancements have improved visibility into coverage gaps and population health trends
- Workflow improvements have streamlined provider onboarding and participation

These enhancements have been successfully deployed across multiple jurisdictions, ensuring that innovation delivers measurable impact.

4.2.2.1.1 CONTINUOUS IMPROVEMENT AND SHARED ENHANCEMENTS

VAULT provides a structured, collaborative approach to developing, evaluating, and delivering system enhancements that benefit all jurisdictions.

Enhancements originating from individual jurisdictions are evaluated through a formal product management process and validated through cross-jurisdictional input, including feedback from user groups and real-world system usage. Enhancements that demonstrate broad applicability are incorporated into the core platform and delivered as standardized capabilities at no additional cost.

VAULT's Agile-based delivery model ensures that enhancements are developed, validated through user acceptance testing, and released through controlled, predictable release cycles. Comprehensive communication, training, and in-application guidance support rapid adoption of new capabilities.

Through structured governance, transparent communication, and active user participation, VAULT enables jurisdictions to remain informed, engaged, and directly involved in shaping platform evolution.

Together, these capabilities ensure that West Virginia benefits from continuous, shared innovation while contributing to the advancement of a scalable, modern public health platform.

4.2.2.1.1.1 EVALUATION OF ENHANCEMENTS

VAULT meets this requirement by applying a structured, product-driven evaluation process to determine whether enhancements developed for a specific jurisdiction should be incorporated into the broader platform for the benefit of all users.

All enhancements are evaluated through a formal product management process that includes:

- Assessment of the originating jurisdiction's requirement or use case
- Evaluation of applicability across other jurisdictions and programs

- Review of alignment with CDC standards, interoperability requirements, and overall platform architecture
- Input from cross-jurisdictional stakeholders, including feedback gathered through user groups and industry engagement

Cross-Jurisdictional Collaboration and Industry Input

VAULT actively incorporates feedback from a broad network of users and stakeholders to inform enhancement decisions.

This includes:

- A user group that meets at least quarterly to provide input on system enhancements, priorities, and emerging needs
- Ongoing engagement with public health partners and industry organizations to identify trends and best practices
- Continuous feedback from real-world system use across multiple jurisdictions

This ensures that enhancement decisions are informed not only by a single implementation, but by the evolving needs of the broader public health community.

Platform-Based Enhancement Model

Enhancements that demonstrate broad value are incorporated into the core PrepModEcosystem platform and delivered as standardized capabilities rather than one-off customizations.

This approach:

- Ensures consistency across implementations
- Reduces duplication of effort
- Enables all jurisdictions to benefit from ongoing innovation
- Supports long-term sustainability and maintainability of the platform

At the same time, the platform's configurability allows jurisdictions to address specific needs without compromising the integrity of the shared system.

Continuous Improvement Approach

VAULT maintains a continuous improvement model in which enhancements are regularly evaluated and incorporated as public health needs evolve.

This ensures that the platform remains responsive to changing requirements while delivering ongoing value to all jurisdictions without requiring separate redevelopment efforts.

Summary

VAULT ensures that system enhancements are evaluated and implemented in a way that maximizes value across all jurisdictions.

By combining structured product management, cross-jurisdictional collaboration, and a continuous improvement model, VAULT enables West Virginia to benefit from shared innovation while contributing to the advancement of a modern, scalable public health platform.

4.2.2.1.1.2 RELEASE PROCESS AND TIMELINE

VAULT meets this requirement by following a structured, Agile-based release management process that ensures enhancements are developed, validated, and deployed efficiently while maintaining system stability, usability, and adoption.

Agile Development and Iterative Delivery

VAULT utilizes an Agile delivery model to support continuous enhancement and timely release of new capabilities.

Key elements include:

- Bi-weekly sprint cycles for development and internal testing
- Continuous prioritization of enhancements based on impact, urgency, and cross-jurisdictional value
- Iterative delivery of features to support rapid progression from concept to deployment

This approach enables VAULT to respond quickly to evolving needs while maintaining a steady cadence of improvements.

User Acceptance Testing and Validation

Enhancements undergo structured validation prior to release to ensure they meet functional requirements and perform effectively in real-world scenarios.

This includes:

- User Acceptance Testing (UAT) with jurisdictional stakeholders, where applicable
- Validation of workflows and data accuracy in representative use cases
- Incorporation of feedback from pilot implementations or early adopters

This ensures that enhancements are both technically sound and operationally effective.

Release Management and Deployment

VAULT follows a controlled release process to ensure stability and minimize disruption to ongoing operations.

This includes:

- Regular release cycles that bundle validated enhancements into standard platform updates
- Deployment through controlled release pipelines with testing and quality assurance checkpoints
- Communication of upcoming releases and included enhancements to all jurisdictions

Enhancements identified as broadly beneficial are incorporated into upcoming release cycles and made available to all jurisdictions as part of standard platform updates.

Training, Communication, and User Enablement

VAULT ensures that jurisdictions are fully informed and prepared to adopt new capabilities through a comprehensive communication and training approach.

This includes:

- Detailed release notes outlining new features, enhancements, and any changes to existing workflows
- Live training sessions for new capabilities, with recordings made available for on-demand access

- Short-form training videos and documentation to support quick understanding and adoption
- In-application guidance and contextual help, where appropriate, to support users at the point of need

This approach ensures that users can quickly understand and effectively utilize new features without placing additional burden on the State.

Predictable and Scalable Timeline

VAULT's structured release model provides a predictable and scalable timeline for enhancement delivery.

This includes:

- Short development cycles (typically within sprint intervals) for initial feature completion
- Inclusion in scheduled release cycles following validation and testing
- Ability to accelerate delivery for high-priority or time-sensitive enhancements when needed

This ensures timely access to new capabilities while maintaining system reliability.

Summary

VAULT ensures that enhancements are delivered through a structured, validated, and user-centered process that balances speed, quality, and adoption.

By combining Agile development, stakeholder validation, controlled release management, and comprehensive training and communication, VAULT enables West Virginia to benefit from continuous improvements that are delivered efficiently, reliably, and fully adopted by users.

4.2.2.1.1.3 GOVERNANCE AND COMMUNICATION

VAULT meets this requirement by maintaining a structured governance and communication model that ensures jurisdictions are consistently informed of system improvements and actively engaged in the evolution of the platform.

Structured Governance and Stakeholder Engagement

VAULT establishes clear governance practices that enable jurisdictions to participate in decision-making and prioritization of system enhancements.

This includes:

- Regular product roadmap reviews with client stakeholders to align on priorities and upcoming enhancements
- Ongoing engagement with jurisdictional partners to gather input on system performance, emerging needs, and enhancement opportunities
- Use of feedback mechanisms, including user groups and direct stakeholder input, to inform product direction

These practices ensure that jurisdictions have visibility into and influence over platform evolution.

Transparent Release Communication

VAULT provides clear and consistent communication regarding system updates and enhancements.

This includes:

- Detailed release notes outlining new features, enhancements, and changes to existing workflows
- Advance communication of upcoming releases and planned updates
- Access to training resources and supporting materials associated with new capabilities

This approach ensures that jurisdictions are fully informed and prepared for system updates.

User Group Collaboration and Knowledge Sharing

VAULT facilitates cross-jurisdictional collaboration through structured user group engagement.

This includes:

- Regular user group meetings to share best practices, highlight new capabilities, and gather feedback

- Opportunities for jurisdictions to learn from one another and identify shared challenges and solutions
- Incorporation of user group input into product planning and enhancement prioritization

This collaborative model strengthens the overall platform and promotes shared innovation.

Direct Communication and Support

VAULT maintains direct communication channels between jurisdictions and the product and account management teams.

This includes:

- Dedicated account management support for ongoing communication and coordination
- Direct access to product teams for clarification, feedback, and issue resolution
- Timely responses to questions related to system updates and enhancements

This ensures that jurisdictions remain informed, supported, and engaged throughout the lifecycle of the platform.

Summary

VAULT ensures that jurisdictions are informed of and engaged in system improvements through a structured governance model, transparent communication practices, and ongoing collaboration.

By combining roadmap visibility, stakeholder engagement, and consistent communication, VAULT enables West Virginia to actively participate in platform evolution while maintaining awareness of all available enhancements.

4.2.2.1.1.4 EXAMPLES OF SHARED ENHANCEMENTS

VAULT meets this requirement by consistently delivering enhancements that originate from one or more jurisdictions and are evaluated, prioritized, and deployed across the broader customer base at no additional cost.

Enhancements are identified through a combination of jurisdiction-specific requests, cross-jurisdictional demand, and structured input from VAULT's user community. When similar needs are identified across multiple jurisdictions, these enhancements are elevated for broader consideration and incorporated into the shared platform roadmap.

User Group–Driven Enhancement Prioritization

VAULT maintains an active user group that meets at least quarterly and plays a central role in identifying, validating, and prioritizing system enhancements.

This includes:

- A dedicated forum within user group meetings for jurisdictions to propose enhancements and share emerging needs
- Discussion and validation of common requirements across multiple jurisdictions
- Prioritization of enhancements based on shared value, operational impact, and alignment with public health priorities

This structured, collaborative approach ensures that enhancements reflect real-world needs and are broadly applicable across the customer base.

Examples of Shared Enhancements

VAULT has successfully implemented numerous enhancements that originated in one or more jurisdictions and were subsequently deployed across all customers, including:

- **School-Based Clinic Workflow Enhancements**
  Introduction of check-in and check-out functionality for school-based clinics, improving tracking of student flow and operational visibility during clinic events
- **Streamlined Staff Management for Clinic Operations**
  Simplification of workflows for adding and managing staff within clinic rosters, improving efficiency in onboarding and scheduling clinic personnel
- **Enhanced Data Visualization for Billing and Reporting**
  Improvements to data visualization capabilities for customers using billing modules, enabling better insight into performance, revenue, and service delivery

- **Expanded Interoperability through IISConnex**
  Development of multi-state data exchange capabilities, enabling seamless interoperability across jurisdictions
- **Enhanced Reporting and Analytics Frameworks**
  Expanded reporting capabilities to support more flexible coverage, compliance, and operational analysis
- **Updates to Clinical Decision Support**
  Enhancements aligned with evolving CDC guidance to ensure accurate and up-to-date clinical recommendations

Continuous, Collaborative Delivery Model

In Maryland and other jurisdictions, VAULT's collaborative development model—supported by regular stakeholder engagement, user group input, and ongoing feedback loops—has enabled a continuous stream of enhancements aligned with real-world program needs.

This approach ensures that improvements are not isolated to a single jurisdiction but are shared across the platform, delivering ongoing value to all users.

4.2.2.1.2 HL7 ERROR AND HOLD QUEUE MANAGEMENT

VAULT meets this requirement by providing a comprehensive HL7 message management framework that delivers real-time validation, explicit ACK/NACK handling, configurable error and hold queue logic, and complete end-to-end message lifecycle management. This approach ensures that invalid or incomplete messages are immediately identified, appropriately routed, and efficiently resolved without compromising data integrity or system performance.

HL7 Message Processing Lifecycle and Validation

VAULT processes inbound and outbound HL7 messages through a structured, real-time pipeline that ensures immediate validation and response.

The message lifecycle includes:

1. Message receipt and ingestion
2. Validation against CDC HL7 v2.5.1 standards and jurisdiction-specific rules
3. Generation of HL7 acknowledgment (ACK/NACK)
4. Routing to processing, error, or hold queues
5. Resolution and resubmission as needed

Validation is performed automatically upon receipt and includes:

- Structural and format validation (segment structure, required fields)
- Code set validation (CVX, MVX, NDC where applicable)
- Business rule validation aligned with WV and CDC requirements

Messages that pass validation receive an AA (Application Accept) acknowledgment and proceed to processing. Messages that fail validation receive an AE (Application Error) or AR (Application Reject) response, depending on severity, and are routed to the appropriate queue.

Error and Hold Queue Management

VAULT distinguishes between error and hold conditions using configurable validation rules:

- **Error Queue:**

  Messages that fail critical validation (e.g., missing required fields, invalid codes) are rejected and placed in the error queue for correction.
- **Hold Queue:**

  Messages that cannot be fully processed due to temporary or dependent conditions (e.g., missing patient match, pending reference data) are placed in a hold queue for deferred processing.

Both queues provide:

- Centralized visibility into message status
- Filtering by provider, message type, error category, and date
- Prioritization capabilities to support operational workflows
- Configurable rules for queue routing and handling

Messages in the hold queue may be automatically reprocessed when conditions are resolved or manually released by authorized users.

ACK/NACK Handling and Trading Partner Feedback

VAULT generates HL7 acknowledgments in real time to ensure timely feedback to submitting systems.

This includes:

- Immediate ACK/NACK responses upon message validation
- Clear indication of acceptance, error, or rejection status (AA, AE, AR)
- Inclusion of detailed error descriptions tied to specific segments and fields

To support trading partners:

- Error details are made available through interface reporting and logs
- Configurable notifications (e.g., alerts, reports) can be provided to submitting organizations
- Interface support teams can use system-generated diagnostics to assist providers in resolving issues

This approach ensures rapid identification and correction of data quality issues at the source.

Correction, Reprocessing, and Resubmission Workflows

VAULT provides controlled workflows for resolving message errors and ensuring successful reprocessing.

This includes:

- Tools for reviewing and correcting message data within the system where appropriate
- Support for coordination with source systems when upstream correction is required
- Controlled resubmission of corrected messages with full audit tracking

The system maintains a complete audit trail of:

- Original message submission
- Validation errors
- Corrections applied
- Resubmission attempts and outcomes

Messages may be reprocessed individually or in bulk, supporting efficient resolution of high-volume issues.

Monitoring, Performance, and Operational Visibility

VAULT provides real-time monitoring and reporting tools to support operational oversight and continuous improvement.

Capabilities include:

- Dashboards displaying message volume, processing status, and error rates
- Identification of recurring validation issues to support upstream data quality improvements
- Monitoring of queue backlogs and processing times
- Alerts for thresholds or delays in message processing

The system is designed to support high-volume, real-time message processing without degradation of performance.

User Access and Usability

VAULT provides role-based access to HL7 message management tools, ensuring that both technical and operational users can effectively manage message workflows.

This includes:

- Intuitive interfaces for reviewing and resolving message errors
- Advanced filtering, sorting, and search capabilities
- Clear, actionable error messaging linked to validation rules

Role-based permissions ensure that users have appropriate access to view, correct, and resubmit messages while maintaining data security and governance.

Outcome for West Virginia

This approach provides West Virginia with:

- Immediate identification and rejection of invalid messages
- Clear separation and management of error and hold conditions
- Efficient resolution workflows that reduce provider burden
- Real-time visibility into message processing and data quality
- Scalable, high-performance HL7 message handling aligned with CDC standards

4.2.2.1.3 CODE SET SYNCHRONIZATION (CVX, MVX, NDC)

VAULT meets this requirement by providing automated, standards-based processes for maintaining and synchronizing vaccine-related code sets, including CVX, MVX, and NDC tables, ensuring continuous alignment with national standards and authoritative sources.

Automated Code Set Updates

VAULT supports automated ingestion and synchronization of code sets to reflect updates published by authoritative sources such as the CDC.

This includes:

- Regular automated updates to CVX, MVX, and NDC code sets
- Scheduled or event-driven synchronization processes
- Centralized management of code sets across the platform

These capabilities ensure that the system remains current with evolving standards without requiring manual intervention.

Validation and Data Integrity

VAULT integrates code set validation directly into system workflows to ensure data accuracy and consistency.

This includes:

- Validation of incoming and existing data against current code sets
- Enforcement of code usage within clinical workflows, data entry, and HL7 messaging
- Identification of invalid or deprecated codes during data processing

This approach reduces the risk of data inconsistencies and supports high-quality data exchange.

Version Control and Traceability

VAULT maintains version control and historical tracking of code set updates to support auditability and transparency.

This includes:

- Tracking of code set versions and effective dates
- Historical reference to prior code values for reporting and auditing purposes
- Controlled deployment of updates to ensure traceability of changes

These capabilities support compliance and enable accurate historical analysis.

Seamless Integration with System Workflows

Updated code sets are fully integrated into platform functionality and available immediately for use.

This includes:

- Integration with clinical decision support, validation rules, and reporting
- Alignment with HL7 messaging and interoperability requirements
- Immediate availability of updated codes for providers and administrators

This ensures that code updates are not isolated but actively support system operations.

Minimal Disruption and Controlled Deployment

VAULT ensures that code set updates are deployed with minimal impact to ongoing operations.

This includes:

- Controlled update processes that do not interrupt system availability
- Pre-deployment validation to ensure compatibility with existing workflows
- Seamless transition to updated code sets without requiring user intervention

Configurable Support for Jurisdiction-Specific Needs

VAULT provides configuration options to accommodate jurisdiction-specific requirements related to code usage and validation.

This allows jurisdictions to:

- Apply specific validation rules or constraints
- Manage local variations while maintaining alignment with national standards

Summary

VAULT ensures that CVX, MVX, and NDC code sets are maintained accurately, updated automatically, and fully integrated into system workflows.

By combining automated synchronization, validation, version control, and seamless deployment, VAULT enables West Virginia to maintain compliance, support accurate data exchange, and reduce administrative overhead.

4.2.2.1.4 BULK MANAGEMENT OF PROVIDERS, FACILITIES, AND USERS

VAULT meets this requirement by providing scalable, flexible tools for bulk loading, activation, and deactivation of providers, facilities, and users, enabling efficient management of large and dynamic populations across the system.

Bulk Data Upload and Management

VAULT supports efficient onboarding and updates through bulk data processing capabilities. This includes:

- Spreadsheet-based (e.g., CSV) bulk upload of providers, facilities, and users
- Bulk updates to existing records, including demographic, organizational, and role-based data
- Pre-processing validation to identify and resolve data issues prior to import
- Batch processing to support large-scale administrative operations

These capabilities enable rapid onboarding and system updates with minimal manual effort.

Bulk Activation and Deactivation Workflows

VAULT provides controlled workflows for activating and deactivating users, providers, and facilities at scale.

This includes:

- Bulk activation and deactivation of users and organizations
- Ability to apply role assignments and permission updates in bulk
- Effective date management to support scheduled activation or deactivation

These tools ensure that system access and participation can be managed efficiently and securely.

Automated Lifecycle Management

VAULT supports automated lifecycle controls to manage inactive users and maintain system integrity.

This includes:

- Configurable rules that allow administrators to define inactivity thresholds
- Automatic deactivation of users after a defined period of inactivity
- Bulk deactivation capabilities to manage large groups of inactive users

This reduces administrative burden while ensuring that system access remains current and appropriate.

Data Integrity and Validation

VAULT ensures that bulk operations maintain accuracy and consistency across the system.

This includes:

- Validation of uploaded data prior to processing
- Error identification and reporting for correction before import
- Audit logging of bulk operations for traceability and compliance

Integration and Synchronization

VAULT supports integration with external systems to enable automated synchronization of provider, facility, and user data where applicable.

This includes:

- API-based integration with external systems
- Automated updates to maintain alignment across systems
- Reduction of duplicate data entry and administrative overhead

Scalability for Routine and Emergency Operations

These capabilities support both routine system administration and large-scale operational events.

This includes:

- Rapid onboarding of providers and users during emergency response scenarios
- Efficient management of changing participation across jurisdictions and programs
- Support for large-scale administrative updates without system disruption

Summary

VAULT enables West Virginia to efficiently manage providers, facilities, and users through scalable bulk processing, automated lifecycle management, and robust validation controls. By combining flexibility, automation, and auditability, VAULT ensures accurate, secure, and efficient administration of system participants across both routine operations and emergency scenarios.

4.2.2.2 IMPLEMENTATION PLAN

VAULT's implementation approach provides West Virginia with a structured, transparent, and low-risk path to deploying the new IIS, ensuring continuity of operations, high data integrity, and successful system adoption.

The approach is grounded in a phased implementation methodology supported by strong governance, defined roles and responsibilities, and continuous collaboration with Agency stakeholders. Each phase includes validation checkpoints, including User Acceptance Testing (UAT), to ensure readiness prior to progression.

VAULT's data migration strategy ensures accurate and complete transition of all system components—including patient and immunization data, providers and organizations, user accounts and roles, program participation data, and HL7 interfaces—through phased migration, iterative validation, and parallel system operation to prevent disruption.

A structured change management process ensures that all changes are evaluated, approved, and implemented in a controlled manner, while proactive risk mitigation strategies—including parallel operations, incremental validation, and defined contingency plans—minimize implementation risk and ensure continuity.

Comprehensive training, knowledge transfer, and ongoing support ensure that users are fully prepared to adopt and operate the system, enabling long-term sustainability and independence.

This implementation approach is tailored to West Virginia's existing IIS environment and provider landscape, ensuring a seamless transition with minimal disruption to ongoing public health operations and data exchange workflows.

Key Outcomes of VAULT's Implementation Approach

- Controlled, phased implementation with defined milestones and validation checkpoints
- No disruption to operations through parallel system and interface operation
- High data integrity ensured through rigorous migration, validation, and reconciliation
- Transparent governance and change management with Agency involvement

- Proactive risk mitigation and contingency planning
- Rapid user readiness and long-term operational independence

What Sets Us Apart

VAULT distinguishes itself by delivering implementation and migration as a controlled, validated, and low-risk process—ensuring continuity of operations, data integrity, and successful system adoption from day one.

Key differentiators include:

No-Downtime, Parallel Operations Model

VAULT enables the State to operate the legacy IIS and the new platform concurrently during migration, ensuring uninterrupted access to immunization records, reporting, and data exchange. This approach significantly reduces risk and allows for real-time validation prior to final cutover.

Phased Migration with Data Quality Sprints

VAULT employs an iterative migration approach using defined data quality sprints, enabling early identification and resolution of data issues. This structured, incremental model provides continuous validation and minimizes the risks associated with large-scale, one-time data migrations.

Comprehensive, End-to-End Migration Scope

VAULT migrates all system components—not just core data—including patient and immunization records, providers and organizations, user accounts and roles, program participation data, and HL7 interfaces. This ensures full continuity of operations and eliminates gaps in system functionality.

Rigorous Validation, Reconciliation, and UAT

VAULT applies multiple layers of validation, including reconciliation of source and target systems and User Acceptance Testing (UAT) with State stakeholders. This ensures that all data, relationships, and workflows are fully verified prior to go-live.

Parallel Interface Migration and Validation

All HL7 interfaces are migrated and operated in parallel during transition, with comprehensive end-to-end testing to ensure uninterrupted interoperability with external systems and partners.

Structured Governance and Change Control

VAULT implements a formal governance model that includes defined roles and responsibilities, transparent change management processes, and active stakeholder engagement. This ensures that all decisions are controlled, documented, and aligned with State priorities.

Proactive Risk Mitigation and Contingency Planning

VAULT anticipates and manages risks through early data analysis, incremental validation, continuous monitoring, and defined rollback procedures. This ensures that potential issues are addressed before they impact operations.

Comprehensive Training and Knowledge Transfer

VAULT delivers role-based training, hands-on workshops, on-demand learning resources, and in-system guidance to ensure rapid user readiness and long-term operational independence for the State.

4.2.2.2.1 PROJECT MANAGEMENT STRATEGY AND TIMELINE

VAULT meets this requirement by applying a structured, hybrid Agile and governance-driven implementation methodology that ensures flexibility, transparency, and controlled delivery throughout the project lifecycle.

For West Virginia, this methodology is specifically designed to support a seamless transition from the existing IIS, ensuring continuity of HL7 data exchange, preservation of historical data (approximately 31 million vaccination records), and minimal disruption to providers and OEPS operations.

This approach combines iterative development with formal oversight, enabling the State to maintain visibility, validate progress, and minimize risk at each stage of implementation.

Project Governance and Management Approach

VAULT establishes a clear governance structure to support coordination, accountability, and decision-making throughout the implementation.

Key components include:

- Dedicated Project Manager and Product Manager responsible for delivery, coordination, and stakeholder alignment
- Weekly status meetings with West Virginia OEPS to review progress, risks, and upcoming activities
- Sprint-based delivery cycles to support iterative configuration and enhancement
- Formal milestone reviews and approvals to validate readiness before advancing to subsequent phases
- Transparent issue and risk tracking using Jira or Agency-approved tools

VAULT will collaborate closely with OEPS through recurring working sessions, similar to the model successfully implemented with the Maryland Department of Health, where continuous alignment between program leadership and technical teams supported efficient delivery and rapid issue resolution.

Phased Implementation Approach

VAULT follows a phased implementation model that ensures structured progression, validation at each stage, and readiness prior to production deployment.

Phase	Milestone	Description	Estimated Timeline
Phase 1	Project Initiation & Planning	Kickoff, stakeholder alignment, requirements validation, and project plan finalization	Weeks 1–4
Phase 2	Environment Setup	Provisioning of Development, Test, and Production environments; security configuration	Weeks 3–6

Phase	Milestone	Description	Estimated Timeline
Phase 3	System Configuration	Configuration of workflows, user roles, reporting, and jurisdiction-specific requirements	Weeks 5–12
Phase 4	Data Migration (Initial Loads)	Data extraction, transformation, and initial migration into test environment. Data migration includes comprehensive validation processes to ensure accuracy, completeness, and integrity of all migrated records. This includes record-level validation, reconciliation of patient and vaccination counts, and comparison against source system benchmarks to confirm successful migration.	Weeks 8–16
Phase 5	Interface Development & Testing	HL7 interfaces, FHIR endpoints, IIS integrations, and external system connections. During interface development and testing, VAULT ensures continuity of HL7 data exchange by validating message formats, maintaining existing provider connections, and coordinating with partners to prevent disruption to ongoing data submissions.	Weeks 10–18
Phase 6	User Acceptance Testing (UAT)	Agency-led validation of functionality, workflows, and data accuracy	Weeks 16–20
Phase 7	Training & Knowledge Transfer	End-user training, administrator training, and documentation delivery	Weeks 18–22
Phase 8	Go-Live Preparation	Final data migration, cutover planning, and readiness validation. VAULT employs a controlled cutover strategy	Weeks 20–24

Phase	Milestone	Description	Estimated Timeline
		that may include parallel processing, final data validation, and rollback contingency planning to ensure uninterrupted system availability and data integrity during transition.	
Phase 9	Go-Live & Stabilization	Production launch and stabilization period with enhanced support	Weeks 24–28

Risk Mitigation and Controlled Progression

VAULT's implementation methodology is designed to minimize risk and ensure successful transition through:

- Validation checkpoints at each phase, including milestone approvals and UAT
- Parallel testing and staged migration to identify and resolve issues prior to go-live
- Controlled cutover planning to ensure continuity of operations
- Dedicated stabilization support following go-live to address any issues quickly

This approach ensures that the State can transition to the new IIS in a controlled, predictable, and low-risk manner.

Implementation activities are structured to minimize disruption to providers, ensuring continued access to the system for data submission, query, and reporting throughout the transition.

Summary

VAULT's implementation approach combines structured governance, phased delivery, and rigorous validation to ensure a seamless transition for West Virginia. By addressing key risks such as data migration integrity, HL7 interface continuity, and provider impact, VAULT minimizes disruption while ensuring system readiness.

This approach enables OEPS to maintain uninterrupted operations, preserve data accuracy, and confidently transition to a modern IIS that supports both current needs and future growth.

4.2.2.2.2 ENVIRONMENT SETUP

VAULT meets this requirement by providing fully managed, secure, and scalable environments for Development (Dev), Testing/User Acceptance Testing (Test/UAT), and Production (Prod), ensuring a controlled and reliable implementation and operational framework.

All environments are provisioned within VAULT's cloud-based infrastructure and configured to meet security, performance, and compliance requirements.

Environment Segmentation and Isolation

VAULT maintains strict separation between Development, Test/UAT, and Production environments to ensure stability and minimize risk.

This includes:

- Isolated environments that prevent testing or development activities from impacting production operations
- Dedicated Test/UAT environments that support validation of system configuration, workflows, and data prior to deployment
- Controlled promotion of code and configuration changes between environments

This approach ensures that all changes are thoroughly tested before being introduced into production.

Security and Access Control

VAULT implements strong security controls across all environments to protect system integrity and data.

This includes:

- Role-based access controls to manage user permissions by environment
- Secure authentication and authorization mechanisms
- Environment-specific access restrictions to limit exposure of sensitive data

These controls ensure that access is appropriately managed and aligned with security best practices.

Continuous Integration and Deployment

VAULT utilizes continuous integration and deployment (CI/CD) pipelines to support efficient and controlled system updates.

This includes:

- Automated build and deployment processes across environments
- Controlled promotion of validated changes from Dev to Test/UAT to Production
- Integration with testing and validation workflows to ensure quality and consistency

This approach enables rapid delivery of enhancements while maintaining system stability.

Scalability and Performance

VAULT's cloud infrastructure supports scalable performance across all environments.

This includes:

- Elastic scaling to accommodate varying workloads during development, testing, and production operations
- Performance monitoring to ensure system responsiveness
- Infrastructure designed to support both routine operations and high-demand scenarios

Support for Implementation and Ongoing Operations

The environment structure is designed to support both initial implementation and ongoing system evolution.

This includes:

- Dedicated Test/UAT environments for validating configuration, data migration, and interfaces during implementation
- Support for regression testing and future enhancements
- Stable Production environment to ensure uninterrupted system operations

Summary

VAULT provides secure, isolated, and scalable environments that support all phases of implementation and ongoing system operations.

By combining strong security controls, environment separation, and controlled deployment processes, VAULT ensures that West Virginia can implement and operate the IIS in a stable, secure, and low-risk environment.

4.2.2.2.3 SYSTEM CONFIGURATION AND WORKFLOW CUSTOMIZATION

VAULT meets this requirement by providing a highly configurable platform that can be tailored to align with West Virginia's specific workflows, policies, and program requirements without the need for custom code development.

The PrepModEcosystem is designed to support jurisdiction-specific configuration through flexible, parameter-driven capabilities that enable adaptation while maintaining a standardized, maintainable system.

Configurable Workflows and Business Rules

VAULT supports configuration of workflows and business rules to reflect jurisdictional requirements.

This includes:

- Configuration of immunization workflows, including registration, administration, and reporting processes
- Implementation of jurisdiction-specific business rules and validation logic
- Configuration of exemption policies and associated workflows

- Support for program-specific requirements and operational variations

These capabilities ensure that the system aligns with State policies while maintaining consistency across the platform.

Role-Based Access and Permissions

VAULT provides configurable role-based access controls to support different user types and organizational structures.

This includes:

- Definition of user roles aligned with State and provider responsibilities
- Assignment of permissions based on role and function
- Flexibility to configure access across providers, facilities, and administrative users

This ensures appropriate access control while supporting efficient system use.

Reporting and Analytics Configuration

VAULT enables configuration of reporting and analytics to support jurisdiction-specific needs.

This includes:

- Customizable dashboards and reporting views
- Configuration of reports to support compliance, coverage, and operational monitoring
- Ability to tailor data outputs to meet State and federal reporting requirements

Collaborative Configuration Process

Configuration is performed in close collaboration with West Virginia OEPS to ensure alignment with operational needs and priorities.

This includes:

- Joint working sessions to define workflows, policies, and reporting requirements
- Iterative configuration and validation within Test/UAT environments
- Ongoing refinement based on stakeholder feedback during implementation

This approach ensures that system configuration is accurate, validated, and aligned with real-world operations.

Maintainable and Scalable Configuration Model

VAULT's configuration-driven approach enables flexibility without introducing long-term maintenance complexity.

This includes:

- Avoidance of one-off custom code that can create upgrade challenges
- Consistent application of configuration across environments
- Ability to adapt to future changes in policy or program requirements without system redesign

Summary

VAULT enables West Virginia to tailor the IIS to its specific workflows and policies through a flexible, configuration-driven approach.

By combining configurable workflows, role-based access, and collaborative implementation, VAULT ensures alignment with State requirements while maintaining a scalable, maintainable, and future-ready system.

4.2.2.2.4 DATA MIGRATION STRATEGY

VAULT employs a structured, phased, and low-risk data migration methodology designed to ensure data accuracy, continuity of operations, and full transparency throughout the transition from the State's existing IIS to the VAULT platform.

This approach is grounded in VAULT's experience supporting large-scale public health data migrations and is specifically designed to address the volume, complexity, and sensitivity of immunization data, including patient histories, provider relationships, and real-time data exchange requirements.

A core principle of VAULT's methodology is a parallel, no-downtime transition model, ensuring that the existing IIS remains fully operational while the new system is implemented, validated, and prepared for cutover.

Parallel Operations and Controlled Cutover

VAULT implements a parallel operations model in which the legacy IIS and the new platform operate concurrently during migration.

This enables:

- Continuous access to immunization records for all users
- Uninterrupted clinical workflows, reporting, and data exchange
- Ongoing synchronization and validation between systems

Cutover is executed only after:

- Data reconciliation thresholds are met
- User Acceptance Testing (UAT) is completed
- Formal State approval is obtained

Rollback procedures are maintained through cutover to ensure continuity in the event of critical issues.

Phased Migration and Iterative Data Quality Sprints

To reduce risk and improve data quality, VAULT executes migration in controlled phases supported by iterative data quality sprints.

Each sprint includes:

- Migration of defined data subsets (e.g., cohorts, providers, historical ranges)
- Data profiling, cleansing, normalization, and deduplication
- Validation against CDC HL7 Message Mapping Guides (MMGs) and State-specific rules
- Reconciliation of record counts and key data elements
- Stakeholder review and formal sign-off

This iterative approach:

- Identifies issues early
- Enables continuous refinement
- Avoids risk associated with single-event migrations

Comprehensive Data Scope and Validation Framework

VAULT's migration includes all critical system domains required for full operational continuity:

- Patient and immunization records
- Provider, facility, and organization data
- User accounts and role-based permissions
- Program participation and eligibility data
- HL7 interfaces and external integrations

Data integrity is ensured through:

- Deterministic and probabilistic deduplication
- Validation of relationships and hierarchies
- Field-level and record-level reconciliation
- UAT-driven validation with State stakeholders

Secure Migration Environment and Testing

All migration activities are conducted in secure, isolated environments with strict separation of development, test, staging, and production systems.

This includes:

- Multiple full migration dry runs

- Automated validation scripts and reconciliation checks
- End-to-end testing of workflows and integrations

Final Cutover and Data Certification

VAULT executes a controlled production migration and cutover aligned with State readiness.

This includes:

- Final data synchronization and reconciliation
- Go/no-go decision checkpoint with State stakeholders
- Transition of users, interfaces, and workflows

Post-migration:

- Temporary data is securely removed
- A Certificate of Data Destruction is provided
- Final migration and validation documentation is delivered

4.2.2.2.4.1 EXISTING IIS DATA MIGRATION

VAULT performs a structured, multi-phase migration of legacy IIS data to ensure accuracy, completeness, and traceability.

Data Extraction and Source Analysis

- Extraction of all relevant IIS data sources
- Identification of data structures, dependencies, and relationships
- Assessment of data quality and anomalies

Data Profiling and Cleansing

- Identification of duplicates, invalid values, and gaps
- Standardization and normalization of data
- Collaboration with the State to resolve issues prior to migration

Transformation and Mapping

- Mapping of source data to VAULT schema
- Application of transformation rules
- Alignment with CDC standards and system requirements

Iterative Migration and Validation

- Test migrations in UAT environment
- Record-level and field-level reconciliation
- Iterative refinement based on validation results

Auditability and Traceability

- Documentation of mappings and transformations
- Audit logs of migration activity
- Traceability of records from source to target

4.2.2.2.4.2 USER AND ROLES MIGRATION

VAULT ensures accurate and secure migration of users and role-based access controls.

- Migration of user identities, affiliations, and attributes
- Mapping of legacy roles to VAULT RBAC framework
- Normalization of permissions to align with current policies

Validation includes:

- Verification of access across user types
- Testing in UAT environment
- Controlled activation at go-live

All role assignments are auditable and aligned with security best practices.

4.2.2.2.4.3 PROVIDER, FACILITY, AND ORGANIZATION MIGRATION

VAULT ensures accurate migration of provider, facility, and organizational structures through validation, reconciliation, and hierarchy preservation.

This includes:

- Migration of all entities and relationships
- Validation of provider-to-organization linkages
- Deduplication and normalization of records

Reconciliation includes:

- Record count validation across entities
- Field-level validation of critical attributes
- Resolution of discrepancies prior to go-live

State stakeholders validate data during UAT to confirm accuracy and usability.

4.2.2.2.4.4 PROGRAM ENROLLMENT MIGRATION

VAULT migrates all program participation and eligibility data while aligning with current system configuration.

This includes:

- Migration of provider program participation (e.g., VFC)
- Migration of patient eligibility and enrollment records
- Preservation of historical program data

Data is:

- Mapped to VAULT's configurable program framework
- Validated against current program rules
- Reviewed with State stakeholders

This ensures continuity of program tracking, compliance, and reporting.

4.2.2.2.4.5 INTERFACE MIGRATION AND TESTING

VAULT ensures continuity of data exchange through structured migration and validation of all HL7 interfaces.

Interface Migration

- Migration of all inbound and outbound interfaces (VXU, QBP, ACK)
- Alignment with VAULT integration framework
- Mapping of interface specifications

Testing and Validation

- Validation against CDC HL7 standards
- End-to-end testing with EHRs, HIEs, and partner systems
- Verification of ACK/NACK handling and workflows

Parallel Operation

- Concurrent operation of legacy and new interfaces

- Monitoring of message consistency
- Resolution of discrepancies prior to cutover

Post-Go-Live Stabilization

- Monitoring of message flow and error rates
- Rapid issue resolution
- Ongoing validation of performance

Summary

VAULT's data migration strategy provides West Virginia with a controlled, transparent, and low-risk transition that:

- Ensures no disruption to operations through parallel execution
- Maintains high data quality through iterative validation and reconciliation
- Supports full auditability and traceability
- Preserves interoperability and program continuity
- Enables a confident, validated cutover to the new IIS

4.2.2.2.5 CHANGE REQUEST MANAGEMENT

VAULT meets this requirement by implementing a structured, transparent change request management process that ensures all changes are documented, evaluated, approved, and executed in a controlled and predictable manner.

Formal Change Request Submission and Tracking

VAULT utilizes a standardized process for submitting and tracking change requests throughout the implementation lifecycle.

This includes:

- Formal submission of change requests through a centralized tracking system (e.g., Jira or Agency-approved tools)
- Unique identification and tracking of each request
- Full visibility into request status, ownership, and progress

This ensures that all changes are captured and managed consistently.

Impact Analysis and Prioritization

All change requests undergo structured evaluation prior to approval.

This includes:

- Assessment of impact on scope, timeline, cost, and system performance
- Evaluation of dependencies and potential risks
- Prioritization based on business value, urgency, and alignment with project goals

This process ensures that changes are well understood and aligned with project priorities.

Approval and Governance

VAULT works collaboratively with West Virginia OEPS to ensure that all changes are reviewed and approved before implementation.

This includes:

- Defined approval workflows involving Agency stakeholders
- Joint decision-making on change acceptance, prioritization, and timing
- Documentation of approvals and associated decisions

This ensures that the State maintains full control over project changes.

Integration with Agile Delivery

Approved changes are incorporated into VAULT's Agile delivery process in a controlled manner.

This includes:

- Integration of approved changes into sprint planning and backlog prioritization
- Iterative development and testing of changes
- Validation of changes in Test/UAT environments prior to release

This ensures that changes are implemented efficiently while maintaining system stability.

Communication and Transparency

VAULT maintains clear communication regarding all change requests.

This includes:

- Regular updates during status meetings
- Visibility into upcoming changes and release schedules
- Documentation of changes included in each release

This approach ensures that all stakeholders remain informed and aligned.

Summary

VAULT ensures that all change requests are managed through a structured, transparent, and collaborative process.

By combining formal tracking, impact analysis, stakeholder approval, and controlled implementation, VAULT enables West Virginia to manage changes effectively while maintaining project stability, alignment, and predictability.

4.2.2.2.6 ROLES AND RESPONSIBILITIES

VAULT meets this requirement by establishing a clearly defined governance and accountability model that delineates roles and responsibilities between VAULT and West Virginia OEPS, ensuring effective coordination, transparency, and successful project execution.

VAULT Responsibilities

VAULT is responsible for overall project delivery, technical implementation, and system readiness.

This includes:

- Project management, including planning, coordination, and status reporting
- System configuration, deployment, and environment management
- Data migration, validation, and reconciliation activities
- Interface development, testing, and integration
- Delivery of training, documentation, and user support

- Ongoing issue tracking, risk management, and resolution

VAULT ensures that all technical and operational aspects of the implementation are delivered in alignment with project timelines and quality standards.

Agency Responsibilities (West Virginia OEPS)

The Agency plays a critical role in providing input, validation, and oversight throughout the implementation process.

This includes:

- Validation of requirements, workflows, and business rules
- Participation in User Acceptance Testing (UAT) and system validation
- Review and approval of deliverables, milestones, and configuration decisions
- Data validation and formal sign-off for migration activities
- Coordination with internal stakeholders and external partners

This collaborative involvement ensures that the system aligns with State policies and operational needs.

Shared Responsibilities and Collaboration

VAULT and OEPS work collaboratively to ensure alignment, timely decision-making, and successful delivery.

This includes:

- Participation in regular status meetings and working sessions
- Joint review of risks, issues, and mitigation strategies
- Coordination of testing, training, and go-live readiness activities
- Alignment on priorities, timelines, and change management decisions

This shared responsibility model ensures continuous communication and coordinated execution.

Governance and Oversight Framework

VAULT establishes a governance framework that supports accountability and transparency throughout the project lifecycle.

This includes:

- Regular status reporting and milestone tracking
- Structured risk management and issue tracking processes
- Defined escalation paths for resolving issues or decisions
- Ongoing stakeholder communication and engagement

This framework ensures that all parties remain informed, aligned, and accountable throughout the implementation.

Summary

VAULT's clearly defined roles and responsibilities model ensures that all aspects of the implementation are owned, coordinated, and executed effectively.

By combining defined accountability, collaborative engagement, and structured governance, VAULT enables West Virginia to implement the IIS with clarity, confidence, and minimal risk.

4.2.2.2.7 RISK MITIGATION AND CONTINGENCY PLANNING

VAULT meets this requirement by implementing a proactive, structured approach to risk identification, mitigation, and contingency planning, ensuring that potential issues are anticipated, managed, and resolved without impacting project success.

Proactive Risk Identification and Management

VAULT identifies and tracks risks throughout the implementation lifecycle using formal risk management processes.

This includes:

- Early identification of risks during project planning and requirements validation
- Continuous risk monitoring through regular status meetings and project tracking tools
- Maintenance of a centralized risk and issue log with defined ownership and mitigation strategies

This ensures that risks are visible, tracked, and addressed in a timely manner.

Data Migration Risk Mitigation

VAULT applies specific strategies to reduce risk during data migration activities.

This includes:

- Early data profiling and validation to identify data quality issues
- Incremental migration and iterative testing cycles
- Multiple validation and reconciliation steps prior to go-live

These practices reduce the likelihood of data loss, corruption, or inconsistency.

Operational Continuity and Parallel Operations

VAULT ensures continuity of operations during implementation through controlled transition strategies.

This includes:

- Parallel operation of legacy and new systems during migration
- Parallel interface operation to maintain uninterrupted data exchange
- Ongoing monitoring to ensure consistency across systems

This approach minimizes disruption and provides additional validation prior to cutover.

Contingency Planning and Rollback Procedures

VAULT establishes contingency plans to address potential issues during implementation and go-live.

This includes:

- Defined rollback procedures to revert to the legacy system if necessary
- Backup and recovery strategies to protect data integrity
- Predefined escalation paths for rapid issue resolution

These capabilities ensure that the State is protected against unexpected events.

Continuous Monitoring and Issue Resolution

VAULT maintains active monitoring and rapid response capabilities throughout implementation and stabilization.

This includes:

- Real-time monitoring of system performance, data processing, and interfaces
- Centralized issue tracking and resolution workflows

- Dedicated support during go-live and stabilization periods

This ensures that any issues are identified and resolved quickly.

Summary

VAULT's risk mitigation and contingency planning approach ensures that potential risks are proactively identified, managed, and resolved throughout implementation.

By combining structured risk management, phased validation, parallel operations, and defined contingency procedures, VAULT enables West Virginia to implement the new IIS with minimal risk and full confidence in system stability and continuity.

4.2.2.2.8 TRAINING, SUPPORT, AND KNOWLEDGE TRANSFER

VAULT meets this requirement by providing a comprehensive, role-based training and knowledge transfer program designed to ensure rapid user readiness, effective system adoption, and long-term operational independence for West Virginia OEPS.

Role-Based Training Approach

VAULT delivers targeted training aligned with user roles and responsibilities.

This includes:

- Role-based training for providers, clinic staff, administrators, and public health personnel
- Tailored training for system administrators and technical users
- Focus on real-world workflows, including registration, vaccination, reporting, and system administration

This ensures that each user group receives relevant, practical training aligned with their responsibilities.

Training Delivery Methods

VAULT utilizes multiple training formats to support diverse learning needs and schedules.

This includes:

- Live, instructor-led training sessions

- Hands-on workshops and scenario-based exercises
- Recorded training sessions available on demand
- Self-paced training materials and documentation

This flexible approach enables users to learn effectively and revisit materials as needed.

Documentation and In-System Guidance

VAULT provides comprehensive training materials and embedded system guidance.

This includes:

- User guides, administrative documentation, and quick-reference materials
- Release notes and feature updates
- In-application guidance and prompts to support users during live operations

This ensures that users have ongoing access to support resources beyond formal training sessions.

Knowledge Transfer and Operational Readiness

VAULT emphasizes knowledge transfer to ensure that the State can independently operate and manage the system.

This includes:

- Training of Agency administrators to manage configuration, reporting, and user management
- Knowledge transfer sessions for technical and operational staff
- Support for transition from implementation to steady-state operations

This ensures long-term sustainability and reduces reliance on vendor support.

Ongoing Support During and After Implementation

VAULT provides continuous support throughout implementation and post-go-live stabilization.

This includes:

- Dedicated support during User Acceptance Testing (UAT) and go-live
- Rapid response to user questions and issues
- Ongoing support channels for troubleshooting and guidance

This ensures that users are supported during critical phases of adoption.

Summary

VAULT's training and knowledge transfer approach ensures that West Virginia is fully prepared to adopt, operate, and sustain the IIS solution.

By combining role-based training, flexible delivery methods, comprehensive documentation, and ongoing support, VAULT enables rapid user readiness, confident system adoption, and long-term operational independence.

4.2.2.3 VACCINE EXEMPTION FUNCTIONALITY

VAULT Technologies provides a comprehensive, highly configurable, and policy-driven approach to vaccine exemption management within the PrepModEcosystem and OptimIIS platform. The system is designed to support jurisdiction-specific policies while ensuring accurate tracking, reporting, and compliance with school-entry requirements and public health mandates.

VAULT supports granular exemption tracking by vaccine, disease, and immunization series, along with flexible classification of exemption types and reasons. Exemption data is fully integrated with patient demographics, school roster functionality, and immunization records, enabling comprehensive analysis across schools, grades, districts, and population groups.

The platform provides robust reporting and longitudinal tracking capabilities, allowing the State to monitor exemption trends, compliance status, and immunization coverage over time.

Configurable workflows and role-based review processes enable jurisdictions to independently manage exemption submission, review, and approval processes, ensuring alignment with evolving policies without requiring custom development.

What Sets VAULT Apart

VAULT distinguishes itself by delivering a highly configurable, policy-driven exemption management framework that goes beyond basic tracking to support compliance, reporting, and evolving jurisdictional needs—without requiring custom development or vendor dependency.

Independent, Configuration-Driven Policy Control

VAULT enables jurisdictions to configure exemption types, reasons, workflows, and review processes independently. This allows West Virginia to adapt to changing policies, legislative updates, and operational needs without relying on vendor intervention, reducing long-term costs and increasing agility.

Granular and Flexible Exemption Management

VAULT supports exemption tracking at the vaccine, disease, and series level, along with multiple exemption types and reasons. This level of granularity ensures precise alignment with clinical guidelines, school-entry requirements, and jurisdictional policies.

Seamless Integration with School Workflows

VAULT integrates exemption data directly with school roster functionality, enabling real-time visibility into compliance at the student, school, and district levels. This supports efficient school-entry compliance monitoring and coordinated public health action.

Longitudinal Tracking and Population Insights

VAULT provides longitudinal tracking of exemption and immunization status, allowing the State to monitor trends over time as students progress through grades and across school systems. This supports both operational oversight and long-term public health planning.

Comprehensive Reporting and Analytics

VAULT delivers multi-dimensional reporting across schools, grades, districts, exemption types, and compliance status. By integrating exemption data with immunization coverage and demographic information, the system enables identification of trends, disparities, and areas of risk.

Policy-Aligned Workflows with Built-In Accountability

VAULT supports configurable, role-based workflows for exemption submission, review, and approval, with full auditability and lifecycle tracking. This ensures transparency, consistency, and alignment with jurisdictional policies and compliance requirements.

4.2.2.3.1 ABILITY TO RECORD EXEMPTIONS BY VACCINE OR DISEASE CATEGORY

VAULT meets this requirement by supporting the recording of vaccine exemptions at a highly granular level, including by individual vaccine, disease category, or immunization series. This flexibility enables West Virginia to align exemption tracking with jurisdictional policies, school-entry requirements, and clinical guidelines.

Granular Exemption Tracking

VAULT allows exemptions to be recorded at multiple levels, including:

- Individual vaccines (e.g., MMR, DTaP)
- Disease categories (e.g., measles, pertussis)
- Immunization series or grouped vaccine requirements

The system supports multiple exemptions per patient, ensuring that all applicable exemptions are accurately captured and managed.

Integration with the Patient Immunization Record

Exemption records are fully integrated into the patient's immunization record. This includes:

- Display of exemption status alongside administered doses and vaccination history
- Visibility of exemptions within clinical workflows and decision-making tools
- Inclusion of exemption data in compliance and coverage evaluations

This ensures that providers and public health users have a complete and accurate view of each patient's immunization and exemption status.

Configurable to Jurisdictional Requirements

VAULT's exemption framework is configurable to reflect State-specific policies. This includes:

- Ability to define which vaccines or disease categories are eligible for exemption
- Alignment with jurisdictional immunization schedules and requirements
- Flexibility to adapt to changes in policy without system redesign

Summary

VAULT enables West Virginia to record and manage exemptions at the vaccine, disease, and series level through a flexible, configurable framework.

By integrating exemption data directly into the patient record and supporting multiple exemption scenarios, VAULT ensures accurate tracking, informed decision-making, and alignment with State policies and clinical requirements.

4.2.2.3.2 SUPPORT FOR EXEMPTION TYPES: PERMANENT, TEMPORARY, AND PROVISIONAL

VAULT meets this requirement by supporting multiple exemption types, including permanent, temporary, and provisional classifications, with configurable attributes to manage each type throughout its lifecycle.

Support for Multiple Exemption Types

VAULT enables jurisdictions to define and manage exemption types, including:

- Permanent exemptions, which remain in effect without expiration
- Temporary exemptions, which include defined expiration dates
- Provisional exemptions, which include review or follow-up dates

This flexibility allows the State to align exemption tracking with policy requirements and public health guidelines.

Lifecycle Management and Monitoring

VAULT provides built-in capabilities to manage exemptions over time and ensure timely follow-up.

This includes:

- Tracking of expiration dates for temporary exemptions
- Tracking of review dates for provisional exemptions
- Automated identification of expiring or overdue exemptions
- Support for updating exemption status based on follow-up actions

These capabilities ensure that exemption records remain current and actionable.

Compliance and Operational Support

VAULT integrates exemption type management into compliance workflows.

This includes:

- Inclusion of exemption status in compliance and school-entry evaluations
- Visibility of active, expired, and pending exemptions within user workflows
- Support for monitoring and reporting on exemption status over time

This ensures that jurisdictions can maintain accurate records and enforce policies effectively.

Summary

VAULT supports permanent, temporary, and provisional exemption types through a flexible, configurable framework that enables full lifecycle management.

By incorporating expiration tracking, review workflows, and compliance integration, VAULT ensures that exemption records remain accurate, up to date, and aligned with jurisdictional requirements

4.2.2.3.3 SUPPORT FOR EXEMPTION REASONS: MEDICAL, RELIGIOUS, PHILOSOPHICAL

VAULT meets this requirement by supporting structured categorization of exemption reasons, including medical, religious, and philosophical classifications, with configurable options to align with jurisdictional policies.

Standardized Exemption Reason Classification

VAULT enables consistent capture and classification of exemption reasons across all providers and organizations.

This includes:

- Support for standard exemption categories, including medical, religious, and philosophical
- Structured data capture to ensure consistency and reduce variation in how exemptions are recorded
- Alignment of exemption reasons with jurisdictional reporting and compliance requirements

This ensures that exemption data is reliable and comparable across the State.

Configurable to Jurisdictional Policies

VAULT allows jurisdictions to define and manage exemption reason categories.

This includes:

- Ability to configure additional exemption reason categories as required
- Flexibility to modify or refine categories based on evolving State policies
- Support for jurisdiction-specific definitions and classifications

This enables West Virginia to adapt exemption tracking without system changes.

Integration with Reporting and Analytics

VAULT integrates exemption reason data into reporting and analysis capabilities.

This includes:

- Reporting by exemption reason across schools, providers, and geographic areas
- Support for identifying trends and patterns in exemption types
- Alignment with public health reporting and compliance monitoring

This ensures that exemption reason data supports both operational and analytical needs.

Summary

VAULT supports standardized and configurable exemption reason classification, enabling consistent data capture and alignment with State policies.

By integrating exemption reasons into reporting and analytics, VAULT enables West Virginia to monitor trends, support compliance, and make informed public health decisions.

4.2.2.3.4 LINKAGE OF EXEMPTION RECORDS TO PATIENT DEMOGRAPHICS

VAULT meets this requirement by fully linking exemption records to patient demographic data, enabling comprehensive analysis across key population attributes and supporting both compliance monitoring and public health decision-making.

Integrated Demographic Linkage

Exemption records are natively linked to patient demographic data within the IIS.

This includes:

- Age and date of birth
- Race and ethnicity
- Geographic attributes (e.g., county, ZIP code, jurisdiction)
- School and organizational affiliations, where applicable

This integrated data model ensures that exemption information is directly associated with the populations it impacts.

Support for Equity and Disparity Analysis

VAULT enables analysis of exemption patterns across demographic groups.

This includes:

- Identification of trends in exemption rates by age group, race/ethnicity, and geography
- Detection of disparities in exemption patterns across communities
- Support for targeted public health interventions and outreach strategies

These capabilities align with public health priorities related to equity and population health outcomes.

Integration with Coverage and Compliance Metrics

VAULT integrates exemption data with immunization coverage and compliance reporting.

This includes:

- Analysis of exemption rates in the context of overall immunization coverage
- Identification of areas or populations with both high exemption rates and low coverage
- Support for school-entry compliance monitoring and enforcement

This ensures that exemption data is actionable within broader immunization program management.

Reporting and Data Accessibility

VAULT enables flexible reporting and data access across demographic dimensions.

This includes:

- Reporting by demographic attributes, school, district, and geographic region
- Support for ad hoc queries and dashboards
- Data availability for public health analysis and decision-making

Summary

VAULT ensures that exemption records are fully integrated with patient demographic data, enabling comprehensive analysis, equity-focused insights, and informed public health action. By linking exemption data with demographic, geographic, and coverage information, VAULT enables West Virginia to identify trends, address disparities, and support compliance and population health goals.

4.2.2.3.5 REPORTING CAPABILITIES BY SCHOOL, GRADE, DISTRICT, EXEMPTION TYPE, AND COMPLIANCE STATUS

VAULT meets this requirement by providing comprehensive, configurable reporting capabilities that enable analysis of exemption data across schools, grades, districts, and other jurisdictional groupings, supporting both compliance monitoring and public health decision-making.

Multi-Dimensional Reporting

VAULT enables reporting across multiple dimensions to support detailed analysis.
This includes:

- School-level reporting, including individual schools and aggregated views
- Grade-level reporting to assess compliance by age group or cohort
- District and jurisdictional reporting (e.g., county, region, statewide)
- Reporting by exemption type (e.g., medical, religious, philosophical)
- Reporting by compliance status, including fully compliant, exempt, and non-compliant populations

This allows users to evaluate exemption patterns and compliance at multiple levels of granularity.

Integration with Immunization Coverage and Compliance

VAULT integrates exemption reporting with broader immunization and compliance metrics.
This includes:

- Combined reporting of exemption rates and vaccination coverage
- Identification of populations with high exemption rates and low immunization coverage

- Support for school-entry compliance monitoring and enforcement

This ensures that exemption data is interpreted within the full context of immunization program performance.

Operational and Regulatory Reporting

VAULT supports reporting required for operational management and regulatory compliance. This includes:

- Reports for school compliance tracking and follow-up
- Support for jurisdictional and federal reporting requirements
- Ability to generate standardized and ad hoc reports for program oversight

This enables the State to meet reporting obligations and manage day-to-day operations effectively.

Configurable and Flexible Reporting Tools

VAULT provides flexible reporting capabilities to meet evolving needs.
This includes:

- Configurable dashboards and report parameters
- Ability to filter and segment data by demographic, geographic, and organizational attributes
- Support for ad hoc queries and data exploration

This allows users to adapt reporting to changing policies and program requirements.

Summary

VAULT provides robust, multi-dimensional reporting capabilities that enable West Virginia to monitor exemption trends, assess compliance, and support informed decision-making.
By integrating exemption data with coverage metrics and supporting flexible, configurable reporting across schools, grades, and districts, VAULT ensures that users have the insights needed to manage immunization programs effectively.

4.2.2.3.6 INTEGRATION WITH SCHOOL ROSTER FUNCTIONALITY AND LONGITUDINAL TRACKING

VAULT meets this requirement by providing seamless integration between exemption tracking and school roster functionality, along with robust support for longitudinal tracking of exemption and immunization status over time.

Integration with School Roster Functionality

VAULT integrates exemption data directly with school roster management capabilities, enabling jurisdictions to manage exemption and compliance status alongside student enrollment and immunization records.

This includes:

- Association of students with schools, districts, and grade levels
- Integration of exemption status into school roster views and workflows
- Visibility of compliance status (e.g., compliant, exempt, non-compliant) at the student, school, and district levels
- Support for managing exemption data within school-based workflows

This enables schools and public health users to efficiently monitor and manage immunization compliance across student populations.

Support for School Compliance and Operational Workflows

VAULT supports school-entry compliance and follow-up activities through integrated workflows.

This includes:

- Identification of students requiring follow-up due to exemptions or non-compliance
- Integration of exemption status into compliance reporting and monitoring
- Support for coordinated outreach and intervention efforts

This ensures alignment with school-entry requirements and public health program objectives.

Longitudinal Tracking of Exemption and Immunization Status

VAULT provides longitudinal tracking capabilities that allow users to monitor exemption and immunization status over time.

This includes:

- Tracking of exemption status as students progress through grades

- Monitoring of changes in exemption status (e.g., provisional, expired, compliant)
- Ability to follow students across schools and districts
- Analysis of exemption and compliance trends over time

This longitudinal view supports both operational management and long-term public health analysis.

Proven Implementation Experience

VAULT has successfully implemented these capabilities in real-world environments.

In Maryland, VAULT supported school-based immunization workflows that integrated student data, vaccination records, and compliance indicators. This enabled the State to track student populations across school systems, identify gaps in compliance, and support coordinated outreach efforts.

Summary

VAULT integrates exemption management with school roster functionality and provides longitudinal tracking of exemption and immunization status.

By enabling visibility across students, schools, and districts—and over time—VAULT supports effective compliance monitoring, operational efficiency, and data-driven public health decision-making.

4.2.2.3.7 CONFIGURATION OPTIONS FOR JURISDICTION-SPECIFIC EXEMPTION WORKFLOWS AND REVIEW PROCESSES

VAULT meets this requirement by providing highly configurable, policy-driven workflows for exemption submission, review, and approval, enabling West Virginia to independently manage and adapt exemption processes without requiring custom development or vendor intervention.

Configurable Exemption Workflows

VAULT enables jurisdictions to define and manage exemption workflows aligned with State policies and operational needs.

This includes:

- Configuration of end-to-end workflows for exemption submission, review, approval, and renewal
- Support for different workflows by exemption type (e.g., medical vs. non-medical)
- Ability to define required data elements, documentation, and validation rules
- Flexibility to modify workflows as policies evolve

This ensures that exemption processing is fully aligned with jurisdictional requirements.

Role-Based Review and Approval Processes

VAULT supports structured, role-based workflows for reviewing and approving exemptions.

This includes:

- Assignment of roles such as school nurses, providers, and public health administrators
- Configuration of review and approval steps based on role and responsibility
- Tracking of review status, decisions, and timestamps
- Support for provisional approvals and follow-up review cycles

This ensures accountability and consistency in exemption decision-making.

Independent Configuration and Operational Autonomy

VAULT is designed to allow jurisdictions to independently configure workflows and policies.

This includes:

- Ability for authorized administrators to update workflows without vendor involvement
- Configuration-driven approach that avoids one-off custom development
- Support for rapid policy changes without system redesign

This approach enhances flexibility, reduces long-term costs, and enables the State to respond quickly to evolving requirements.

Auditability and Lifecycle Tracking

VAULT provides full visibility into the lifecycle of exemption records and workflow activities.

This includes:

- Audit tracking of all submission, review, and approval actions
- Status management for exemption records throughout their lifecycle
- Visibility into pending, approved, rejected, and expired exemptions

This ensures transparency, accountability, and support for compliance and audit requirements.

Summary

VAULT provides configurable, policy-driven exemption workflows that enable West Virginia to manage submission, review, and approval processes with flexibility and independence.

By supporting role-based workflows, independent configuration, and full auditability, VAULT ensures that exemption management is adaptable, transparent, and aligned with evolving jurisdictional requirements.

4.2.2.4 COVERAGE REPORTING AND POPULATION DEFINITION

VAULT meets the requirements of Section 4.2.2.4 by providing a configurable, transparent, and standards-aligned framework for defining populations and generating immunization coverage reports. The system enables West Virginia to accurately calculate coverage rates using clearly defined numerator and denominator logic, apply jurisdiction-specific filters, and produce consistent, defensible reports aligned with CDC methodologies.

VAULT provides a comprehensive, flexible, and transparent framework for defining populations and reporting immunization coverage, enabling West Virginia to accurately measure performance, monitor trends, and support data-driven public health decisions.

These capabilities enable West Virginia to monitor vaccination coverage across rural, school-based, and at-risk populations, supporting targeted outreach and improved health outcomes.

Operational Workflow

1. OEPS or authorized users define population criteria (e.g., age cohort, geography, provider, program participation)

2. The system applies standardized numerator and denominator logic aligned with CDC methodologies
3. Users generate reports filtered by jurisdiction (state, county, district, school, or custom regions)
4. The system calculates coverage metrics in real time
5. Results are displayed through dashboards or exported for further analysis and reporting

The platform supports precise definition of numerator and denominator populations using configurable criteria, including age cohorts, geographic boundaries, provider attribution, program participation, and vaccination status. These definitions are fully documented and consistently applied, ensuring that coverage rates are accurate, defensible, and aligned with CDC methodologies and jurisdictional requirements.

For West Virginia, this enables OEPS staff, county health departments, and school-based programs to evaluate coverage at multiple levels, identify under-vaccinated populations, and support targeted intervention strategies across rural and underserved areas.

VAULT's reporting capabilities enable multi-dimensional analysis across geographic regions, demographic groups, and organizational structures. Users can evaluate immunization coverage at the state, county, district, school, and population levels, and combine geographic, demographic, and programmatic filters to produce targeted and actionable insights.

The system supports full lifecycle reporting of vaccine series, including initiation, completion, and identification of individuals requiring additional doses. These capabilities are integrated with population definitions and coverage calculations, enabling the State to not only measure performance but also identify gaps and support targeted outreach and intervention strategies. VAULT's configurable reporting framework allows users to define, save, and reuse report parameters, as well as schedule recurring reports for ongoing monitoring. This empowers the State to independently manage reporting, adapt to evolving requirements, and reduce reliance on vendor support.

All reports are generated from a consistent, validated data source, ensuring that coverage metrics remain uniform across users, reports, and time periods, eliminating discrepancies and improving confidence in reported outcomes.

What Sets VAULT Apart

VAULT delivers a fully transparent, configurable, and State-controlled reporting framework that ensures consistent, defensible coverage calculations while enabling independent reporting without vendor dependency.

Key differentiators include:

State-Controlled Population Definition (Numerator & Denominator)

VAULT enables jurisdictions to define and manage numerator and denominator populations with precision, using configurable criteria aligned with CDC methodologies and State-specific requirements. This ensures that coverage rates are both accurate and fully defensible.

Transparent and Defensible Reporting Logic

All population definitions, filters, and calculation methods are visible and documented within the system. This transparency ensures consistency across reports and allows the State to clearly explain and validate how coverage rates are derived.

Multi-Dimensional and Highly Granular Analysis

VAULT supports reporting across geographic, demographic, and organizational dimensions, including custom-defined regions. Users can combine filters to produce highly targeted insights that support both operational management and strategic planning.

Full Lifecycle Coverage Measurement (Initiation → Completion → Gaps)

VAULT goes beyond static reporting by supporting the full lifecycle of immunization tracking, including series initiation, completion, and identification of individuals requiring additional doses. This enables the State to move from measurement to action.

Reusable and Automated Reporting

VAULT allows users to save report configurations and schedule recurring reports, enabling consistent, automated monitoring of coverage and compliance metrics. This reduces manual effort and ensures ongoing visibility into program performance.

Independent Configuration Without Vendor Dependency

VAULT's configuration-driven approach enables authorized users to define, modify, and manage reporting without requiring vendor involvement. This provides flexibility, reduces long-term costs, and allows the State to adapt quickly to changing requirements.

4.2.2.4.1 ABILITY TO DEFINE AND DOCUMENT THE DEMOGRAPHIC POPULATION USED FOR RATE CALCULATIONS (NUMERATOR AND DENOMINATOR)

VAULT meets this requirement by providing flexible, transparent, and configurable tools to define and document populations used in immunization rate calculations, including both numerator and denominator definitions.

Configurable Numerator and Denominator Definitions

VAULT enables users to define both numerator and denominator populations with a high degree of precision.

This includes:

- Numerator definitions based on vaccination status (e.g., series completion, dose administration)
- Denominator definitions based on defined population criteria (e.g., age cohorts, enrollment status, geographic location)
- Support for inclusion and exclusion criteria based on factors such as provider association, program eligibility, and exemption status

This ensures that immunization rates are calculated accurately and reflect jurisdiction-specific requirements.

Flexible Population Definition Criteria

VAULT supports multi-dimensional population definition capabilities.

This includes:

- Age-based cohort definitions (e.g., 19–35 months, school-entry cohorts)
- Geographic filters (e.g., state, county, district)
- Provider or organization attribution
- Program participation and eligibility criteria

This flexibility enables the State to define populations aligned with both operational and reporting needs.

Transparency and Documentation of Rate Calculations

VAULT ensures that all population definitions and rate calculations are transparent and well-documented.

This includes:

- Clear visibility into numerator and denominator logic used for each report
- Documentation of applied filters, inclusion/exclusion criteria, and calculation methods
- Consistent application of definitions across reports and users

This supports defensible reporting and ensures consistency across analyses.

Alignment with CDC and Jurisdictional Methodologies

VAULT supports alignment with CDC methodologies and State-defined coverage metrics.

This includes:

- Ability to configure population definitions to match CDC-recommended measures
- Flexibility to support jurisdiction-specific calculation methodologies
- Support for standard and custom reporting requirements

This ensures that coverage rates are both compliant and adaptable.

Independent Configuration and Ongoing Refinement

VAULT allows authorized users to refine population definitions without vendor involvement.

This includes:

- Ability to update numerator and denominator criteria as program needs evolve

- Configuration-driven approach that avoids custom development
- Support for iterative refinement of definitions over time

This enables the State to maintain control, reduce costs, and adapt quickly to changing requirements.

4.2.2.4.2 SUPPORT FOR JURISDICTIONAL FILTERING BY STATE, COUNTY, OR OTHER GEOGRAPHIC BOUNDARIES

VAULT meets this requirement by providing robust, configurable jurisdictional filtering capabilities that enable users to segment and analyze immunization data across multiple geographic levels.

Multi-Level Geographic Filtering

VAULT supports filtering and reporting across a range of geographic boundaries.
This includes:

- Statewide, county, and regional views
- City and ZIP code–level filtering
- Districts, service areas, or other jurisdiction-defined geographic groupings

This enables users to analyze coverage at varying levels of granularity, from high-level summaries to localized insights.

Configurable Geographic Definitions

VAULT allows jurisdictions to define and manage geographic groupings based on their needs.
This includes:

- Ability to configure custom geographic boundaries (e.g., health districts, program regions)
- Alignment with jurisdiction-specific reporting structures
- Flexibility to update geographic definitions as organizational or policy needs evolve

This ensures that geographic filtering reflects how the State manages and reports on populations.

Combined Filtering for Targeted Analysis

VAULT enables geographic filtering to be combined with other population criteria.

This includes:

- Integration with demographic filters (e.g., age, race/ethnicity)
- Combination with program participation and provider attribution
- Alignment with numerator and denominator population definitions

This allows for highly targeted and precise analysis of coverage rates and population segments.

Support for Coverage Analysis and Public Health Action

VAULT's jurisdictional filtering capabilities support both reporting and operational decision-making.

This includes:

- Identification of geographic areas with low coverage or high exemption rates
- Detection of disparities across communities
- Support for targeted outreach, intervention, and resource allocation

Summary

VAULT provides flexible, configurable jurisdictional filtering capabilities that enable West Virginia to analyze immunization coverage across multiple geographic levels.

By supporting custom geographic definitions and combined filtering with demographic and programmatic criteria, VAULT enables precise, actionable insights to support reporting, compliance, and public health decision-making.

4.2.2.4.3 ABILITY TO GENERATE REPORTS REFLECTING COVERAGE STATUS

VAULT provides comprehensive support for vaccine series reporting, enabling West Virginia to measure, monitor, and improve immunization coverage across the full lifecycle of vaccination. The platform supports identification of individuals who have initiated vaccine series, completed required series, and those who require additional doses to achieve completion. These capabilities are aligned with CDC-recommended schedules and can be configured to reflect jurisdiction-specific requirements.

VAULT integrates series reporting with defined population cohorts and coverage calculations, ensuring that initiation, completion, and gap metrics are accurately reflected in numerator and denominator definitions. This enables the State to produce consistent, defensible coverage rates across reporting scenarios.

In addition to measurement, VAULT supports operational use of this data by identifying populations that have initiated but not completed vaccination and those who are due or overdue for additional doses. This enables targeted reminder and recall efforts, supports school-entry compliance, and improves overall immunization program performance.

4.2.2.4.3.1 COMPLETE VACCINE SERIES

VAULT meets this requirement by enabling identification and reporting of individuals who have completed required vaccine series based on CDC-recommended schedules and jurisdiction-defined criteria.

CDC-Aligned Series Completion Logic

VAULT supports determination of series completion using standardized immunization schedules.

This includes:

- Evaluation of completed vaccine series based on CDC schedules and recommendations
- Support for jurisdiction-specific variations in series requirements
- Consideration of dose timing, intervals, and valid dose criteria

This ensures that series completion is calculated accurately and consistently.

Configurable Series Definitions

VAULT allows jurisdictions to define and manage series completion criteria.

This includes:

- Ability to configure which vaccines and dose combinations constitute a completed series
- Support for program-specific or jurisdiction-specific series definitions
- Flexibility to update definitions as guidelines evolve

This enables the State to maintain control over how completion is defined and reported.

Integration with Population Definitions

VAULT integrates series completion reporting with defined numerator and denominator populations.

This includes:

- Alignment with configured population cohorts (e.g., age groups, school-entry populations)
- Inclusion of completed series in numerator calculations for coverage rates
- Consistent application of definitions across reporting

This ensures that coverage metrics are accurate and defensible.

Reporting and Analysis

VAULT provides reporting capabilities to analyze series completion across populations.

This includes:

- Reporting by geographic, demographic, and organizational dimensions
- Identification of populations with high or low completion rates
- Support for compliance monitoring and program evaluation

Summary

VAULT enables accurate and configurable identification of individuals who have completed vaccine series, aligned with CDC schedules and jurisdictional requirements.
By integrating series completion logic with population definitions and reporting tools, VAULT ensures that West Virginia can produce reliable, defensible coverage metrics and evaluate immunization program performance effectively.

4.2.2.4.3.2 INITIATION OF SERIES (1 OR MORE DOSES)

VAULT meets this requirement by supporting the identification and reporting of individuals who have initiated vaccine series, defined as receipt of one or more valid doses within a series, in alignment with CDC guidance and jurisdictional criteria.

CDC-Aligned Initiation Logic

VAULT determines initiation of vaccine series based on valid dose administration.
This includes:

- Identification of individuals who have received at least one valid dose in a vaccine series
- Evaluation of dose validity based on CDC schedules, timing, and interval rules
- Support for jurisdiction-specific definitions of initiation where applicable

This ensures that initiation metrics are calculated accurately and consistently.

Integration with Population Definitions

VAULT integrates initiation reporting with defined numerator and denominator populations.

This includes:

- Alignment with configured population cohorts (e.g., age groups, school-entry populations)
- Inclusion of initiated individuals in numerator calculations for coverage metrics
- Consistent application of definitions across reports

This ensures that initiation rates are accurate, comparable, and defensible.

Identification of Gaps in Series Completion

VAULT enables users to identify populations that have initiated but not completed vaccine series.

This includes:

- Analysis of drop-off between initiation and completion
- Identification of individuals and populations requiring follow-up
- Support for targeted outreach and intervention strategies

This capability is critical for improving immunization coverage and program effectiveness.

Reporting and Analysis

VAULT provides flexible reporting on series initiation.

This includes:

- Reporting across geographic, demographic, and organizational dimensions
- Integration with coverage and compliance reporting
- Support for trend analysis over time

Summary

VAULT enables accurate and configurable reporting on initiation of vaccine series, aligned with CDC standards and jurisdictional requirements.

By integrating initiation metrics with population definitions and reporting tools, VAULT allows West Virginia to identify early engagement, monitor gaps in completion, and support targeted public health interventions.

4.2.2.4.3.3 FINAL DOSE NEEDED TO COMPLETE A SERIES

VAULT meets this requirement by enabling identification of individuals who require one or more additional doses to complete a vaccine series, based on CDC-recommended schedules and jurisdiction-defined criteria.

CDC-Aligned Forecasting of Remaining Doses

VAULT determines the remaining doses required for series completion using immunization forecasting logic.

This includes:

- Identification of missing doses within a vaccine series
- Evaluation of dose validity, timing, and interval requirements based on CDC schedules
- Determination of when the next dose is due or overdue

This ensures that completion requirements are calculated accurately and consistently.

Integration with Population and Coverage Definitions

VAULT integrates identification of incomplete series with population definitions and coverage calculations.

This includes:

- Alignment with defined cohorts (e.g., age groups, school-entry populations)
- Identification of individuals included in denominators but not yet meeting numerator criteria

- Support for consistent and defensible coverage reporting

Support for Reminder and Recall Activities

VAULT enables targeted outreach to individuals who have not completed vaccine series.

This includes:

- Identification of individuals due or overdue for final doses
- Support for reminder and recall workflows
- Ability to segment populations for targeted intervention

This capability supports improved completion rates and public health outcomes.

Operational and Compliance Use Cases

VAULT supports use of incomplete series data in operational and compliance workflows.

This includes:

- Identification of students or populations not meeting school-entry requirements
- Integration with compliance reporting and follow-up activities
- Support for program monitoring and performance evaluation

Summary

VAULT enables accurate identification of individuals who require additional doses to complete vaccine series, using CDC-aligned forecasting and configurable criteria.

By integrating this capability with population definitions, reporting, and outreach workflows, VAULT supports improved completion rates, compliance monitoring, and effective public health intervention.

4.2.2.4.4 CONFIGURATION OPTIONS FOR CUSTOMIZING REPORT PARAMETERS AND ALIGNING WITH CDC AND STATE-DEFINED COVERAGE METRICS

VAULT meets this requirement by providing extensive, user-driven configuration capabilities that enable jurisdictions to define, generate, and manage coverage reports aligned with both CDC standards and State-defined metrics—without reliance on vendor intervention.

Configurable Reporting Parameters

VAULT enables users to define and adjust reporting parameters to meet specific program and policy needs.

This includes:

- Population criteria (e.g., age cohorts, enrollment status, program participation)
- Timeframes for analysis and reporting periods
- Vaccine groupings and series definitions
- Geographic filters (e.g., state, county, district, custom regions)

This flexibility ensures that coverage reports reflect both federal requirements and jurisdiction-specific priorities.

User-Defined and Reusable Report Configurations

VAULT allows users to create, save, and reuse report configurations.

This includes:

- Ability to save customized report parameters for repeated use
- Standardization of commonly used reports across teams
- Consistent application of definitions across reporting cycles

This reduces manual effort and ensures consistency in reporting.

Scheduled and Recurring Reporting

VAULT supports automation of reporting through scheduled execution.

This includes:

- Ability to schedule reports to run on a recurring basis (e.g., daily, weekly, monthly)

- Automated generation of reports using predefined parameters
- Support for ongoing monitoring of coverage and compliance metrics

This enables continuous visibility into immunization performance without manual intervention.

Support for Standard and Custom Reporting

VAULT supports both standardized and custom reporting needs.

This includes:

- Predefined reports aligned with CDC and federal reporting requirements
- Custom reports tailored to jurisdictional priorities and program needs
- Ability to adapt reporting as requirements evolve

User-Friendly Configuration and Access

VAULT's reporting tools are designed for use by program staff without technical expertise.

This includes:

- Intuitive interfaces for configuring and generating reports
- Ability for authorized users to modify parameters independently
- Reduced reliance on technical resources or vendor support

This empowers the State to manage reporting efficiently and independently.

Proven Implementation Experience

VAULT has successfully implemented advanced, configurable coverage reporting in real-world environments.

In Maryland, VAULT enabled the State to analyze vaccination rates across diverse populations and geographic regions, identify gaps in coverage, support school compliance monitoring, and inform targeted outreach initiatives. The ability to configure, save, and adapt reports over time has been critical in supporting ongoing program evaluation and improvement.

4.2.2.5 SUPPORT SCALABLE DATA EXCHANGE AND REPORTING VIA READ REPLICA INTEGRATION

VAULT meets this requirement by providing a dedicated, read-only replica architecture that enables secure, high-performance access to IIS data for reporting, analytics, and external data exchange without impacting production system operations.

The solution is designed around strict separation of transactional and analytical workloads, ensuring that all read-intensive operations—including queries, reporting, and integrations—are executed against the replica environment while production remains optimized for real-time clinical and operational use.

VAULT utilizes continuous replication mechanisms (e.g., streaming/log-based replication) to maintain near real-time synchronization between production and replica environments. This ensures that downstream systems have timely access to current data while preserving system stability and performance.

The architecture supports:

- Read-only enforced access to protect production data integrity
- Role-based and secure access controls for all users and systems
- Multiple access methods (SQL, APIs, data extracts, BI tools)
- Monitoring of replication health, latency, and data exchange volumes
- Full documentation of architecture, access protocols, and data structures

Outcome for West Virginia:

A scalable, secure, and independent data access environment that supports enterprise analytics, reporting, and integration without impacting core IIS operations.

4.2.2.5.1 INCLUSION OF A READ-ONLY REPLICA OR EQUIVALENT MECHANISM

VAULT provides a dedicated read-only replica database that mirrors the production IIS environment and is specifically optimized for reporting, analytics, and external system access. This replica operates as a logically separate database instance, ensuring complete isolation of analytical workloads from transactional processing.

Workload Isolation and System Protection

- All reporting, analytics, and external queries are routed exclusively to the replica
- Production system performance is protected from read-intensive workloads
- Providers and end users experience consistent system responsiveness

External Integration Support

- Direct integration with downstream systems (e.g., Data Bridge, warehouses, BI tools)
- Support for structured data pipelines and cross-system data exchange
- Read-only enforcement ensures no risk to production data

Flexible Access Methods

- SQL-based querying for advanced analytics
- API-based access for application integration
- Structured data extracts for batch processing

State-Controlled Access

- Authorized State users and systems access data directly
- No vendor mediation required for reporting or analytics
- Enables independent development of dashboards and analytical workflows

4.2.2.5.2 UPDATE FREQUENCY OF THE REPLICA

VAULT provides continuous, near real-time data replication from production to the read replica.

Replication Method and Latency

- Log-based or streaming replication ensures minimal delay
- Typical replication latency measured in seconds to minutes (environment-dependent)
- Continuous synchronization supports operational and analytical use cases

Configurable Replication Cadence

- Near real-time (continuous streaming)
- Scheduled intervals (e.g., hourly, daily) where required
- Configurable to balance performance and data freshness

Data Consistency Controls

- Transactional integrity maintained across environments
- Monitoring of replication lag and synchronization status
- Automatic alignment with production updates

Result:

West Virginia has access to current, reliable data suitable for real-time reporting and decision-making.

4.2.2.5.3 MANAGEMENT OF READ-ONLY ACCESS TO PROTECT PRODUCTION PERFORMANCE

VAULT enforces strict read-only access controls and workload isolation to ensure that analytical activity never impacts production operations.

Workload Separation

- All read operations executed in replica environment
- Production reserved exclusively for transactional workflows

Read-Only Enforcement

- No write operations permitted in replica
- Eliminates risk of data corruption or unintended changes

Performance Optimization

- Query optimization and indexing strategies
- Support for high-concurrency analytical workloads
- Resource isolation for large-scale queries

Security Controls

- Role-based access control (RBAC)
- Least-privilege enforcement
- Secure access protocols for all users and systems

4.2.2.5.4 CONFIGURATION, DEPLOYMENT, AND MAINTENANCE OF REPLICATION

VAULT manages the full lifecycle of replication infrastructure, including configuration, deployment, monitoring, and maintenance.

Replication Architecture Management

- Configuration of replication pipelines and synchronization processes
- Deployment in secure, scalable cloud infrastructure
- Alignment with production schema and updates

Automated Replication Operations

- Continuous synchronization processes
- Automated monitoring and failover readiness
- Minimal manual intervention required

Scalability and Resilience

- Elastic infrastructure supporting increasing data volume
- High availability and redundancy
- Secure network and system configurations

Reduced State Burden

- VAULT manages infrastructure and replication pipelines
- State focuses on data use rather than system maintenance

4.2.2.5.5 MONITORING, TROUBLESHOOTING, AND DATA CONSISTENCY

VAULT provides continuous monitoring and validation to ensure replication reliability and data integrity.

Replication Monitoring

- Tracking of replication lag and synchronization status
- Monitoring of system performance and resource utilization
- Automated alerts for anomalies or failures

Proactive Issue Resolution

- Automated diagnostics and root cause analysis

- Rapid remediation of synchronization issues
- Defined escalation processes

Data Validation

- Verification of data consistency between environments
- Detection of discrepancies or incomplete replication
- Assurance of accurate downstream reporting

4.2.2.5.6 DOCUMENTATION OF REPLICATION ARCHITECTURE AND ACCESS PROTOCOLS

VAULT provides comprehensive documentation to support transparency, integration, and independent use.

This includes:

- Architecture diagrams and data flow documentation
- Replication methods and update cadence
- Access methods and security protocols
- Schema documentation and data structures
- Integration guidance for external systems

4.2.2.5.7 SECURE AND EFFICIENT QUERYING BY AUTHORIZED USERS

VAULT enables secure, high-performance querying through standardized access methods.

Access and Security

- Role-based access control (RBAC)
- Secure authentication and authorization
- Enforcement of least-privilege access

Query Methods

- SQL-based querying
- API access
- Integration with BI and analytics platforms

Performance at Scale

- Optimized for large datasets and complex queries
- Support for concurrent users and workloads
- Tuned indexing and resource management

4.2.2.5.8 QUANTIFICATION OF DATA EXCHANGE VOLUMES

VAULT provides **comprehensive tracking and reporting of data exchange activity**.

Data Flow Monitoring

- Tracking of inbound/outbound interface traffic (HL7, APIs)
- Monitoring of replica access and data extracts
- Visibility into system-to-system data movement

Volume Metrics and Reporting

- Measurement of data volumes across interfaces and integrations
- Reporting on frequency and usage trends
- Identification of high-volume workloads

Capacity Planning

- Insight into system utilization and growth patterns
- Support for infrastructure scaling decisions
- Monitoring of load from reporting and integration activity

4.2.2.6 DATABASE SCHEMA AND DATA DICTIONARY

VAULT provides comprehensive, transparent, and standards-aligned documentation of the system's data architecture, enabling West Virginia to fully understand, manage, and utilize its IIS data environment.

The platform includes detailed entity-relationship diagrams, field-level definitions, and documentation of key tables and data domains, providing clear visibility into how data is structured and how it flows across clinical, operational, and reporting functions.

VAULT's data dictionary aligns with CDC standards and HL7 v2.5.1 messaging specifications, ensuring consistency between internal data structures and external data exchange requirements. Support for both HL7 and FHIR further enables modern, flexible interoperability.

Through structured versioning, controlled schema updates, and comprehensive documentation, VAULT ensures that the data model evolves in a stable, predictable manner while maintaining backward compatibility and minimizing disruption to integrations and workflows.

This approach supports strong data governance, accurate reporting, and long-term sustainability of the IIS data environment.

What Sets VAULT Apart

VAULT distinguishes itself by providing full transparency into the system's data architecture, combined with structured governance and standards alignment that enable the State to independently understand, manage, and evolve its data environment over time.

Key differentiators include:

Complete Visibility into Data Structures and Relationships

VAULT provides detailed ERDs, schema documentation, and table definitions that clearly illustrate how all data elements are structured and connected across the system. This enables full understanding of the IIS data model across clinical, operational, and reporting domains.

Comprehensive, Standards-Aligned Data Dictionary

VAULT delivers field-level definitions aligned with CDC IIS Functional Standards, HL7 v2.5.1 messaging, and standardized code sets. This ensures consistency, accuracy, and interoperability across internal data storage and external data exchange.

Operationalized Interoperability (HL7 + FHIR)

VAULT provides fully implemented and maintained mappings between internal data structures and HL7 message standards through IISConnex, while also supporting FHIR-based data exchange. This ensures both current compliance and future readiness.

Structured Governance and Controlled Schema Evolution

VAULT's versioning and change management framework ensures that schema updates are implemented in a controlled, transparent manner, with impact analysis, backward compatibility, and clear communication to stakeholders.

State Independence and Long-Term Sustainability

VAULT's documentation and governance approach enables the State to independently understand and utilize its data without reliance on vendor support. This reduces long-term costs and supports sustainable system operation and evolution.

4.2.2.6.1 ENTITY-RELATIONSHIP DIAGRAMS (ERDS)

VAULT meets this requirement by providing comprehensive entity-relationship diagrams (ERDs) and schema documentation that clearly illustrate the structure of the system and relationships between core data entities.

Comprehensive Data Model Representation

VAULT delivers detailed ERDs that represent both logical and physical data models.
These diagrams include:

- Patient and demographic data structures
- Immunization records and vaccination events
- Provider, organization, and facility entities
- Inventory management structures
- Exemption and program participation data
- School roster and population-based modules

This ensures full visibility into the system's data architecture.

Clear Definition of Data Relationships

VAULT's ERDs clearly depict relationships between entities.

This includes:

- Primary and foreign key relationships
- Data dependencies across modules
- Linkages between clinical, operational, and reporting datasets

This enables stakeholders to understand how data flows across the system and supports accurate integration and reporting.

Support for Integration and Data Exchange

VAULT's schema documentation is designed to support interoperability and external system integration.

This includes:

- Clear mapping of relationships across data domains
- Support for interface development and data exchange workflows
- Alignment with IIS data structures and integration requirements

This enables efficient integration with external systems, including EHRs, data warehouses, and public health platforms.

Accessible and Usable Documentation

VAULT provides ERDs in formats that are accessible to both technical and non-technical stakeholders.

This includes:

- Visual representations that support system understanding and onboarding
- Use during implementation, integration, and ongoing system management
- Availability to authorized users for reference and planning

This ensures that stakeholders can easily understand and utilize the system's data structure.

Summary

VAULT provides detailed, accessible entity-relationship diagrams that deliver full transparency into the system's data architecture.

By clearly defining data structures and relationships, VAULT enables West Virginia to understand, integrate with, and effectively manage its IIS data environment.

4.2.2.6.2 FIELD-LEVEL DEFINITIONS

VAULT meets this requirement by providing a comprehensive data dictionary that includes detailed, field-level definitions for all system data elements, ensuring full transparency into how data is structured, validated, and used within the IIS.

Comprehensive Field-Level Metadata

VAULT's data dictionary includes detailed metadata for each data element.

This includes:

- Field names and clear descriptions
- Data types and formats (e.g., string, date, numeric)
- Required versus optional field designation
- Allowable values and standardized code sets (e.g., CVX, MVX)

- Validation rules, constraints, and business logic
- Default values where applicable

This ensures that all data elements are clearly defined and consistently applied across the system.

Alignment with National Standards

VAULT aligns field definitions with recognized standards and messaging specifications.

This includes:

- Alignment with CDC IIS Functional Standards
- Support for HL7 v2.5.1 message structures and data elements
- Use of standardized code sets for vaccines, manufacturers, and related data

This ensures consistency between internal data structures and external data exchange requirements.

Support for Data Governance and Data Quality

VAULT's data dictionary supports strong data governance practices.

This includes:

- Clear documentation of validation rules and constraints
- Support for consistent data entry and processing
- Enablement of data quality monitoring and reporting

This ensures that data remains accurate, complete, and reliable.

Support for Integration and Reporting

VAULT's field-level documentation enables efficient integration and reporting.

This includes:

- Clear understanding of data elements for interface development
- Support for mapping to external systems and data warehouses
- Enablement of consistent and accurate reporting across platforms

Accessible and Maintainable Documentation

VAULT provides the data dictionary in formats accessible to both technical and operational stakeholders.

This includes:

- Availability to authorized users for reference and system understanding
- Support for onboarding, training, and ongoing system use
- Updates aligned with system enhancements and schema changes

Summary

VAULT provides a comprehensive, standards-aligned data dictionary that delivers full visibility into field-level definitions, validation rules, and allowable values.

By ensuring transparency, consistency, and alignment with national standards, VAULT enables West Virginia to support strong data governance, accurate reporting, and seamless system integration.

4.2.2.6.3 DEFINITIONS OF KEY TABLES AND DATA DOMAINS

VAULT meets this requirement by providing detailed documentation of all key tables and data domains within the system, ensuring full transparency into how data is structured, related, and used across the IIS.

Comprehensive Coverage of Core Data Domains

VAULT's schema documentation includes detailed definitions of all major tables and data domains.

This includes:

- **Patient Records:** Demographic information, identifiers, and cross-system linkages
- **Vaccination Events:** Administration details, vaccine types, lot numbers, and provider attribution

- **Inventory Management:** Vaccine stock levels, lot tracking, distribution, and reconciliation
- **Exemptions:** Medical and non-medical exemption records, including status, review cycles, and expiration tracking
- **School Roster Modules:** Student-to-school associations supporting compliance monitoring and population-based reporting

This ensures that all critical components of the IIS data model are clearly defined and accessible.

Defined Relationships Across Data Domains

VAULT documents how key tables relate to one another across the system.

This includes:

- Relationships between patients, providers, and vaccination events
- Linkages between inventory, administration, and reporting datasets
- Integration of exemption and school roster data with patient and immunization records

This cross-domain visibility enables stakeholders to understand how data flows across clinical, operational, and reporting functions.

Inclusion of Business Rules and Data Usage Context

VAULT's table definitions include not only structure, but also how data is used within the system.

This includes:

- Business rules governing data creation, validation, and updates
- Context for how tables support workflows such as vaccination, inventory management, and compliance tracking
- Alignment with reporting and analytics use cases

This ensures that the data model is not only understood structurally, but also operationally.

Support for Integration, Reporting, and System Maintenance

VAULT's structured approach to table definitions supports long-term system usability and interoperability.

This includes:

- Enablement of efficient interface development and data exchange
- Support for accurate reporting and analytics across domains
- Facilitation of ongoing system maintenance and future enhancements

Summary

VAULT provides comprehensive, well-structured documentation of key tables and data domains, including their relationships, business rules, and usage within the system.

By delivering clear, integrated visibility across all major data components, VAULT enables West Virginia to effectively manage, analyze, and evolve its IIS data environment over time.

4.2.2.6.4 MAPPING TO CDC HL7 V2.5.1 STANDARDS

VAULT meets this requirement by providing comprehensive, standards-aligned mapping between internal data structures and CDC HL7 v2.5.1 message specifications, ensuring consistent and reliable interoperability with external systems.

Detailed Mapping to HL7 Message Structures

VAULT maintains explicit mappings between internal data elements and HL7 message components.

This includes:

- Mapping of internal data fields to HL7 segments and fields (e.g., PID, RXA, ORC)
- Support for core IIS message types, including VXU (unsolicited vaccination updates), QBP (query), and ACK (acknowledgment)

- Documentation of transformation logic between internal schema and HL7 message formats

This ensures that data is accurately translated between internal and external systems.

Alignment with CDC Validation Rules and Specifications

VAULT aligns all mappings with CDC IIS implementation guidance and validation requirements.

This includes:

- Enforcement of validation rules consistent with CDC message specifications
- Support for required and optional fields as defined by HL7 v2.5.1
- Continuous updates to reflect evolving CDC standards and guidance

This ensures compliance and consistency across all data exchange activities.

Operationalized Through IISConnex

VAULT's HL7 mappings are implemented and managed within IISConnex, the platform's interoperability framework.

This includes:

- Centralized management of message transformations and mappings
- Support for scalable, multi-jurisdictional data exchange
- Proven implementation across high-volume, real-world environments

This demonstrates that VAULT's interoperability approach is not theoretical, but operational and production-tested.

Support for Both HL7 and FHIR Standards

VAULT supports both traditional and modern interoperability standards.

This includes:

- HL7 v2.5.1 messaging for IIS integration
- Mapping to FHIR resources for modern API-based data exchange
- Consistent alignment between HL7 and FHIR representations of data

This dual-standard approach ensures long-term flexibility and future readiness.

Summary

VAULT provides comprehensive, standards-aligned mapping between internal data structures and CDC HL7 v2.5.1 specifications, supported by a robust interoperability framework.
By combining detailed mapping, continuous compliance with CDC standards, and support for both HL7 and FHIR, VAULT ensures that West Virginia can achieve reliable, scalable, and future-ready data exchange across systems.

4.2.2.6.5 VERSIONING AND UPDATE PROTOCOLS

VAULT meets this requirement by maintaining a structured data governance and versioning framework that manages schema changes in a controlled, transparent, and minimally disruptive manner.

Version-Controlled Schema Management

VAULT maintains version-controlled schema documentation to track all changes over time.
This includes:

- Versioning of database schema and data dictionary artifacts
- Historical tracking of changes to tables, fields, and relationships
- Clear documentation of schema evolution

This ensures traceability and consistency across system updates.

Structured Change Management Process

VAULT implements formal change management processes for all schema updates.
This includes:

- Impact analysis for proposed changes to data structures
- Evaluation of effects on reporting, integrations, and downstream systems
- Controlled approval and release processes

This ensures that all changes are carefully assessed and aligned with system requirements.

Backward Compatibility and Integration Stability

VAULT prioritizes backward compatibility to protect existing integrations and workflows.

This includes:

- Design of schema updates to minimize disruption to existing interfaces
- Support for continued operation of integrations during transition periods
- Coordination with stakeholders for any required updates

This ensures stability for external systems and ongoing operations.

Controlled Release and Communication

Schema updates are implemented through structured release cycles with clear communication to stakeholders.

This includes:

- Deployment through tested and validated release processes
- Advance notice of changes that may impact data exchange or reporting
- Release notes and updated documentation for all schema modifications

This ensures that the State and its partners are informed, prepared, and able to adapt.

Living Data Dictionary and Continuous Alignment

VAULT maintains the data dictionary as a continuously updated resource.

This includes:

- Ongoing updates aligned with system enhancements and regulatory changes
- Consistent documentation across users, systems, and reporting processes
- Support for long-term data governance and system evolution

Summary

VAULT provides a structured, version-controlled approach to schema management that ensures transparency, stability, and controlled evolution of the IIS data model.

By combining rigorous change management, backward compatibility, and proactive communication, VAULT enables West Virginia to adopt system enhancements with confidence while maintaining continuity for reporting, interoperability, and operational workflows.

4.2.2.7 ORAL HEALTH MODULE

VAULT provides a flexible and scalable approach to supporting oral health workflows within the IIS, enabling documentation, tracking, and reporting of school-based and community-delivered services.

The platform supports integration with school rosters, allowing students to be linked to schools, grades, classrooms, and teachers, and enabling population-based tracking, targeted outreach, and program management.

VAULT's role-based workflow model enables dental professionals to document care at the point of service, while school nurses and administrative staff can manage rosters, enter historical data, and coordinate follow-up activities. This ensures that services delivered across clinical, school, and community settings are captured within a unified, longitudinal student record.

Comprehensive reporting capabilities enable identification of students who have and have not received services, analysis of gaps in care, and prioritization of high-need populations using demographic, geographic, and programmatic filters.

VAULT's role-based access control framework ensures that appropriate permissions are assigned across user types, with full administrative control over roles and access.

Importantly, these capabilities are delivered through a flexible and configurable platform that extends beyond oral health, enabling the State to support a wide range of school-based and community health services within a single, unified system.

What Sets VAULT Apart

VAULT distinguishes itself by delivering not just an oral health module, but a flexible, population-based platform designed to support a wide range of school-based and community health services.

Key differentiators include:

Platform-Based Approach (Not a Single-Purpose Module)

VAULT's architecture supports oral health as part of a broader ecosystem of clinical and community-based services. The same workflows, data model, and reporting capabilities can be extended to screenings, preventive services, and treatment programs—eliminating the need for separate systems.

Deep Integration with School-Based Workflows

VAULT supports detailed student-to-school linkage, including associations by school, grade, classroom, and teacher. This enables real-world school operations, including classroom-level organization, group-based workflows, and targeted outreach to specific student populations.

Population-Based Care and Outreach

VAULT enables identification of students who have and have not received services, along with filtering by geography, demographics, and urgency of care. This supports targeted interventions, equitable resource allocation, and data-driven program management.

Coordinated Multi-Role Workflows

VAULT supports distinct but integrated workflows for dental professionals, school nurses, and administrative users. This enables real-time documentation, retrospective data entry, and coordinated follow-up across multiple stakeholders and care settings.

Unified Longitudinal Student Record

VAULT ensures that all services—regardless of where they are delivered—are captured within a single, comprehensive student record. This supports continuity of care and enables a complete view of student health over time.

Scalable, Configurable Access Control

VAULT's role-based access control framework enables secure, flexible management of user permissions across all programs. Administrators can configure roles and permissions independently, supporting scalability and alignment with jurisdictional policies.

4.2.2.7.1 ROSTER INTEGRATION

VAULT meets this requirement by providing robust school roster integration that enables students to be linked to schools, grades, classrooms, and instructional groups, supporting highly targeted outreach, reporting, and care coordination.

Comprehensive Student-to-School Linkage

VAULT supports detailed linkage of students to educational structures.

This includes:

- Association of students with schools, districts, and counties
- Linkage to grade levels and age-based cohorts
- Support for classroom- and teacher-level grouping

This level of granularity enables more precise identification of populations and supports targeted interventions within school environments.

Support for Population-Based Outreach and Reporting

By aligning health records with school roster data, VAULT enables jurisdictions to:

- Identify students with or without oral health records
- Analyze service gaps across schools, grades, and geographic regions

- Target outreach to specific classrooms, cohorts, or high-need populations

This supports data-driven decision-making and more effective delivery of school-based services.

Flexible Support for School-Based Workflows

VAULT's roster functionality is designed to support real-world school operations.

This includes:

- Ability to organize students by classroom, teacher, and grade
- Support for bulk operations (e.g., screenings, follow-ups, and documentation by group)
- Alignment with school-based clinic workflows and mobile health delivery models

This flexibility allows the system to adapt to a wide range of school health program needs.

Extensible Beyond Oral Health

While supporting oral health use cases, VAULT's roster integration is not limited to a single program area.

This includes:

- Support for immunizations, screenings, and other school-based health services
- Ability to capture and manage multiple types of clinical and community-based services
- Enablement of coordinated care across programs using a single, unified data model

This ensures that the State can expand beyond oral health to broader school and community health initiatives.

Proven Implementation Experience

VAULT has successfully implemented roster-based workflows in production environments.

In Maryland, VAULT supports school health programs by linking student records to schools and populations, enabling the State to:

- Track student populations across school systems
- Identify gaps in service delivery
- Conduct targeted outreach to underserved groups

This demonstrates VAULT's ability to operationalize school-based health workflows at scale.

Summary

VAULT provides advanced roster integration capabilities that support detailed student-to-school linkage, targeted outreach, and population-based reporting.

By enabling classroom-level organization and supporting a wide range of school-based health services, VAULT delivers a flexible and scalable solution that extends beyond oral health to support broader public health initiatives in educational settings.

4.2.2.7.2 DUAL WORKFLOWS

VAULT meets this requirement by supporting distinct, role-based workflows for different user types, enabling coordinated data capture and management across clinical, school-based, and community settings.

Workflow Support for Dental Professionals

VAULT enables dental professionals and clinical providers to document care directly within the system at the point of service.

This includes:

- Entry of oral health screenings, assessments, and treatments
- Real-time documentation during school-based or clinic-based encounters
- Association of services with specific students, schools, and populations

This ensures timely, accurate capture of care delivered in both fixed and mobile settings.

Workflow Support for School Nurses and Administrative Staff

VAULT supports workflows for school nurses and administrative users responsible for managing student records and historical data.

This includes:

- Entry of historical or externally provided oral health records
- Management and maintenance of school rosters
- Coordination of follow-up care and tracking of service status

This enables continuity of care and ensures that all relevant data is captured, even when services are delivered outside the IIS environment.

Coordinated, Multi-Role Workflow Model

VAULT's platform enables collaboration across user roles while maintaining data integrity and workflow clarity.

This includes:

- Role-based access and permissions aligned with user responsibilities
- Shared visibility into student records across clinical and school users
- Seamless coordination between screening, documentation, follow-up, and reporting

This ensures that multiple stakeholders can contribute to and utilize the same data in a coordinated manner.

Extensible Beyond Oral Health

VAULT's workflow model is not limited to oral health and can support a wide range of services delivered in school and community settings.

This includes:

- Health screenings (e.g., vision, hearing, behavioral health)
- Preventive and clinical services
- Community-based and mobile health initiatives

This flexibility enables the State to leverage the same platform across multiple programs without requiring separate systems.

Summary

VAULT provides flexible, role-based workflows that support coordinated data capture across dental professionals, school nurses, and other stakeholders.

By enabling real-time documentation, retrospective data entry, and cross-role collaboration, VAULT ensures that oral health and other school-based services can be effectively managed within a unified system.

4.2.2.7.2.1 DENTAL PROFESSIONAL WORKFLOW

VAULT meets this requirement by enabling dental professionals to document oral health services directly within the system at the point of care, ensuring timely, accurate, and standardized capture of clinical information.

Point-of-Care Documentation

VAULT supports real-time entry of oral health data by dental professionals in a variety of care settings.

This includes:

- Entry of oral health screenings, assessments, and treatment data
- Documentation during school-based clinics, community outreach events, and traditional clinical encounters
- Immediate association of services with individual students and school populations

This ensures that care delivered in the field is captured accurately and without delay.

Structured and Standardized Data Capture

VAULT provides structured data entry aligned with public health reporting and program requirements.

This includes:

- Standardized fields for screenings, findings, and treatment outcomes
- Consistent data capture across providers and locations
- Alignment with reporting and population health analysis needs

This ensures that collected data is usable for both operational and reporting purposes.

Support for High-Volume Screening Environments

VAULT is designed to support high-throughput care delivery environments.

This includes:

- Efficient workflows for rapid data entry during large-scale school-based screening programs
- Ability to capture data across large student populations in a single session
- Performance and usability optimized for mobile and community-based care settings

This enables providers to deliver care at scale without compromising data quality.

Integration with School-Based Workflows

VAULT integrates clinical workflows with school roster data to support population-based care delivery.

This includes:

- Linking services to specific students, classrooms, and schools
- Supporting batch or group-based workflows aligned with school operations
- Enabling coordinated tracking of services across student populations

This ensures that clinical activities are fully aligned with school-based program needs.

Summary

VAULT enables dental professionals to efficiently document oral health services at the point of care, supporting real-time, standardized, and high-volume data capture across school and community settings.

By integrating clinical workflows with school-based population data, VAULT provides a scalable solution that supports both service delivery and public health reporting.

4.2.2.7.2.2 SCHOOL NURSE WORKFLOW

VAULT meets this requirement by enabling school nurses and administrative staff to manage student populations, maintain records, and support ongoing care coordination within the Oral Health module.

Roster Management and Population Oversight

VAULT enables school nurses to manage and organize student populations through integrated roster functionality.

This includes:

- Management of student rosters by school, grade, classroom, and teacher
- Identification of students requiring screenings, follow-up care, or documentation updates
- Support for tracking service status across defined student populations

This allows school personnel to serve as a central point of coordination for school-based health activities.

Retrospective Data Entry and Record Maintenance

VAULT supports entry and maintenance of historical oral health records.

This includes:

- Documentation of services performed outside of the IIS (e.g., external providers, prior screenings)
- Updates to student records as new information becomes available
- Maintenance of complete and longitudinal health records over time

This ensures that student records remain comprehensive and accurate, regardless of where services are delivered.

Support for Continuity of Care and Follow-Up

VAULT enables school nurses to support ongoing care coordination and follow-up activities.

This includes:

- Tracking of students requiring additional services or referrals
- Monitoring of care status across school populations
- Coordination between schools, providers, and public health programs

This supports continuity of care and ensures that students receive appropriate follow-up services.

Integration with Broader School-Based Health Workflows

VAULT's workflow model supports a wide range of school-based health activities beyond oral health.

This includes:

- Integration with immunization tracking, screenings, and other health services
- Use of a unified student record across multiple programs
- Enablement of coordinated care delivery within school settings

This allows the State to leverage a single platform for multiple school-based health initiatives.

Summary

VAULT enables school nurses to manage student populations, maintain comprehensive records, and support coordinated follow-up care within school environments.

By combining roster management, retrospective data entry, and care coordination capabilities, VAULT ensures continuity of care and supports effective delivery of oral health and other school-based health services

4.2.2.7.3 REPORTING CAPABILITIES

VAULT meets this requirement by providing robust, multi-dimensional reporting capabilities that enable analysis of oral health data across student populations, schools, and geographic regions.

Population-Based Reporting

VAULT enables reporting across defined student populations.

This includes:

- Analysis by school, district, county, and State
- Reporting by grade level, age group, classroom, and teacher
- Identification of populations that have received services versus those who have not

This supports comprehensive visibility into service delivery across student populations.

Identification of Gaps and Disparities

VAULT enables users to identify gaps in oral health services and disparities across populations.

This includes:

- Detection of underserved schools, regions, or demographic groups
- Analysis of service coverage across different populations
- Support for equity-focused program evaluation

This allows jurisdictions to prioritize resources and target interventions effectively.

Integration with School and Clinical Data

VAULT integrates oral health data with school roster and student demographic information.

This includes:

- Linking services to student populations and school structures
- Combining clinical data with demographic and geographic data
- Supporting comprehensive analysis across multiple data domains

This ensures that reporting reflects both clinical activity and population context.

Actionable Insights for Program Management

VAULT's reporting capabilities support operational decision-making.

This includes:

- Identification of students requiring follow-up or additional services
- Monitoring of program performance over time
- Support for planning and evaluating outreach initiatives

Summary

VAULT provides comprehensive, multi-dimensional reporting capabilities that enable West Virginia to analyze oral health services across student populations, schools, and geographic regions.

By integrating oral health data with school roster and demographic information, the platform enables population-based reporting that reflects both clinical activity and real-world student populations.

VAULT supports identification of gaps in care and disparities across schools and communities, allowing the State to prioritize high-need populations and allocate resources effectively.

In addition, VAULT's reporting capabilities deliver actionable insights by identifying students requiring follow-up services, monitoring program performance over time, and supporting targeted outreach and intervention strategies.

Because these capabilities are built on a flexible and extensible platform, the same reporting framework can be applied beyond oral health to support a wide range of school-based and community health programs.

4.2.2.7.3.1 IDENTIFICATION OF STUDENTS WITH OR WITHOUT ORAL HEALTH RECORDS

VAULT meets this requirement by enabling users to identify students who have received oral health screenings as well as those who have not, supporting targeted outreach, follow-up, and program management.

Identification of Screened and Unscreened Students

VAULT allows users to distinguish between students who have received oral health services and those who remain unserved.

This includes:

- Identification of students who have completed screenings
- Identification of students who have not yet received services
- Visibility into screening status across defined student populations

Population-Based Gap Analysis

VAULT enables analysis of screening coverage across schools and student groups.

This includes:

- Identification of gaps in service delivery by school, grade, classroom, or geographic area
- Analysis of screening rates across populations
- Ability to prioritize high-need or underserved groups

Support for Targeted Outreach and Follow-Up

VAULT supports actionable use of screening data.

This includes:

- Targeting students or groups requiring outreach or follow-up
- Supporting coordination of additional screening events or services
- Tracking progress toward program goals and coverage targets

Summary

VAULT enables identification of students who have and have not received oral health screenings, supporting population-based analysis and targeted intervention.

By providing visibility into screening coverage and service gaps, VAULT enables West Virginia to ensure that all students have access to preventive services and supports effective program evaluation and improvement.

4.2.2.7.3.2 FILTERING AND PRIORITIZATION FOR OUTREACH

VAULT meets this requirement by enabling users to filter and analyze oral health data across multiple dimensions, allowing prioritization of outreach and services for high-need populations.

Multi-Dimensional Filtering Capabilities

VAULT supports flexible filtering across key population and program attributes.

This includes:

- School, district, and county-level filtering
- Grade, age group, classroom, and teacher-level segmentation
- Identification of urgency of care and service needs
- Combination of demographic and geographic criteria

This enables users to analyze data at varying levels of granularity and tailor reporting to specific program needs.

Prioritization of High-Need and Underserved Populations

VAULT enables public health officials to identify and prioritize populations requiring immediate attention.

This includes:

- Identification of students with urgent or unmet oral health needs
- Detection of underserved schools, regions, or demographic groups
- Support for equity-focused program planning and intervention

This ensures that resources are directed to populations with the greatest need.

Support for Targeted Outreach and Resource Allocation

VAULT's filtering capabilities support actionable program management.

This includes:

- Targeting specific student groups for outreach and follow-up services

- Planning school-based or community-based interventions
- Monitoring the impact of outreach efforts over time

This enables more effective and efficient delivery of services.

Summary

VAULT provides flexible filtering and prioritization capabilities that enable West Virginia to identify high-need populations and focus outreach efforts where they are most needed. By combining oral health data with demographic and geographic context, VAULT supports data-driven decision-making, equitable resource allocation, and improved access to care.

4.2.2.7.4 USER ACCESS AND PERMISSIONS

VAULT meets this requirement by providing a comprehensive, configurable role-based access control (RBAC) framework that governs access to oral health functionality, data, and workflows at a granular level, while enabling efficient administration across large user populations.

Role-Based Access for Oral Health Users

VAULT supports distinct role configurations for oral health participants, including dental professionals and school nurses, ensuring that each user type has access to the appropriate functionality.

4.2.2.7.4.1 Dental professionals are configured as providers within the system and are available within provider selection workflows (e.g., provider dropdowns), enabling them to document oral health services and access relevant patient records.

4.2.2.7.4.2 School nurses are granted role-based access to:

- View and manage school rosters
- Access oral health reports
- Support follow-up and care coordination activities
- Review historical oral health records

This role differentiation ensures that users can perform their responsibilities efficiently while maintaining appropriate data access controls.

Granular Permission Controls

4.2.2.7.4.3 VAULT enables administrators to assign specific capabilities through configurable permissions, including but not limited to:

- "Enable Oral Health Reports" — allows access to oral health reporting and analytics
- "Enable Health Service" — allows documentation and management of oral health services

Permissions can be assigned:

- At the individual user level
- At the role level for groups of users

This approach ensures flexibility while maintaining consistency across user populations.

Bulk Role Assignment and Management

VAULT supports efficient management of permissions across large user groups through bulk update capabilities.

- Administrators can assign or modify permissions using master role templates
- Bulk updates can be applied across multiple users simultaneously
- Role configurations can be reused and standardized across jurisdictions

This enables rapid onboarding and consistent permission management without manual, user-by-user configuration.

Administrative Control and Configuration

4.2.2.7.4.4 Jurisdictional administrators have full control over role and permission management, including the ability to:

- Create and define new roles
- Modify existing roles and associated permissions

- Activate or inactivate roles based on program needs
- Align access controls with State policies and governance requirements

All role and permission changes are applied in real time and can be adjusted as program requirements evolve.

Enforcement and Security Controls

VAULT enforces RBAC consistently across all system modules and workflows.

- Access to oral health functionality is restricted based on assigned roles and permissions
- Users only see and interact with features and data they are authorized to access
- Sensitive data is protected through least-privilege access principles

Additionally, the system maintains audit logs of role assignments and permission changes, providing traceability and supporting compliance with security and governance requirements.

Outcome for West Virginia

This approach provides West Virginia with:

- Precise control over user access to oral health functionality
- Efficient management of large user populations through bulk role updates
- Clear separation of responsibilities between dental professionals and school staff
- Secure, auditable access aligned with State policies

Requirement Response

VAULT MEETS THE REQUIREMENTS OF SECTION 4.2.2.8 BY DELIVERING A PRODUCTION-READY, STANDARDS-BASED FHIR R4 INTEROPERABILITY FRAMEWORK THAT ENABLES WEST VIRGINIA TO SECURELY EXCHANGE IMMUNIZATION DATA IN REAL TIME, SUPPORT BIDIRECTIONAL INTEGRATION WITH EXTERNAL SYSTEMS, AND INCREMENTALLY ADOPT MODERN INTEROPERABILITY STANDARDS WHILE MAINTAINING EXISTING HL7-BASED OPERATIONS.

Operational Workflow

1. External system (e.g., EHR, HIE, pharmacy) submits a FHIR request or query
2. VAULT's API layer authenticates and authorizes the request (OAuth2)
3. The system retrieves or processes immunization data in real time
4. CDS engine evaluates immunization status where applicable
5. FHIR resources (e.g., Immunization, ImmunizationRecommendation) are returned
6. Data is simultaneously available for reporting, analytics, and downstream workflows

VAULT delivers a modern, standards-based interoperability framework built on HL7 FHIR Release 4 (R4), enabling secure, real-time exchange of immunization data across healthcare and public health ecosystems.

The platform supports core FHIR resources, including Immunization and ImmunizationRecommendation, powered by an integrated clinical decision support engine that provides dynamic, ACIP-aligned forecasting. VAULT's interoperability capabilities are implemented through a secure, RESTful API architecture and are designed to operate in parallel with HL7 v2.5.1, allowing jurisdictions to transition to FHIR incrementally while maintaining compliance.

A clear, phased roadmap ensures scalable adoption, from foundational infrastructure through multi-jurisdictional interoperability aligned with national frameworks such as TEFCA. Comprehensive API documentation, developer tools, and onboarding support enable rapid and reliable integration with external partners.

Together, these capabilities ensure that the IIS is positioned to support current operational needs while evolving alongside federal and industry interoperability initiatives.

For West Virginia, this enables secure, real-time integration with providers, pharmacies, and public health partners while allowing the State to modernize interoperability capabilities without disrupting existing HL7 interfaces or reporting workflows.

What Sets VAULT Apart

VAULT delivers a production-ready, scalable, and operationally integrated FHIR framework that extends beyond data exchange to support real-time clinical decision support and public health workflows.

- **Real-Time Clinical Intelligence (Not Just Data Exchange)**
  VAULT integrates FHIR with a powerful clinical decision support engine, delivering real-time immunization forecasting and recommendations—not just data transport.
- **True Bidirectional, Event-Driven Interoperability**
  Supports both ingestion and generation of FHIR resources, enabling dynamic, two-way communication with EHRs, HIEs, pharmacies, and public health systems.
- **Parallel HL7 v2.5.1 + FHIR Strategy (Zero Disruption Transition)**
  Jurisdictions can adopt FHIR incrementally without risking compliance or disrupting existing interfaces. This parallel approach ensures continuity of existing provider integrations while enabling gradual adoption of FHIR, minimizing disruption to data submission, reporting, and operational workflows across the State.
- **Proven, Production-Ready Infrastructure**
  Core FHIR capabilities are already deployed within IISConnex, supporting real-world, multi-state interoperability today—not future concepts.
- **Developer-First Integration Model**
  Comprehensive API documentation, sandbox environments, and onboarding support significantly reduce integration time and complexity for partners.

- **Future-Proof, Modular Architecture**
  Designed to evolve with FHIR (R5+) and align with CDC, ONC, and TEFCA initiatives without requiring system rearchitecture.

These capabilities are already deployed in production environments supporting multi-state interoperability, ensuring that West Virginia is not adopting a future-state concept, but a proven, operational capability.

4.2.2.8.1 FHIR STANDARD SUPPORT

The PrepModEcosystem supports HL7 FHIR Release 4 (R4), the current industry standard for healthcare interoperability and the foundation for federal and national data exchange initiatives.

FHIR R4 support is implemented through a secure, RESTful API architecture that enables real-time data exchange using modern web standards (e.g., HTTPS, OAuth2, and token-based authentication). These APIs are purpose-built to support public health workflows, including immunization reporting, patient record access, and clinical decision support.

VAULT's FHIR APIs support a wide range of interoperability use cases, including:

- Provider and system queries for patient immunization histories and forecasts
- Patient access and engagement, enabling retrieval of immunization records
- Integration with external systems, including EHRs, HIEs, pharmacies, and digital health platforms
- Data exchange with public health partners, supporting bidirectional communication and reporting

VAULT's FHIR implementation is aligned with national implementation guides and CDC interoperability direction, ensuring consistency with evolving public health standards. The platform is designed to support parallel operation with HL7 v2.5.1 interfaces, allowing jurisdictions to maintain current compliance while incrementally adopting FHIR-based exchange.

The system architecture includes a modular interoperability layer, enabling the platform to evolve alongside future FHIR releases (e.g., R5) and emerging federal and jurisdictional requirements. Enhancements to FHIR capabilities can be introduced incrementally without disrupting existing integrations, workflows, or system performance.

4.2.2.8.2 REQUIRED RESOURCES

Enhanced Response (Incorporating + Strengthening Team Draft)

VAULT supports the key HL7 FHIR resources required for immunization data exchange, fully aligned with FHIR Release 4 (R4) and applicable national implementation guides.

Immunization Resource

VAULT implements the FHIR Immunization resource to represent vaccine administration events, including vaccine type (CVX), administration date, lot number, manufacturer, administering provider, and patient demographics.

The system supports both ingestion and generation of Immunization resources, enabling bidirectional exchange with external systems such as EHRs, pharmacies, HIEs, and public health partners. Immunization data is processed in real time and reconciled against existing patient records to maintain a complete and longitudinal immunization history.

ImmunizationRecommendation Resource

VAULT implements the FHIR ImmunizationRecommendation resource to deliver patient-specific forecasting and recommended actions based on ACIP guidelines and jurisdiction-specific rules. This capability is powered by VAULT's integrated clinical decision support (CDS) engine, which:

- Evaluates immunization histories in real time
- Applies ACIP schedules and configurable jurisdictional rules
- Generates up-to-date vaccine forecasts and next-dose recommendations
- Supports complex scenarios (catch-up schedules, contraindications, age/interval validation)

Recommendations are dynamically generated at the time of query or transaction, ensuring that providers and systems always receive the most current and clinically appropriate guidance.

Supporting Resources

In addition to core immunization resources, VAULT supports related FHIR resources required for comprehensive interoperability, including:

- **Patient** – for demographic and identity management
- **Practitioner** – for provider attribution
- **Organization** – for facility and jurisdictional context
- **Location** – for site-specific service delivery

These resources enable complete, context-rich data exchange across systems and support coordinated care and reporting across public health and clinical environments.

All resources are implemented in accordance with FHIR R4 specifications and applicable implementation guides, ensuring consistency with national interoperability standards and readiness for integration with a broad ecosystem of partners.

4.2.2.8.3 ROADMAP AND TIMELINE

VAULT provides a clear, phased, and actionable roadmap for FHIR adoption that aligns with both current operational requirements and long-term interoperability goals.

FHIR capabilities are implemented in parallel with existing HL7 v2.5.1 interfaces, enabling the State to maintain compliance with mandatory reporting requirements while incrementally expanding modern, standards-based interoperability.

The roadmap includes:

Phase 1 – Foundation (Current State)

Deployment of core FHIR infrastructure, including API gateway, authentication and authorization (e.g., OAuth2), and foundational FHIR resources.

These capabilities are already implemented and in active use within IISConnex, supporting multi-state interoperability and establishing a proven baseline for expansion.

Phase 2 – Expansion

Incremental implementation of additional FHIR resources and enhancement of bidirectional data exchange with EHRs, HIEs, pharmacies, and other partner systems.

This phase focuses on increasing interoperability coverage while maintaining system stability and performance.

Phase 3 – Scaling and Integration

Expansion of FHIR-based exchange across jurisdictions, enabling:

- Real-time data exchange at scale
- Cross-jurisdictional and interstate interoperability
- Alignment with national frameworks such as TEFCA and emerging federal interoperability initiatives

Phase 4 – Continuous Evolution

Ongoing enhancement of FHIR capabilities in alignment with:

- CDC and ONC guidance
- Updates to national implementation guides
- Future FHIR releases (e.g., R5 and beyond)

This ensures that the platform remains compliant, modern, and adaptable to evolving public health priorities.

VAULT's phased approach minimizes implementation risk by leveraging proven, production-ready capabilities while enabling jurisdictions to expand FHIR adoption in a controlled and scalable manner. Enhancements can be introduced incrementally without disruption to existing workflows or interfaces.

4.2.2.8.4 API DOCUMENTATION

VAULT provides comprehensive, publicly accessible API documentation for all FHIR endpoints to support seamless integration with the IIS and external partners.

API documentation is delivered through a centralized developer portal, providing a structured and user-friendly experience for integrators, developers, and partner organizations. Documentation includes:

- Endpoint specifications and supported operations (e.g., GET, POST, PUT, DELETE)
- Detailed resource definitions and FHIR-compliant data structures
- Authentication and authorization requirements, including OAuth2 and token-based access
- Sample requests and responses, including real-world immunization use cases
- Error handling frameworks and standardized response codes to support efficient troubleshooting

The developer portal is continuously maintained and version-controlled, ensuring that all documentation reflects current capabilities, enhancements, and updates to FHIR standards and implementation guides.

To support successful integration, VAULT provides a full developer enablement environment, including:

- Sandbox environments for testing and validation
- API testing tools and utilities
- Technical onboarding support, including guidance from implementation specialists
- Clear versioning and backward compatibility strategies, allowing partners to adopt updates without disruption

This approach ensures that integration partners can rapidly and confidently connect to VAULT, reducing onboarding time and minimizing implementation risk.

4.2.3 MANDATORY PROJECT REQUIREMENTS

VAULT will comply with all mandatory project requirements as defined in Attachment B – IIS Baseline Requirements RTM. A complete and detailed response to each requirement has been provided within the RTM, including support for both required and optional functionality.

The PrepModEcosystem, anchored by OptimIIS, is a proven, production-ready platform that has been purpose-built to support statewide immunization programs and is already operating in environments with comparable regulatory, operational, and technical requirements. This approach reduces implementation risk and ensures rapid time to value.

VAULT's methodology emphasizes traceability and accountability, with each requirement mapped directly to system capabilities and implementation activities within the RTM. This ensures that all requirements are addressed, validated, and verifiable by evaluators.

The platform is built on a standards-based, configurable architecture aligned with federal and industry requirements, including HL7, FHIR, NIST, HIPAA, and CDC IIS Functional Standards. This enables consistent compliance while allowing flexibility to meet jurisdiction-specific needs.

In addition to meeting mandatory requirements, VAULT's solution exceeds expectations in several key areas:

- **Scalability and Performance** – Supports high transaction volumes, large user populations, and millions of records without performance degradation
- **Advanced Interoperability** – Extends beyond baseline requirements through IISConnex and FHIR-based APIs, enabling real-time, bidirectional exchange and alignment with national frameworks such as TEFCA
- **Continuous Innovation** – Microservices-based architecture supports ongoing enhancements without disruptive system upgrades
- **Integrated Ecosystem** – Combines IIS functionality with scheduling, outreach, billing, and emergency response capabilities to improve operational efficiency
- **Proven Implementation Model** – Phased, collaborative approach supported by experience in multi-jurisdiction deployments

VAULT recognizes that compliance is an ongoing responsibility. The platform is continuously monitored, maintained, and enhanced to remain aligned with evolving standards, regulations, and public health priorities.

4.2.3.1 IIS BASELINE REQUIREMENTS RTM

VAULT Technologies confirms that the proposed solution fully meets the essential requirements outlined in Attachment B – IIS Baseline Requirements RTM, as defined by the CDC and incorporated into this Solicitation.

As part of this submission, VAULT has completed all required fields within Attachment B, including all sections and all columns designated for Vendor Response. This includes responses for both required and optional functionality, ensuring comprehensive coverage of all baseline IIS capabilities.

The completed RTM reflects VAULT's alignment with CDC IIS Functional Standards and demonstrates how the PrepModEcosystem, including OptimIIS and IISConnex, satisfies each requirement through existing, production-ready functionality. Responses are detailed, specific, and mapped directly to system capabilities, ensuring that evaluators can clearly verify compliance.

VAULT confirms that the following RTM sections have been fully completed and are included as part of the Technical Proposal submission:

- 4.2.3.1.1 Administer System
- 4.2.3.1.2 Manage Organizations and Facilities
- 4.2.3.1.3 Manage Users
- 4.2.3.1.4 Support Interoperability
- 4.2.3.1.5 Ensure Data Quality
- 4.2.3.1.6 Evaluate and Forecast
- 4.2.3.1.7 Manage Patient and Immunization Record
- 4.2.3.1.8 Manage Vaccine Inventory
- 4.2.3.1.9 Provide Data Access
- 4.2.3.1.10 Non-functional Requirements

In accordance with the Solicitation requirements, VAULT will provide printed, bound physical copies of the completed RTM as part of the Technical Proposal submission. These materials will be formatted to ensure clarity, legibility, and ease of review, enabling evaluators to readily verify compliance with each requirement.

The RTM is structured to provide clear traceability between requirements and system functionality, supporting efficient evaluation and validation. Each response is written to demonstrate not only compliance, but also how VAULT's solution meets or exceeds the intent of the requirement based on real-world implementation experience.

Through this approach, VAULT ensures full compliance with Attachment B while providing the Agency with a transparent, verifiable, and comprehensive view of system capabilities.

4.2.3.2 SYSTEM COMPATIBILITY REQUIREMENTS

VAULT's system compatibility approach ensures that the IIS is accessible, reliable, and easy to use across a wide range of environments. As a fully cloud-based, browser-accessible solution, the platform requires no specialized hardware, software installation, or elevated permissions. This approach minimizes technical barriers, simplifies deployment, and enables rapid adoption by diverse user groups while reducing ongoing IT overhead for the State.

4.2.3.2.1 CLOUD-BASED SOFTWARE WITH VENDOR-PROVIDED HOSTING

VAULT complies with this requirement.

The VAULT solution is a fully cloud-based, vendor-hosted platform in AWS, managed by VAULT Technologies within a secure, scalable cloud infrastructure. VAULT is responsible for all aspects of hosting, including infrastructure provisioning, system monitoring, maintenance, and updates.

The platform is designed to deliver high availability, fault tolerance, and scalable performance, ensuring reliable system access under both routine operations and peak demand scenarios, such as mass vaccination events.

4.2.3.2.2 COMPATIBILITY WITH MAJOR WEB BROWSERS

VAULT complies with this requirement.

The system is fully compatible with all major, current web browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari. VAULT designs, tests, and validates the platform to ensure consistent functionality and performance across supported browsers.

Browser compatibility is verified as part of the standard development and release process, ensuring reliable access for users regardless of browser preference.

4.2.3.2.3 OPERATION ON STANDARD DESKTOP AND LAPTOP ENVIRONMENTS

VAULT complies with this requirement.

The PrepModEcosystem operates efficiently on standard desktop and laptop computers and does not require specialized hardware. The system is delivered through a lightweight, browser-based interface that supports a responsive user experience with minimal resource requirements.

This approach enables broad accessibility, including for users in resource-constrained environments, and simplifies deployment by eliminating the need for additional hardware or device configuration.

4.2.3.2.4 ACCESS WITHOUT ELEVATED PERMISSIONS OR LOCAL INSTALLATION

VAULT complies with this requirement.

The system is accessed through a standard web browser and does not require local software installation or elevated user permissions. All application functionality is delivered through a secure, browser-based interface.

This approach simplifies deployment, reduces reliance on IT support, and enables rapid onboarding of users across a wide range of environments, including healthcare settings, schools, and community-based organizations.

Centralized application management within the hosted environment ensures that updates and security patches are applied consistently without requiring end-user intervention.

4.2.3.3 SERVICE LEVEL AGREEMENT (SLA)

VAULT will comply with all Service Level Agreement (SLA) requirements as defined in **Attachment C**, including those related to system availability, support responsiveness, issue resolution, reporting, and performance monitoring.

VAULT's service delivery model is designed to support a highly available, secure, and operationally dependable Immunization Information System. The platform is supported through a structured operational framework that includes continuous system monitoring, formal issue management, defined escalation procedures, and regular performance reporting.

VAULT will support the State's requirement for 24/7/365 system availability with a minimum monthly uptime of 99.9%. The hosting model leverages resilient cloud infrastructure, redundancy, and proactive monitoring to maintain system stability and minimize downtime. Scheduled maintenance will be coordinated with the State and performed outside of standard business hours.

VAULT will align its support operations with the State's severity-based response and resolution framework, ensuring that critical issues receive immediate attention and that all incidents are managed according to defined service levels. A formal issue tracking and defect management process will be used to log, prioritize, resolve, and report all issues.

VAULT will provide the required monthly SLA reporting, including system availability, support performance, issue resolution metrics, and corrective actions where applicable. This ensures transparency, accountability, and continuous service improvement.

Overall, VAULT's SLA approach combines resilient infrastructure, disciplined support operations, and measurable performance management to ensure compliance with State requirements and reliable day-to-day system performance.

4.2.3.4 MAINTENANCE AND SUPPORT

VAULT's maintenance and support services provide a comprehensive framework for ensuring system reliability, security, and continuous improvement. Through structured support processes, proactive monitoring, controlled release management, and ongoing documentation updates, VAULT ensures that the IIS remains stable, secure, and aligned with evolving public health requirements.

This approach enables the State to operate the system with confidence, supported by a mature and responsive maintenance and support model.

4.2.3.4.1 HELP DESK SUPPORT AND ESCALATION PROCEDURES

VAULT complies with this requirement.

VAULT provides live help desk support during standard business hours (Monday–Friday, 8:00 AM–5:00 PM local time), with documented intake, triage, and escalation procedures. Support is accessible through multiple channels, including phone, email, and a ticketing system.

Issues are categorized by severity and routed to appropriate technical resources to ensure timely resolution. VAULT's escalation framework ensures that critical issues receive immediate attention, with structured communication and status updates provided throughout the resolution process.

VAULT also offers extended support coverage, including evenings and weekends, for critical issues and high-demand periods.

4.2.3.4.2 BUG FIXES AND SECURITY PATCHING

VAULT complies with this requirement.

VAULT delivers bug fixes and security patches in accordance with industry best practices and defined service levels. Critical vulnerabilities are prioritized and addressed promptly, particularly those impacting system security, availability, or data integrity.

Updates are managed through a structured release management process that includes testing, validation, and controlled deployment. Emergency patches may be deployed outside of standard release cycles to address urgent issues.

VAULT continuously monitors for emerging security threats to ensure that the system remains secure and compliant with applicable standards.

4.2.3.4.3 SYSTEM PERFORMANCE MONITORING AND PROACTIVE ISSUE RESOLUTION

VAULT complies with this requirement.

VAULT provides continuous monitoring of system performance across all hosted and managed environments, including system health, application performance, infrastructure utilization, and interface activity.

Proactive alerting mechanisms are used to identify and address potential issues before they impact users. This includes performance tuning, capacity management, and early resolution of emerging issues.

This approach supports high system availability and a consistent user experience, including during periods of increased demand.

4.2.3.4.4 VERSION UPGRADES AND COMPATIBILITY ASSURANCE

VAULT complies with this requirement.

VAULT provides regular version upgrades and enhancements to ensure that the system remains aligned with evolving technology standards, CDC guidance, and jurisdictional requirements.

Upgrades are managed through a structured release process that includes testing, validation, and stakeholder communication. The platform's architecture supports seamless updates with minimal disruption to users.

VAULT maintains ongoing compatibility with federal and industry standards, including HL7 messaging requirements and emerging interoperability frameworks such as FHIR, ensuring long-term alignment with national initiatives.

VAULT has successfully implemented a continuous delivery model in existing state deployments, enabling regular system enhancements without requiring disruptive system overhauls.

4.2.3.4.5 DOCUMENTATION UPDATES

VAULT complies with this requirement.

VAULT maintains and updates system documentation to reflect changes made during the maintenance period, including technical documentation, user guides, configuration details, and operational procedures.

Documentation updates are delivered alongside system enhancements, ensuring that users and administrators have access to current and accurate information to support system use, training, and ongoing operations.

4.2.3.5 DATA STORAGE

VAULT provides a secure, compliant, and resilient data management and recovery framework designed to protect IIS data and ensure continuous system availability. All data, including production data, backups, logs, and recovery environments, is stored and maintained exclusively within U.S.-based infrastructure, in full alignment with federal and state data residency requirements.

VAULT's Business Continuity and Disaster Recovery (BCP/DR) capabilities are built on a structured, standards-based approach aligned with NIST SP 800-34 and related federal guidance. The platform supports reliable backup, failover, and recovery processes, combined with annual testing, formal reporting, and continuous plan updates to ensure operational readiness.

Through this approach, VAULT ensures that the IIS remains secure, available, and recoverable under a wide range of scenarios, including system failures, infrastructure disruptions, and public health emergencies, while maintaining compliance with all applicable regulatory and program requirements.

🚀 **What Sets VAULT Apart**

- **Strict U.S.-Only Data Residency (End-to-End Enforcement)**
  All IIS data—including backups, failover environments, and DR operations—is confined to U.S.-based infrastructure, ensuring full compliance under all operating conditions.
- **Proven, Cloud-Native Resilience**
  Built on modern, redundant cloud architecture designed for high availability, rapid recovery, and seamless scalability during peak demand and emergency events.
- **Operationalized BCP/DR (Not Just Plans on Paper)**
  Regular testing, real-world failover capabilities, and structured reporting ensure that continuity plans are actionable, validated, and continuously improved.
- **Standards-Aligned and Continuously Maintained**
  Alignment with NIST and federal guidance is maintained throughout the contract lifecycle, with updates driven by testing outcomes, incidents, and system changes.
- **Integrated Monitoring and Rapid Response**
  Continuous system monitoring and proactive alerting enable early detection and rapid mitigation of potential disruptions before they impact users.
- **Designed for Public Health Continuity**
  The platform is engineered to support uninterrupted immunization operations, reporting, and data exchange—even during large-scale public health events.

4.2.3.5.1 BUSINESS CONTINUITY AND DISASTER RECOVERY (BCP/DR)

VAULT's Business Continuity and Disaster Recovery approach is structured, standards-aligned, and continuously maintained. Through documented plans, NIST-aligned frameworks, annual testing, U.S.-based recovery operations, and ongoing updates, VAULT ensures that the IIS environment remains resilient, recoverable, and compliant with federal and state requirements.

4.2.3.5.1.1 PLAN DOCUMENTATION

VAULT complies with this requirement.

VAULT maintains formal Business Continuity Plan (BCP) and Disaster Recovery (DR) documentation, including detailed procedures for system recovery, data restoration, and operational continuity. These plans will be provided to the Agency within 60 calendar days of contract execution and upon request thereafter.

Documentation includes system architecture, recovery processes, roles and responsibilities, and escalation procedures, ensuring clarity and transparency for stakeholders.

4.2.3.5.1.2 NIST ALIGNMENT

VAULT complies with this requirement.

VAULT's Business Continuity Plan (BCP) and Disaster Recovery (DR) plans are aligned with NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems), or its successor publications. These plans are maintained and updated throughout the contract term to ensure continued alignment with federal and state requirements.

This alignment supports consistent implementation of contingency planning, risk assessment, and recovery strategies in accordance with recognized standards.

4.2.3.5.1.3 ANNUAL TESTING

VAULT complies with this requirement.

VAULT conducts annual BCP/DR testing, including tabletop exercises and live failover scenarios where appropriate, to validate recovery procedures and system restoration capabilities.

Following each test, VAULT documents results, identifies corrective actions, and will provide a summary report to the Agency within 30 calendar days of test completion. Reports include findings, remediation actions, and associated timelines.

4.2.3.5.1.4 U.S. DATA RESIDENCY

VAULT complies with this requirement.

All BCP/DR activities, including backups, failover environments, and recovery operations, are conducted within U.S.-based infrastructure in accordance with data residency requirements. VAULT ensures that all replication and recovery environments adhere to the same U.S.-only data residency standards as production systems.

This approach ensures that IIS data is not transmitted, processed, or stored outside U.S. jurisdiction under any operational scenario, including disaster recovery events.

4.2.3.5.1.5 CONTINUOUS IMPROVEMENT

VAULT complies with this requirement.

VAULT maintains a continuous improvement approach to BCP/DR planning. Plans are updated based on lessons learned from testing, operational incidents, and changes to the system or hosting environment.

VAULT will update BCP/DR plans within 60 calendar days of such events to ensure that recovery strategies remain current and aligned with system architecture and operational needs.

4.2.3.5.1.6 CERTIFICATION

VAULT complies with this requirement.

VAULT performs regular reviews to ensure that BCP/DR plans remain current, tested, and compliant with applicable federal and state requirements. VAULT will provide annual certification to the Agency confirming that these plans meet all required standards.

4.2.3.6 DATA OWNERSHIP

VAULT's data ownership and management approach ensures that the Agency retains full ownership and control of all IIS data throughout the contract lifecycle. Through strict ownership policies, strong security safeguards, complete data portability, structured transition support, and secure data destruction practices aligned with federal standards, VAULT provides a transparent and compliant framework for managing Agency data.

This approach minimizes vendor lock-in, supports long-term sustainability, and ensures that the Agency can confidently manage, access, and transition its data as needed.

4.2.3.6.1 AGENCY OWNERSHIP OF ALL DATA

VAULT recognizes that all data within the IIS is the sole property of the Agency. This includes all information submitted by providers, partners, and external systems, as well as data generated through system use, analytics, and reporting.

VAULT's role is limited to hosting, managing, and processing this data in accordance with Agency direction and contractual obligations. At no point does VAULT assert control or ownership over the data.

4.2.3.6.2 DATA COLLECTED ON BEHALF OF THE AGENCY

VAULT complies with this requirement.

All data related to the execution of this contract is collected on behalf of, and remains the sole property of, the Agency at all times.

VAULT stores and manages this data in accordance with Agency direction and contractual obligations, ensuring that it is accessible for Agency use, reporting, and operations while maintaining appropriate security and access controls.

4.2.3.6.3 PRIVACY AND SECURITY SAFEGUARDS

VAULT complies with this requirement.

VAULT implements strict privacy and security safeguards to protect all IIS data from unauthorized use or disclosure for any purpose other than those defined in this solicitation and authorized by the Agency.

These safeguards include role-based access controls, encryption of data at rest and in transit, audit logging, and continuous system monitoring.

Access to data is limited to authorized personnel based on least-privilege principles, and all personnel are subject to security and confidentiality requirements to ensure that data is used solely for approved purposes.

4.2.3.6.4 DATA RETURN AND PORTABILITY

VAULT complies with this requirement.

VAULT will return the entire IIS dataset to the Agency upon request or upon contract termination, at no additional cost and in a format specified by the Agency.

Data can be provided in standardized, non-proprietary formats such as HL7, CSV, XML, or other agreed-upon structures. VAULT will also provide supporting materials, including data dictionaries, schema definitions, and interface specifications, to ensure data usability and accessibility.

This approach enables a complete and seamless transition of data to the Agency or a subsequent vendor without disruption.

4.2.3.6.5 TRANSITION SUPPORT AND COOPERATION

VAULT complies with this requirement.

In the event of contract termination, VAULT will cooperate fully with the Agency and any subsequent vendor to ensure a smooth and secure transition. VAULT will deliver all data, documentation, and associated work products to the Agency or its designee within thirty (30) working days of receipt of notice of contract termination.

VAULT will also provide reasonable transition support, including knowledge transfer and coordination, to minimize disruption to system operations and public health activities.

4.2.3.6.6 SECURE DATA DESTRUCTION

VAULT complies with this requirement.

Upon written authorization from the Agency, VAULT will securely destroy all Agency data in accordance with NIST SP 800-88 (Guidelines for Media Sanitization) and applicable industry standards.

Data destruction will include all copies of data across production systems, backups, and associated storage environments. VAULT will complete all destruction activities within thirty (30) working days of authorization and will provide formal certification confirming that all data has been permanently removed and cannot be recovered.

4.2.3.7 GENERAL PROJECT REQUIREMENTS

VAULT's approach to project planning and execution is structured, transparent, and aligned with Agency governance requirements. Through a collaboratively developed Project Plan, controlled change management processes, and clearly defined milestones tied to objective acceptance criteria, VAULT ensures disciplined project delivery and full alignment with Agency expectations.

Payments are strictly linked to verified milestone completion and formal Agency approval, with no fees incurred prior to full system acceptance. This approach reinforces accountability, prevents unauthorized changes, and ensures that progress is measurable and outcomes are fully validated.

Together, these practices provide a controlled and low-risk implementation framework that supports predictable delivery, financial transparency, and successful project outcomes.

4.2.3.7.1 FINALIZED PROJECT PLAN AND SCHEDULE

VAULT complies with this requirement.

VAULT will develop a comprehensive Project Plan and Implementation Schedule aligned with the Implementation Plan described in Section 4.2.2.2. The finalized Project Plan and Schedule will be submitted to the Agency for review and approval and will serve as the governing document for project execution.

The Project Plan will include detailed timelines, task dependencies, resource assignments, deliverables, and communication protocols, ensuring that all project activities are traceable, measurable, and aligned with agreed-upon objectives.

VAULT's approach emphasizes structured planning and close collaboration with the Agency to support predictable delivery and successful implementation outcomes.

4.2.3.7.2 CHANGE CONTROL AND DEVIATION MANAGEMENT

VAULT complies with this requirement.

VAULT will not deviate from the approved Implementation Plan without prior written approval from the Agency. Any proposed changes will be formally documented, justified, and submitted for Agency review and approval before execution.

VAULT follows a structured change management process to evaluate the impact of proposed changes on scope, schedule, cost, and risk, ensuring transparency and continued alignment with project objectives.

4.2.3.7.3 MILESTONE-BASED IMPLEMENTATION AND PAYMENT STRUCTURE

VAULT's milestone and payment approach ensures clear accountability, transparency, and alignment with Agency expectations. Milestones are jointly defined, formally approved, and tied to objective acceptance criteria, with all payments contingent upon verified completion and formal Agency approval.

This structured approach enforces disciplined project execution, prevents unauthorized changes, and ensures that the Agency incurs costs only for fully completed and accepted deliverables, minimizing financial risk and supporting successful project outcomes.

4.2.3.7.3.1 MILESTONE DEFINITION AND APPROVAL

VAULT complies with this requirement.

VAULT will collaborate with the Agency during the initial planning sessions to jointly define all implementation milestones. Each milestone will be documented in the Project Plan and will include:

- A clear description of required deliverables
- Objective and measurable acceptance criteria
- Documentation requirements
- A proposed payment amount tied to the milestone

Milestones will not be considered valid until formally approved in writing by the Agency.

4.2.3.7.3.2 NO UNILATERAL CHANGES

VAULT complies with this re dify, subdivide, or consolidate milestones, nor alter milestone definitions or associated paym quirement.

VAULT will not add, remove, moent amounts, without prior written approval from the Agency. All proposed changes will follow a formal change management process and will be submitted for Agency review and approval before implementation.

4.2.3.7.3.3 VERIFICATION BEFORE PAYMENTS

VAULT complies with this requirement.

VAULT will ensure that all milestone deliverables are fully completed and meet all defined acceptance criteria prior to submission for Agency verification. No payment will be invoiced or due until the Agency has verified completion and provided formal written approval of the milestone.

VAULT will support Agency validation activities, including testing, documentation review, and stakeholder sign-off, to confirm successful completion.

4.2.3.7.3.4 NO PARTIAL OR CONDITIONAL PAYMENTS

VAULT complies with this requirement.

VAULT will not invoice or receive final implementation payment until the IIS solution has been fully implemented, is operational, and has received formal written acceptance by the Agency. Final payment is contingent upon complete system delivery and confirmation that all acceptance criteria have been satisfied.

4.2.3.7.3.5 NO RECURRING FEES BEFORE FINAL ACCEPTANCE

VAULT complies with this requirement.

VAULT will not assess or invoice any recurring, subscription, hosting, maintenance, or support fees until the IIS solution has been fully implemented, is operational, and has received formal written acceptance by the Agency.

4.2.3.7.3.6 MILESTONE FAILURE AND REMEDIATION

VAULT complies with this requirement.

If a milestone is not successfully completed, VAULT will remediate all identified deficiencies at no additional cost to the Agency and resubmit the milestone for Agency review and verification. VAULT will cooperate fully with the Agency in any required retesting or review activities to confirm successful remediation.

4.2.3.7.4 LIQUIDATED DAMAGES FOR IMPLEMENTATION DELAYS

VAULT complies with this requirement.

VAULT acknowledges the Agency's right to assess liquidated damages for implementation delays in accordance with the terms outlined in this section and will adhere to all applicable provisions.

4.2.3.8 VENDOR STAFFING

VAULT complies with this requirement.

VAULT will provide qualified and experienced staffing resources to support all phases of the IIS implementation, including system configuration, customization, testing, training, and go-live support. Personnel are assigned based on role-specific expertise to ensure successful delivery. VAULT's hiring and staffing practices comply with all applicable State requirements, including the West Virginia Office of Technology (WVOT) policies and the Office of Management Information Services (OMIS) background check policies and procedures. All personnel are properly vetted, trained, and authorized prior to accessing Agency systems or data.

4.2.3.8.1 COMPLIANCE WITH WV OFFICE OF TECHNOLOGY POLICIES

VAULT complies with this requirement.

VAULT adheres to all applicable West Virginia Office of Technology (WVOT) policies governing information security, access control, contractor management, and system usage. These include requirements related to account management, data protection, acceptable use, change management, and security monitoring.

VAULT aligns its internal security and operational policies with these standards to ensure that all personnel assigned to the project operate in compliance with State requirements.

4.2.3.8.2 COMPLIANCE WITH OMIS POLICY #0529 (BACKGROUND CHECKS)

VAULT complies with this requirement.

VAULT adheres to OMIS Policy #0529 and ensures that all personnel with access to State systems or sensitive data undergo required background checks, including fingerprint-based state and federal checks, prior to being granted system access.

VAULT incorporates these requirements into its onboarding process and ensures that all assigned personnel are properly screened, that documentation is maintained and provided as required, and that only eligible personnel are authorized to access the system.

4.2.3.8.3 COMPLIANCE WITH OMIS PROCEDURE OP-35 AND APPENDIX A

VAULT complies with this requirement.

VAULT adheres to OMIS Procedure OP-35 and Appendix A for vendor and contractor background checks, including fingerprint-based identity verification and state and federal (FBI) background investigations.

VAULT ensures that all personnel complete required background checks and receive favorable adjudication prior to being granted access to State systems or data. VAULT coordinates all required background check activities and maintains compliance with applicable State and federal requirements.

4.2.3.9 PROJECT MANAGER

VAULT complies with this requirement.

VAULT will assign a dedicated Project Manager to lead and oversee all aspects of the IIS implementation in close coordination with the Agency's designated Project Manager. This collaborative governance model ensures clear communication, shared accountability, and alignment throughout the project lifecycle.

The VAULT Project Manager will be responsible for day-to-day project execution, including planning, resource coordination, schedule management, risk mitigation, stakeholder communication, and delivery of all project milestones. The Project Manager will serve as the primary point of contact for the Agency and will ensure that all project activities are transparent, well-documented, and aligned with the approved Project Plan.

Dr. Montressa Washington, PMP will serve as VAULT's Project Manager for this engagement. Dr. Washington brings more than 20 years of experience in project management and public health systems and is a certified Project Management Professional (PMP). She has extensive experience leading complex, large-scale implementations requiring cross-functional coordination, compliance adherence, and structured delivery.

In this role, Dr. Washington will:

- Coordinate closely with the Agency's Project Manager to ensure alignment on priorities, timelines, and deliverables
- Lead regular project status meetings and milestone reviews
- Manage the project schedule and track dependencies
- Identify and mitigate risks through structured risk management practices
- Ensure adherence to quality, security, and compliance standards
- Facilitate issue resolution and escalation as needed

VAULT's project management approach emphasizes proactive communication, disciplined execution, and strong Agency collaboration to support successful implementation outcomes.

4.2.3.10 COMPREHENSIVE AND ROLE-SPECIFIC TRAINING PLAN

VAULT's training program is designed to support both immediate user readiness and long-term success. Through role-based training, comprehensive digital resources, and structured post-implementation support, VAULT ensures that all users achieve and maintain proficiency throughout the contract term.

This approach promotes strong user adoption, improved data quality, and consistent system usage across all stakeholder groups.

4.2.3.10.1 ROLE-SPECIFIC TRAINING STRATEGY

VAULT complies with this requirement.

VAULT provides role-specific training tailored to the distinct responsibilities and workflows of each user group. Training content, format, and depth are customized to ensure that each role gains the knowledge and skills required to effectively use the system in daily operations.

4.2.3.10.1.1 OEPS / AGENCY ADMINISTRATORS

Training focuses on system configuration, user and role management, data quality monitoring, advanced reporting, and overall system oversight. Administrators are also trained on audit functionality, interface monitoring, and governance processes to support statewide program management.

4.2.3.10.1.2 PROVIDER OFFICE STAFF / END USERS

Training emphasizes day-to-day workflows, including patient search and registration, immunization entry, clinical decision support usage, and basic troubleshooting. Instruction is practical and workflow-driven to enable users to become productive quickly in real-world scenarios.

4.2.3.10.1.3 SCHOOL NURSES / PUBLIC HEALTH PARTNERS

Training focuses on roster management, exemption tracking, school-based workflows, and public health follow-up activities. Users are trained to manage defined populations, monitor compliance, and support outreach and reporting efforts.

All training incorporates real-world use cases, system demonstrations, and guided exercises to reinforce learning and support knowledge retention.

4.2.3.10.2 TRAINING DELIVERABLES

VAULT complies with this requirement.

VAULT provides a comprehensive set of training materials and resources to support all user roles. All materials are maintained in digital formats to ensure accessibility, ease of distribution, and timely updates.

Training materials include:

4.2.3.10.2.1 ON-DEMAND VIDEO INSTRUCTIONS OR DEMONSTRATIONS FOR EACH USER ROLE.

On-demand video training modules tailored to each user role, including system walkthroughs, step-by-step demonstrations, and key workflow explanations

4.2.3.10.2.2 DIGITAL USER GUIDES OR MANUALS

Digital user guides and manuals with detailed instructions, screenshots, and reference materials to support both functional and technical users

Quick reference guides and job aids designed to support common tasks and reinforce key workflows

All training materials are regularly updated to reflect system enhancements, policy changes, and evolving user needs.

4.2.3.10.3 POST-IMPLEMENTATION SUPPORT AND REFRESHERS

VAULT complies with this requirement.

VAULT provides structured post-implementation support to ensure a smooth transition following Go-Live and sustained user adoption.

4.2.3.10.3.1 POST-IMPLEMENTATION SUPPORT

VAULT provides a defined period of enhanced support following Go-Live, focused on resolving user adoption challenges and reinforcing training concepts. This support includes:

- Dedicated resources to assist users and respond to questions in real time
- Additional training sessions based on user needs and feedback
- Reinforcement of key workflows and best practices
- Close coordination with the Agency to monitor adoption and address gaps

4.2.3.10.3.2 ANNUAL TRAINING REFRESHERS

VAULT provides ongoing refresher training to ensure continued user proficiency as the system evolves. Refresher training is offered annually and on demand, particularly when new features are introduced, system updates occur, or regulatory requirements change.

Updated training materials are delivered alongside system enhancements to ensure users have access to current and accurate information.

4.2.3.11 PRIVACY

VAULT's privacy framework is designed to ensure full compliance with State and Federal requirements while maintaining strict control, transparency, and accountability over all IIS data. VAULT adheres to applicable privacy laws and regulations, including HIPAA, and enforces comprehensive safeguards governing data access, use, storage, and transmission.

The system provides robust audit logging, controlled access to sensitive information, and immediate incident response aligned with State-defined procedures. VAULT enforces strict data use restrictions, ensuring that Agency data is not used, disclosed, or repurposed without explicit authorization.

In addition, VAULT meets all required certifications and disclosure obligations, providing the Agency with assurance of organizational integrity, security posture, and compliance with all applicable standards.

This approach ensures that IIS data is protected, auditable, and managed in a manner that supports regulatory compliance, operational trust, and long-term program integrity.

4.2.3.11.1 COMPLIANCE WITH PRIVACY LAWS AND REGULATIONS

VAULT complies with this requirement.

VAULT complies with all applicable State and Federal data privacy laws, regulations, and policies, including the HIPAA Privacy and Security Rules and applicable state data protection requirements.

VAULT maintains documented policies and procedures governing the collection, use, access, storage, and transmission of data. These policies are reviewed regularly and updated to align with evolving regulatory requirements and industry best practices.

All personnel with access to sensitive data are trained on applicable privacy requirements and are required to adhere to strict confidentiality and acceptable use policies.

4.2.3.11.2 AUDIT LOGGING AND MONITORING

VAULT complies with this requirement.

The IIS maintains a comprehensive and tamper-resistant audit logging capability that records all user access and activity, including logins, data additions, modifications, deletions, and exports. Audit logs are retained in accordance with Agency requirements, including support for a minimum six (6) year retention period. VAULT provides audit logs to the Agency at designated timeframes and upon request to support compliance monitoring and investigation activities. Access to audit logs is restricted to authorized personnel, and all access to audit logs is itself logged and monitored.

4.2.3.11.3 INCIDENT RESPONSE AND BREACH NOTIFICATION

VAULT complies with this requirement.

In the event of a suspected or confirmed data breach, VAULT will immediately follow the processes outlined in the most current version of the Office of Management Information Services (OMIS) Incident Reporting and Response Procedures.

VAULT will initiate incident response activities, including containment, investigation, impact assessment, and coordination with the Agency to ensure timely reporting and compliance with all applicable requirements.

4.2.3.11.4 RESTRICTIONS ON DATA USE AND DISCLOSURE

VAULT complies with this requirement.

VAULT will not use, release, disclose, or otherwise make available any Agency data for any purpose not explicitly authorized under this contract without prior written approval from the Agency.

This restriction applies to all data, including de-identified, aggregated, and limited datasets.

VAULT does not sell, license, or otherwise monetize Agency data.

4.2.3.11.5 CERTIFICATION OF NO ACTIVE INVESTIGATIONS

VAULT complies with this requirement.

VAULT certifies that it is not currently under investigation by any state or federal authority for a breach of data security.

4.2.3.11.6 DISCLOSURE OF PRIOR INCIDENTS

VAULT complies with this requirement.

VAULT certifies that it has not been involved in any breach of data security.

4.2.3.11.7 DISCLOSURE OF INVESTIGATIONS AND CORRECTIVE ACTIONS

VAULT complies with this requirement.

VAULT certifies that it has not been subject to any prior or current investigations by any state or federal authority related to privacy or security of patient information.

4.2.3.11.7.1 DISCLOSURE AND VERIFICATION

VAULT complies with this requirement.

VAULT acknowledges the State's right to request supporting documentation and to conduct independent verification of information provided in this proposal. VAULT will fully cooperate with any such requests and will provide accurate, complete, and timely documentation as needed to support validation activities.

VAULT affirms that all information provided regarding investigations, incidents, and compliance history is complete and accurate to the best of its knowledge. VAULT understands that failure to disclose relevant investigations may result in disqualification, contract termination, or other remedies, and has taken appropriate measures to ensure full and transparent disclosure.

4.2.3.11.8 CERTIFICATION REGARDING LEGAL COMPLIANCE

VAULT complies with this requirement.

VAULT certifies that it has not been subject to any prior or current investigations by any state or federal authority related to privacy or security of patient information.

4.2.3.11.9 WORKFORCE ELIGIBILITY AND EXCLUSIONS

VAULT complies with this requirement.

VAULT certifies that it does not employ any individuals who have been excluded or debarred by the federal government or any state government from participating in federal or state programs or contracts.

4.2.3.11.10 RESTRICTIONS ON SECONDARY USE OF DATA

VAULT complies with this requirement.

VAULT will not use IIS data for analytics, AI/ML training, model development, or any secondary purpose without explicit written approval from the State.

4.2.3.12 SECURITY AND AUDIT COMPLIANCE

VAULT complies with this requirement.

VAULT maintains a comprehensive security and compliance program designed to protect sensitive public health data and ensure alignment with federal and state cybersecurity requirements. The PrepModEcosystem and OptimIIS platform operate within a layered security model that includes secure cloud infrastructure, encryption, access controls, continuous monitoring, vulnerability management, and incident response.

VAULT's security program spans infrastructure, application, user access, monitoring, and compliance processes to ensure that the IIS environment remains secure, auditable, and aligned with evolving requirements.

4.2.3.12.1 FEDERAL SECURITY COMPLIANCE REQUIREMENTS

VAULT complies with this requirement.

VAULT ensures that the IIS solution complies with applicable federal cybersecurity standards and will provide supporting documentation as required by the Agency.

4.2.3.12.1.1 FEDRAMP AUTHORIZATION

VAULT complies with this requirement.

VAULT will provide a hosting environment that meets the requirement for FedRAMP Moderate or High authorization at the time of contract award. Where a cloud hosting provider is used, VAULT will provide documentation demonstrating the provider's FedRAMP authorization status, including an authorization letter or listing on the FedRAMP Marketplace.

VAULT acknowledges that SOC 2 Type II reports may be provided only as supplemental evidence and do not replace the FedRAMP requirement.

4.2.3.12.1.2 FIPS 140-2/3 VALIDATED CRYPTOGRAPHY

VAULT complies with this requirement.

VAULT uses cryptographic protections for data at rest and data in transit that utilize modules validated under FIPS 140-2 or FIPS 140-3 in accordance with NIST's Cryptographic Module Validation Program (CMVP).

Encryption is applied to databases, data storage, backups, communications, administrative access, and data exchange channels.

4.2.3.12.1.3 TRANSPORT LAYER SECURITY (TLS)

VAULT complies with this requirement.

VAULT secures all IIS data exchanges using Transport Layer Security in accordance with current NIST guidance. The solution supports TLS 1.2 and TLS 1.3 and is designed to implement updated TLS versions and configurations within required timeframes as standards evolve.

All TLS implementations use approved cipher suites and validated cryptographic modules and support secure communication with external systems, including CDC exchange mechanisms, provider interfaces, APIs, and administrative access.

4.2.3.12.1.4 ONGOING COMPLIANCE

VAULT complies with this requirement.

VAULT maintains ongoing compliance with federal cybersecurity standards throughout the contract term. VAULT will monitor and report any changes to FedRAMP authorization, FIPS validation, or TLS support within required timeframes.

VAULT's compliance process includes continuous monitoring, periodic control reviews, and coordination with hosting providers to ensure alignment with evolving federal requirements.

4.2.3.12.2 SOC 2 TYPE II AUDIT REPORT

VAULT complies with this requirement.

VAULT maintains an independent SOC 2 Type II audit to demonstrate the effectiveness of security and operational controls over time.

4.2.3.12.2.1 INITIAL SOC 2 TYPE II REPORT

VAULT complies with this requirement.

VAULT will provide a current SOC 2 Type II audit report within sixty (60) calendar days of contract execution. The report will cover a review period ending no more than twelve (12) months prior to submission and will demonstrate compliance with the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy.

4.2.3.12.2.2 ANNUAL UPDATED SOC 2 TYPE II REPORT

VAULT complies with this requirement.

VAULT will provide updated SOC 2 Type II audit reports annually, within thirty (30) calendar days of the contract anniversary date, for the duration of the contract term.

VAULT acknowledges that the Agency may review the report for sufficiency and request additional documentation or clarification in the event of material changes to the hosting environment or security posture.

4.2.3.12.2.3 ISO/IEC 27001 AS SUPPLEMENTAL EVIDENCE

VAULT complies with this requirement.

VAULT may provide ISO/IEC 27001 certification as supplemental evidence of organizational security maturity. VAULT acknowledges that ISO certification does not replace the requirement for SOC 2 Type II or the State's U.S. data residency requirements.

4.2.3.12.3 PENETRATION TESTING AND VULNERABILITY MANAGEMENT

VAULT complies with this requirement.

VAULT maintains a formal vulnerability management and penetration testing program designed to identify, prioritize, remediate, and validate security findings across the hosted IIS environment.

Third-party penetration testing is conducted at least annually in alignment with NIST 800-53 standards. VAULT will provide a detailed report of findings and remediation actions to the State within thirty (30) calendar days of test completion.

VAULT maintains a documented vulnerability management program that includes continuous scanning, risk prioritization, remediation tracking, and validation of remediation activities. All critical and high-risk findings are remediated within thirty (30) calendar days, unless otherwise approved by the State.

4.2.3.12.4 SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SSDLC) PRACTICES

VAULT's Secure Software Development Lifecycle (SSDLC) ensures that security is integrated throughout the entire system lifecycle, from design through ongoing maintenance. By aligning with NIST SP 800-218 and incorporating automated security testing, vulnerability management, and continuous monitoring, VAULT ensures that security risks are identified early, addressed promptly, and consistently managed.

This approach enables the IIS to be developed and maintained in a secure, controlled, and auditable manner, supporting compliance with federal cybersecurity standards and reducing long-term operational risk.

4.2.3.12.4.1 DOCUMENTED SSDLC PROCESS

VAULT complies with this requirement.

VAULT maintains documented SSDLC policies and procedures aligned with NIST SP 800-218 (Secure Software Development Framework) or equivalent standards. Security requirements are incorporated throughout system design, development, testing, deployment, and maintenance.

4.2.3.12.4.2 STATIC AND DYNAMIC APPLICATION SECURITY TESTING (SAST/DAST)

VAULT complies with this requirement.

VAULT performs static application security testing (SAST) integrated into the development pipeline for each code commit or build. Dynamic application security testing (DAST) is conducted at least quarterly and following major releases or production updates.

All identified vulnerabilities are documented, prioritized, and tracked through resolution. Critical and high-risk findings are remediated within thirty (30) calendar days, unless otherwise approved by the Agency.

4.2.3.12.4.3 VULNERABILITY MANAGEMENT INTEGRATION

VAULT complies with this requirement.

Findings from SAST and DAST are incorporated into VAULT's vulnerability management program and managed in accordance with established remediation timelines and tracking processes.

4.2.3.12.4.4 THIRD-PARTY COMPONENT SECURITY

VAULT complies with this requirement.

VAULT tracks and manages all third-party libraries and components used within the solution. Dependency inventories are maintained and monitored for known vulnerabilities, and components are updated to address identified risks.

4.2.3.12.4.5 CONTINUOUS MONITORING

VAULT complies with this requirement.

VAULT implements continuous monitoring practices aligned with federal and industry guidance. Monitoring includes system activity, infrastructure events, application behavior, and security alerts, supported by automated code scanning, vulnerability assessments, and annual penetration testing.

4.2.3.12.5 CLOUD PROVIDER ATTESTATIONS

Where VAULT utilizes a third-party cloud provider, VAULT will provide the attestations and documentation required by the State to verify the provider's security and residency posture.

4.2.3.12.5.1 CLOUD PROVIDER FEDRAMP DOCUMENTATION

VAULT will provide documentation confirming that the cloud provider maintains FedRAMP Moderate or High authorization, as required by the solicitation.

4.2.3.12.5.2 U.S.-BASED DATA STORAGE AND PROCESSING

VAULT will provide evidence that all IIS data is stored and processed exclusively within U.S.-based data centers, in compliance with federal and West Virginia cybersecurity and data residency requirements.

4.2.3.12.5.3 COMPLIANCE WITH EXECUTIVE BRANCH AND OMIS SECURITY POLICIES

VAULT will support compliance with applicable Executive Branch and OMIS security policies through hosting configuration, operational controls, documentation, and governance practices aligned with State requirements.

4.2.3.12.6 VENDOR ATTESTATION FORM

VAULT complies with this requirement.

VAULT will complete and submit the required Vendor Attestation Form within thirty (30) calendar days of contract execution and will provide updated attestations as requested by the State.

4.2.3.12.6.1 VENDOR ATTESTATION SUBMISSION

VAULT complies with this requirement.

VAULT will submit the Vendor Attestation Form certifying compliance with the requirements outlined in this section, including:

4.2.3.12.6.1.1 U.S.-BASED DATA RESIDENCY AND TRANSMISSION RESTRICTIONS

VAULT WILL ATTEST THAT ALL IIS DATA IS STORED, PROCESSED, AND TRANSMITTED IN COMPLIANCE WITH U.S.-BASED DATA RESIDENCY REQUIREMENTS.

4.2.3.12.6.1.2 SOC 2 TYPE II AUDIT SUBMISSION TIMELINES

VAULT will attest to compliance with SOC 2 Type II audit report submission requirements, including initial and annual reporting timelines.

4.2.3.12.6.1.3 PENETRATION TESTING AND VULNERABILITY REMEDIATION PROTOCOLS

VAULT will attest that penetration testing and vulnerability management practices comply with required standards, including remediation timelines for critical and high-risk findings.

4.2.3.12.6.1.4 CLOUD PROVIDER COMPLIANCE

VAULT will attest that its hosting provider meets required security and authorization standards, including FedRAMP requirements where applicable.

4.2.3.12.6.1.5 APPLICABLE STATE AND FEDERAL CYBERSECURITY POLICIES AND STANDARDS

VAULT will attest that the solution complies with applicable state and federal cybersecurity requirements.

4.2.3.12.6.1.6 APPLICABLE STATE AND FEDERAL INFORMATION SECURITY AND PRIVACY REQUIREMENTS

VAULT will attest that the solution complies with applicable information security and privacy requirements throughout the contract term.

VAULT acknowledges that the State may request updated attestations annually or upon material changes to the hosting environment, security posture, or compliance status and will provide such updates as required.

4.2.3.12.7 INCIDENT RESPONSE (IR) POLICY AND PLAN REQUIREMENTS

VAULT complies with this requirement.

VAULT maintains a formal incident response (IR) policy and plan that define procedures for identifying, reporting, containing, eradicating, and recovering from security incidents.

4.2.3.12.7.1 NIST ALIGNMENT

VAULT complies with this requirement.

VAULT's incident response policy and plan are aligned with the current version of NIST SP 800-61 (Computer Security Incident Handling Guide) or successor publications.

4.2.3.12.7.2 ONGOING UPDATES

VAULT complies with this requirement.

VAULT will update its incident response policy and plan within six (6) months of any NIST revision or federal mandate affecting incident response practices.

4.2.3.12.7.3 INTEGRATION WITH AGENCY PLAN

VAULT complies with this requirement.

VAULT's incident response processes are designed to integrate with the Agency's incident response procedures, ensuring coordinated detection, reporting, containment, eradication, and recovery.

4.2.3.12.7.4 TESTING AND EXERCISES

VAULT complies with this requirement.

VAULT conducts annual incident response exercises, including tabletop and simulated scenarios. VAULT will provide summary reports of findings and corrective actions to the Agency within thirty (30) calendar days of test completion.

4.2.3.12.7.5 AVAILABILITY

VAULT complies with this requirement.

VAULT will make its incident response policy and plan available to the Agency upon request and will certify compliance annually.

4.2.3.12.7.6 CONTINUOUS IMPROVEMENT

VAULT complies with this requirement.

VAULT incorporates lessons learned from incidents and testing into its incident response program and will update its plan within sixty (60) calendar days of identified improvements.

4.2.3.12.8 AUDIT AND ATTESTATION REQUIREMENTS

VAULT complies with this requirement.

VAULT supports Agency oversight and independent verification of required security controls and will cooperate with audit, attestation, and evidence requests.

4.2.3.12.8.1 PROVIDE EVIDENCE AT NO COST

VAULT complies with this requirement.

VAULT will provide system documentation, policies, configurations, testing results, audit reports, and other evidence necessary to verify compliance at no additional cost to the State.

4.2.3.12.8.2 TIMELY RESPONSE

VAULT complies with this requirement.

VAULT will provide requested evidence within thirty (30) calendar days of the State's request, unless otherwise approved by the Agency.

4.2.3.12.8.3 INDEPENDENT VERIFICATION

VAULT complies with this requirement.

VAULT will support independent verification activities conducted by the State or its designee to validate compliance with required security controls.

4.2.3.12.8.4 ONGOING ATTESTATION

VAULT complies with this requirement.

VAULT will complete and submit updated attestations annually and upon material changes to the hosting environment, security posture, or compliance program.

4.2.3.12.8.5 FUTURE STANDARDS ALIGNMENT

VAULT complies with this requirement.

VAULT will ensure that audits, attestations, and supporting controls remain aligned with the most current versions of applicable federal and state cybersecurity standards, including NIST, FedRAMP, FIPS, and OMIS policies.

4.2.3.12.8.6 REMEDIATION OBLIGATION

VAULT complies with this requirement.

VAULT will address any deficiencies identified through audits or attestations within sixty (60) calendar days, or as otherwise approved by the Agency, and will provide written confirmation of remediation.

Summary

VAULT's security and audit compliance program is designed to ensure that the IIS operates within a secure, controlled, and fully auditable environment aligned with federal and state cybersecurity requirements. Through adherence to standards such as FedRAMP, NIST, FIPS, and SOC 2, VAULT implements layered protections across infrastructure, application, data, and operational processes.

The solution incorporates validated encryption, secure communications, continuous monitoring, formal vulnerability management, and a structured secure development lifecycle to proactively identify and mitigate risk. VAULT also maintains a mature incident response program, regular testing practices, and ongoing compliance processes to ensure that security controls remain effective over time.

VAULT supports full transparency and accountability through audit readiness, documentation, attestation, and cooperation with independent verification activities, enabling the State to verify compliance at any time.

This approach ensures that the IIS environment remains secure, resilient, and aligned with evolving cybersecurity standards while providing the Agency with confidence in the protection and integrity of its data.

4.2.3.13 ACCEPTANCE CRITERIA

VAULT Technologies fully acknowledges and agrees to all Acceptance Criteria requirements defined by the Agency and confirms that the proposed solution, implementation methodology, and operational framework are designed to ensure successful, measurable, and fully documented Acceptance.

VAULT's approach to Acceptance is based on a formalized Acceptance Management Framework that has been successfully applied across multiple statewide implementations. This framework ensures that all functional, technical, interoperability, security, and performance requirements are not only met, but validated through structured, repeatable processes aligned with the Agency's expectations.

Acceptance is not treated as a single milestone, but as a progressive validation lifecycle embedded throughout implementation. Each phase of the project includes defined deliverables, validation checkpoints, and acceptance criteria, ensuring that issues are identified and resolved early, reducing risk at final Acceptance.

VAULT maintains full traceability between requirements, system configuration, testing activities, and deliverables through the use of structured project management and quality assurance processes. This ensures that every requirement in the Solicitation is explicitly addressed, tested, and validated prior to formal Acceptance.

4.2.3.13.1 GENERAL ACCEPTANCE REQUIREMENT

VAULT understands that the Agency will issue written Acceptance only after confirming that all requirements have been fully satisfied. To support this requirement, VAULT implements a formal Acceptance Governance Model that ensures transparency, accountability, and alignment at every stage of the project.

At project initiation, VAULT works with the Agency to define a detailed Acceptance Plan, which includes:

- Clearly defined deliverables aligned to each requirement
- Documented acceptance criteria for each deliverable
- Traceability to RFP requirements and implementation scope
- Defined review and approval processes
- Roles and responsibilities for Agency and Vendor stakeholders

Each deliverable is subject to formal review and approval cycles, including demonstration sessions, documentation review, and validation testing. Deliverables are not advanced to subsequent phases without Agency acknowledgment, ensuring that Acceptance is built incrementally rather than deferred to the end of the project.

VAULT also maintains a requirements traceability matrix (RTM) throughout the project lifecycle, ensuring that all requirements are accounted for and validated prior to final Acceptance.

No portion of the system will be considered complete or operationally accepted until all required Acceptance activities have been completed and formally approved in writing by the Agency.

4.2.3.13.2 ACCEPTANCE TESTING

VAULT fully supports and participates in Agency-led Acceptance Testing and provides a structured, multi-layered testing framework designed to validate all aspects of the system prior to production use.

Testing is conducted across multiple phases, including unit testing, system integration testing, performance testing, security validation, and user acceptance testing, ensuring comprehensive coverage.

VAULT provides detailed test plans, test scripts, and validation criteria aligned with Agency requirements. Testing activities are supported by dedicated QA resources, test environments, and real-time issue tracking tools.

4.2.3.13.2.1 FUNCTIONAL TESTING OF ALL MODULES AND WORKFLOWS

VAULT conducts comprehensive functional testing across all system modules, including immunization workflows, patient management, reporting, provider management, and administrative functions.

Functional testing includes:

- Scenario-based test cases reflecting real-world workflows
- Validation of business rules, data entry, and system responses
- Verification of user roles and permissions
- End-to-end workflow validation across modules

Each functional area is validated against documented requirements, ensuring that all system capabilities perform as expected in operational scenarios.

4.2.3.13.2.2 DATA MIGRATION VALIDATION

VAULT executes a structured and repeatable data migration validation process designed to ensure accuracy, completeness, and integrity of all migrated data.

This process includes:

- Data mapping and transformation validation
- Multiple test migration cycles
- Record-level reconciliation between source and target systems
- Validation of historical immunization records, patient demographics, and provider data
- Data quality checks including duplicate detection and error identification

VAULT provides detailed validation reports and works collaboratively with the Agency to resolve discrepancies prior to final migration.

4.2.3.13.2.3 INTERFACE AND INTEROPERABILITY TESTING

All interfaces are rigorously tested to ensure accurate, consistent, and reliable data exchange across all connected systems.

Testing includes:

- HL7 v2.5.1 message validation (VXU, QBP, ACK)
- FHIR API testing for real-time data exchange
- IIS-to-IIS data exchange validation
- Integration with HIEs, EHR systems, pharmacies, and laboratories
- End-to-end message flow validation, including ingestion, processing, and response

IISConnex provides automated validation, message normalization, error handling, and monitoring capabilities to support interoperability testing and ensure compliance with CDC standards.

4.2.3.13.2.4 PERFORMANCE AND LOAD TESTING

VAULT conducts performance and load testing to validate system scalability, responsiveness, and stability under both expected and peak conditions.

Testing scenarios include:

- High-volume transaction processing
- Concurrent user access across multiple roles
- Large data queries and reporting workloads
- Stress testing to identify system limits and ensure resilience

Results are documented and reviewed with the Agency to confirm that performance requirements are met.

4.2.3.13.2.5 SECURITY AND ACCESS CONTROL VERIFICATION

Security validation is conducted to ensure that all access controls and data protection mechanisms are functioning as intended.

This includes:

- Verification of authentication and multi-factor authentication controls
- Role-based access validation across user types
- Audit logging and monitoring validation
- Encryption verification for data at rest and in transit
- Vulnerability scanning and security testing

These activities ensure compliance with Agency security requirements and applicable standards.

4.2.3.13.2.6 USER ACCEPTANCE TESTING (UAT)

VAULT supports Agency-led UAT by providing structured test scripts, training, and real-time support to Agency-designated users.

UAT includes:

- Validation of system functionality against operational workflows
- Confirmation of usability and workflow alignment
- Identification and documentation of issues or enhancements
- Final validation of readiness for production deployment

VAULT provides on-demand support during UAT to ensure timely issue resolution and a smooth validation process.

VAULT confirms that all defects identified during Acceptance Testing will be tracked, prioritized, and resolved at no additional cost to the Agency. A formal defect management process is used to ensure transparency and timely resolution.

4.2.3.13.3 ACCEPTANCE CRITERIA

VAULT confirms that the system will not be considered acceptable until all defined Acceptance Criteria have been fully satisfied.

4.2.3.13.3.1 FULL SYSTEM FUNCTIONALITY

VAULT ensures that all system functionality is fully implemented in accordance with the approved Implementation Plan and RFP requirements through structured configuration, validation, and testing processes.

4.2.3.13.3.2 OPERATIONAL INTERFACES

All required interfaces will be fully operational, supporting accurate and consistent data exchange with Agency-designated systems. Interface performance and reliability are validated through testing and monitoring.

4.2.3.13.3.3 DEFECT RESOLUTION

All Critical and High severity defects will be resolved prior to Acceptance. VAULT maintains a structured defect classification and resolution process to ensure that remaining issues do not impact system performance or workflows.

4.2.3.13.3.4 DOCUMENTATION DELIVERY

VAULT provides comprehensive documentation, including:

- System architecture and technical design
- Configuration and administrative guides
- User manuals and training materials
- Operational procedures

All documentation is reviewed with the Agency and finalized prior to Acceptance.

4.2.3.13.3.5 SECURITY CONTROLS VALIDATION

All security controls are fully implemented and validated, including authentication, authorization, audit logging, and compliance with Agency security standards.

4.2.3.13.3.6 STABILIZATION PERIOD

Following go-live, VAULT supports a defined stabilization (hypercare) period during which system performance, data exchange, and user workflows are closely monitored.

During this period:

- Issues are prioritized and resolved rapidly
- System performance is continuously evaluated
- Additional support resources are available

The system must operate without material errors for the agreed-upon period prior to Acceptance.

4.2.3.13.3.7 CONTRACTUAL DELIVERABLES

VAULT ensures that all contractual deliverables, including reporting, project management artifacts, and communication requirements, are completed and approved prior to final Acceptance.

4.2.3.13.4 FORMAL ACCEPTANCE

Upon successful completion of all Acceptance activities, VAULT will support the Agency in issuing a formal written Notice of Acceptance. This milestone represents confirmation that all requirements have been met and validated.

4.2.3.13.5 REJECTION AND RETESTING

VAULT acknowledges the Agency's right to reject the system if Acceptance Criteria are not met.

In such cases, VAULT will:

- Address all identified deficiencies promptly
- Provide corrective action plans
- Retest affected components
- Support any additional validation required by the Agency

All remediation activities will be completed at no additional cost to the Agency.

4.2.3.13.6 PRORATED ANNUAL FEES POST-IMPLEMENTATION

VAULT agrees to invoice only for the prorated portion of annual fees following formal Acceptance, calculated based on the remaining days in the contract year. Billing practices will strictly adhere to the requirements outlined in this section.

4.2.3.13.7 ANNUAL FEE BILLING LIMITS AND ADVANCE BILLING REQUIREMENTS

VAULT will comply with all billing limitations defined by the Agency. Annual fees will not exceed twelve (12) months for any billing period and will not be invoiced as multi-year lump sums. Billing will be structured as:

- Annual billing in advance for a 12-month period, or
- Quarterly billing in advance, subject to Agency approval

VAULT will not invoice for services beyond the upcoming billing period or for services not yet rendered.

Summary

VAULT's Acceptance approach provides a structured, transparent, and low-risk pathway to system validation, ensuring that all requirements are fully met, tested, and approved prior to formal Acceptance. This methodology reflects VAULT's experience delivering complex, statewide systems and ensures successful outcomes for the State of West Virginia.

VAULT Technologies brings extensive experience in designing, implementing, and supporting public health information systems, including Immunization Information Systems (IIS), patient registration platforms, and billing and reporting solutions. VAULT's experience spans multiple jurisdictions and includes statewide deployments, integrations with federal systems, and support for complex public health workflows.

VAULT's approach is grounded in delivering scalable, secure, and user-centered solutions that meet both operational and regulatory requirements. The company has successfully supported public health agencies in improving immunization tracking, increasing provider participation, enhancing data quality, and enabling data-driven decision-making.

VAULT combines technical expertise, domain knowledge, and proven delivery methodologies to ensure successful outcomes for projects of similar scope and complexity.

Organizational Qualifications

VAULT has deep experience supporting public health programs through its suite of platforms, including PrepMod and OptimIIS. These platforms have been used to support immunization programs, emergency response initiatives, school-based health programs, and provider reporting across multiple jurisdictions.

VAULT's team includes experts in public health informatics, system integration, cloud infrastructure, security and compliance, and project management. This multidisciplinary expertise enables VAULT to address both technical and operational challenges associated with IIS implementations.

VAULT has demonstrated the ability to operate within highly regulated environments, ensuring compliance with HIPAA, CDC IIS Functional Standards, NIST guidance, and state-specific requirements.

Relevant Project Experience

VAULT has successfully delivered projects comparable in scope and complexity to the requirements outlined in this RFP.

In Maryland, VAULT implemented and supports a statewide PrepMod deployment that integrates immunization workflows, school-based programs, and public health reporting. The system supports provider onboarding, patient registration, vaccine administration tracking, and reporting, and has been used extensively for both routine immunization programs and large-scale public health initiatives.

The Maryland implementation required coordination across multiple stakeholders, including state agencies, providers, schools, and community organizations. VAULT delivered a solution that improved operational efficiency, enhanced data quality, and enabled better tracking of immunization coverage.

These projects demonstrate VAULT's ability to deliver solutions that meet jurisdiction-specific needs while maintaining alignment with national standards.

Project Staffing and Expertise

VAULT provides a structured staffing model that aligns resources to project needs across all phases of implementation. The team includes project management, technical leadership, development, quality assurance, training, and support roles.

Dr. Montressa Washington, PMP will serve as Project Manager, bringing more than 20 years of experience in project management and public health systems. Her background includes work with organizations such as IBM and Accenture, where she led large-scale, cross-functional initiatives. She will oversee day-to-day execution, stakeholder coordination, and delivery accountability.

VAULT's staffing approach ensures that each role is clearly defined and aligned with project objectives. Resources are assigned based on expertise and experience, ensuring that the project benefits from specialized knowledge in areas such as interoperability, data quality, security, and user adoption.

Certifications and Professional Qualifications

VAULT's team includes certified professionals with expertise in project management, cloud infrastructure, security, and software development. Relevant certifications include Project Management Professional (PMP), as well as certifications held by cloud and security personnel supporting the platform.

VAULT maintains ongoing training and professional development programs to ensure that staff remain current with evolving technologies, standards, and best practices.

References and Past Performance

VAULT can provide references from prior projects that demonstrate successful delivery of public health solutions similar to those requested in this RFP. These references include state agencies and public health organizations that can speak to VAULT's ability to deliver high-quality solutions, meet project timelines, and provide responsive support.

References will include contact information, project descriptions, and outcomes achieved, consistent with the requirements of this section.

Approach to Meeting Project Goals

VAULT's approach to meeting project goals is based on collaboration, transparency, and continuous improvement. VAULT works closely with Agency stakeholders to understand requirements, define success criteria, and ensure alignment throughout the project lifecycle.

VAULT uses structured methodologies for implementation, risk management, quality assurance, and change management. This ensures that project goals and objectives are clearly defined, tracked, and achieved.

The company's experience with similar projects enables it to anticipate challenges, apply proven solutions, and deliver results efficiently and effectively.

Summary

VAULT Technologies offers a strong combination of technical expertise, public health experience, and proven delivery capability. Through successful implementations in jurisdictions such as Maryland, VAULT has demonstrated its ability to deliver secure, scalable, and effective solutions that meet the needs of public health agencies.

VAULT's qualifications, experienced staff, and track record of successful project delivery position it well to meet the requirements of this RFP and support the State of West Virginia in achieving its immunization program goals.

4.3.1 QUALIFICATIONS AND EXPERIENCE INFORMATION

VAULT Technologies meets and exceeds the desirable qualifications and experience requirements outlined in this RFP through its demonstrated success in delivering large-scale, secure, and interoperable public health systems. VAULT's experience spans the full lifecycle of

Immunization Information System (IIS) implementations, including system design, development, deployment, integration, and ongoing operations and support.

VAULT has extensive experience working with state and local public health agencies to implement solutions that align with CDC IIS Functional Standards, federal reporting requirements, and state-specific program needs. This includes supporting immunization programs, emergency response initiatives, provider onboarding, and public health reporting across diverse jurisdictions.

The company has a proven track record of delivering solutions that operate at scale, support high-volume transactions, and maintain performance during periods of peak demand. VAULT's platforms have been used to support millions of immunization events and have enabled real-time data exchange with federal, state, and partner systems.

VAULT's qualifications are further demonstrated through its ability to integrate complex systems, including electronic health records (EHRs), pharmacy systems, laboratory systems, and federal data exchanges. The company has deep expertise in interoperability standards such as HL7 and FHIR, ensuring seamless data exchange and improved data quality across systems.

In addition to technical capabilities, VAULT brings strong programmatic and operational expertise in public health. The company understands the workflows, challenges, and priorities of immunization programs, including school-based vaccination, community outreach, and provider engagement. This enables VAULT to deliver solutions that are not only technically sound but also aligned with real-world operational needs.

VAULT also demonstrates strong experience operating in highly regulated environments, maintaining compliance with HIPAA, NIST guidance, and other applicable federal and state requirements. The company's cloud-based solutions are designed with security, scalability, and reliability as foundational principles.

Through its combination of technical expertise, domain knowledge, and proven delivery experience, VAULT is well positioned to meet the qualifications and experience requirements of this RFP and to support the State of West Virginia in achieving its immunization program objectives.

4.3.1.1 BUSINESS

VAULT Technologies is a public health-focused technology company specializing in the development and operation of secure, scalable software platforms that support immunization programs and broader healthcare delivery.

VAULT is the developer of the PrepModEcosystem, including OptimIIS, a modern, cloud-based immunization information system designed to meet CDC Functional Standards and support large-scale public health operations.

VAULT has extensive experience delivering technology solutions to government health and human services agencies. During the COVID-19 pandemic, VAULT's platform was widely adopted across the United States, supporting more than 70,000 healthcare providers across over 40 states and enabling the scheduling, administration, and reporting of millions of immunization encounters. The platform was among the first large-scale applications used to support mass vaccination efforts during the pandemic.

VAULT's approach is uniquely informed by deep public health expertise. The company is led by a public health professional with nearly 20 years of experience in immunization programs, including leadership of a county immunization program where early prototypes of a state immunization information system were developed and used operationally.

This experience includes extensive work in school-based and community-based vaccination delivery, providing a practical understanding of how immunization programs operate across diverse settings. This real-world perspective has directly informed the design of the PrepModEcosystem, ensuring that it supports not only data collection, but the full lifecycle of public health operations—from outreach and service delivery to reporting and analysis.

Through these implementations, VAULT has demonstrated the ability to:

- Support high-volume, statewide public health operations
- Rapidly onboard diverse providers and partner organizations

- Enable real-time data exchange and reporting
- Maintain system performance during large-scale emergency response efforts

VAULT's experience spans collaboration with state and local public health agencies, healthcare providers, pharmacies, schools, and community-based organizations, providing a deep understanding of the operational, technical, and regulatory requirements of public health systems.

This combination of proven scale, government experience, and public health leadership positions VAULT to successfully deliver and support a modern IIS for the State of West Virginia.

VAULT's guiding principle—"by public health, for public health"—reflects its commitment to building technology that is grounded in real-world public health practice and designed to serve the needs of the communities it supports.

4.3.1.2 CORPORATE IDENTITY

VAULT has no parent company or subsidiaries.

4.3.1.3 ORGANIZATION AND STRUCTURE

VAULT Technologies operates through a multidisciplinary organizational structure composed of core business units that work together to deliver, implement, and support public health technology solutions.

These business units include:

- Product & Engineering
- Implementation & Delivery
- Customer Success & Account Management
- Operations & Maintenance (M&O)
- Training & Organizational Change Management (OCM)
- Support & Quality Assurance

This structure ensures that all aspects of the State of West Virginia's IIS—from system design and implementation to ongoing operations and user support—are coordinated and aligned with the State's requirements.

Business Unit Responsibilities and Relationships

Each business unit plays a distinct role while operating in a highly coordinated model:

- **Product & Engineering**

Responsible for system architecture, development, interoperability, and performance of the platform, including OptimIIS and related components.

- **Implementation & Delivery**

Leads system configuration, deployment, and data migration, ensuring that the solution is implemented efficiently and in alignment with State workflows.

- **Customer Success & Account Management**

Serves as the primary interface with the State, ensuring alignment with program goals, responsiveness to needs, and long-term success.

- **Operations & Maintenance (M&O)**

Ensures system stability, monitoring, and performance post-implementation, including issue resolution and system updates.

- **Training & Organizational Change Management (OCM)**

Supports user onboarding, training, and adoption across diverse partner groups, including providers, schools, and community organizations.

- **Support & Quality Assurance**

Provides ongoing technical support, testing, and validation to ensure system reliability and compliance with requirements.

Integrated Operational Model

These business units operate in a coordinated and integrated manner, ensuring seamless delivery across all phases of the project lifecycle.

- Product & Engineering collaborates with Implementation to configure and deploy the system
- Implementation transitions to Operations & Maintenance for ongoing support
- Customer Success and Account Management ensure continuous alignment with State priorities
- Training & OCM supports adoption across all user groups
- Support & QA ensures system quality and responsiveness

This integrated model ensures that technical, operational, and programmatic functions work together to support:

- Provider onboarding and engagement
- High-quality data collection and reporting
- Rapid response during public health emergencies
- Ongoing system performance and user satisfaction

Alignment with State Needs

VAULT's organizational structure is specifically designed to support the State's requirements for:

- Scalable implementation and onboarding across diverse partner types
- Continuous system availability and performance
- Rapid response to public health emergencies
- Long-term sustainability and adaptability

Scalability and Flexibility

VAULT's business units are designed to scale as needed, allowing additional resources to be deployed to support:

- Increased provider participation
- Expansion of system usage
- Emergency response scenarios

Conclusion

VAULT's business unit structure provides a coordinated, scalable, and integrated operational model that aligns with the State of West Virginia's technical, operational, and public health needs.

This approach ensures that all aspects of system delivery and support are managed effectively, while maintaining flexibility to adapt to evolving requirements.

4.3.1.4 LOCATIONS

VAULT Technologies is based in Maryland and provides support to jurisdictions nationwide through a US-based cloud-based infrastructure.

U.S.-Based Operations

All functions supporting the proposed solution—including system development, implementation, operations, and customer support—will be performed by personnel located within the United States.

VAULT utilizes a distributed team model, allowing for responsive support across multiple time zones while maintaining centralized coordination and oversight.

Cloud Infrastructure and Data Residency

All system data, including State and Federal data, is:

- Stored and processed exclusively within the United States
- Hosted in secure, U.S.-based cloud environments that meet applicable federal and State security requirements

VAULT does not store, process, or transmit any State or Federal data outside of the United States.

Overseas Operations

VAULT will not utilize any overseas locations, personnel, or infrastructure to support the proposed solution.

Operational Alignment

This U.S.-based operational model ensures:

- Compliance with State and Federal data residency requirements
- Secure handling of sensitive health information
- Reliable and responsive support for West Virginia stakeholders

Summary

VAULT's geographic and operational approach ensures that:

- All work supporting the contract is performed within the United States
- All data remains securely stored within U.S.-based systems
- No overseas resources are used
- The State's security and compliance requirements are fully met

VAULT Technologies operates within the United States and supports jurisdictions nationwide through cloud-based solutions and distributed teams.

4.3.1.5 REFERENCES

VAULT Technologies has successfully implemented and operated large-scale immunization and public health platforms across multiple jurisdictions. The following references demonstrate our experience delivering secure, interoperable, and scalable solutions that support real-world immunization program operations.

Reference 1: Maryland Department of Health (DOH)

Project:

Implementation, ongoing enhancement, and operational support of the PrepMod platform through Maryland's Premier Development Package, supporting statewide immunization workflows and public health initiatives.

Project Goals & Objectives:

The primary objective of this engagement was to provide Maryland with a flexible, continuously evolving platform to support immunization program operations and broader public health initiatives. The project focused on enabling rapid development and deployment of new functionality aligned with state policy goals, improving provider workflows, and ensuring seamless integration with Maryland's IIS (ImmuNet).

A key goal was to establish a collaborative development model that allowed the State to actively participate in prioritizing system enhancements, ensuring that the platform remained aligned with real-world operational needs and emerging public health requirements.

Functionality Delivered:

Through the Premier Development Package, VAULT provided a dedicated team consisting of two software engineers, a project manager, and a product manager who worked directly with Maryland's leadership and program staff.

The platform supports patient registration, scheduling, vaccination documentation, and HL7-based reporting to the State's IIS. Continuous enhancements have been delivered to improve usability, streamline provider workflows, and expand system capabilities in response to evolving program needs.

Weekly collaboration sessions with State leadership allowed for real-time prioritization and refinement of features, while monthly user group meetings captured provider feedback and informed ongoing improvements. This iterative development approach enabled rapid deployment of new functionality aligned with both policy changes and operational demands.

Implementation Timeline:

2021 to present, with continuous enhancements and active development.

Operational Status:

The system is currently in active use statewide and continues to evolve through ongoing collaboration with Maryland DOH. The Premier Development model has enabled a steady stream of enhancements, ensuring that the platform remains aligned with program needs and responsive to changes in public health policy and provider workflows.

This long-term engagement demonstrates VAULT Technologies' ability to operate not only as a technology vendor, but as a strategic partner supporting continuous innovation and operational excellence.

Reference 2: Labcorp

Project:

Implementation of the IISConnex interoperability platform to support nationwide immunization data exchange.

Project Goals & Objectives:

The objective of this engagement was to enable Labcorp to efficiently transmit vaccination data to multiple state IIS systems through a centralized interoperability solution. The project aimed to simplify multi-state reporting, improve data consistency, and support both unidirectional and bidirectional data exchange with state registries. A key focus was creating a scalable solution capable of handling high volumes of data across a national footprint.

Functionality Delivered:

IISConnex provides centralized ingestion and transformation of vaccination records and supports HL7-based data exchange with more than 30 state IIS systems. The platform performs message validation, normalization, and routing to appropriate jurisdictions, ensuring compliance with state and federal standards. It also supports bidirectional exchange, allowing both submission of vaccination records and retrieval of immunization histories. The architecture is designed to scale efficiently, supporting high-volume national data exchange.

Implementation Timeline:

2023 to present.

Operational Status:

The platform is currently in production and supports ongoing nationwide operations for Labcorp. IISConnex enables seamless reporting to more than 30 IIS jurisdictions and continues to expand as additional integrations are added. The system has demonstrated reliability, scalability, and compliance in a complex multi-jurisdictional environment.

Reference 3: Bird's Eye Medical

Project:

Deployment of the PrepMod platform and ReadiBilling solution to support immunization workflows and reimbursement operations across local health departments and school-based clinics in Indiana.

Project Goals & Objectives:

The goal of this engagement was to support immunization operations across distributed provider networks, including local health departments and school-based clinics, while also enabling financial sustainability through billing capabilities. The system was designed to manage patient encounters, generate immunization records, ensure accurate reporting to the state IIS, and provide mechanisms for reimbursement of immunization services. Additional objectives included improving operational efficiency, enhancing data visibility, and supporting high-volume vaccination workflows across multiple sites.

Functionality Delivered:

The PrepMod platform provides patient registration, scheduling, and encounter management capabilities tailored to vaccination clinics. It supports HL7 message generation and submission to the state IIS, ensuring accurate and timely reporting. The system accommodates school-based and community vaccination workflows and is capable of processing high volumes of immunization encounters.

In addition, ReadiBilling was implemented to support claims generation and reimbursement workflows. This functionality enables providers and partner organizations to submit claims for immunization services, improving financial sustainability and supporting continued program expansion. Together, these solutions provide an integrated operational and financial platform for immunization programs.

The platform also includes reporting tools that provide both operational insights and public health analytics, supporting program management, performance monitoring, and compliance.

Implementation Timeline:

2024 to present.

Operational Status:

The system is currently in active use across multiple local health departments and school-based clinics. It processes millions of vaccination encounters and supports ongoing immunization reporting to the state IIS. ReadiBilling is actively used to support reimbursement workflows, enabling participating organizations to sustain and expand immunization services. The combined solution continues to support daily operations while scaling across additional sites and programs.

Additional Note:

VAULT Technologies has been recommended by the Washington State Department of Health based on prior successful implementation and demonstrated operational performance, reinforcing our ability to deliver reliable, scalable, and sustainable public health solutions.

4.3.2 MANDATORY QUALIFICATION/EXPERIENCE REQUIREMENTS

VAULT Technologies meets and exceeds the mandatory qualification and experience requirements outlined in this section through its demonstrated experience delivering and supporting large-scale public health systems, including Immunization Information Systems (IIS) and related platforms, within highly regulated environments.

VAULT has successfully implemented and supported solutions in multiple jurisdictions that align with the scope, scale, and regulatory requirements described in this RFP. These implementations have required compliance with federal and state regulations, integration with external systems, and support for diverse stakeholder groups, including public health agencies, providers, schools, and community partners.

VAULT's experience is recent, relevant, and directly applicable to the requirements of the State of West Virginia.

4.3.2.1 ORGANIZATIONAL EXPERIENCE WITH IIS AND PUBLIC HEALTH SYSTEMS

VAULT exceeds the mandatory qualification requirements by demonstrating not only relevant experience, but proven success in deploying and operating systems in complex, multi-stakeholder public health environments. VAULT demonstrates organizational experience with Immunization Information Systems and large-scale public health data systems through its work supporting statewide and multi-agency implementations.

Unlike traditional IIS vendors, VAULT's experience includes both system implementation and direct support of operational workflows such as school-based programs, provider onboarding, and community-based immunization efforts.

Within the past five years, VAULT has delivered and supported systems that manage immunization workflows, patient records, provider onboarding, reporting, and interoperability with external systems. These systems are designed to support compliance with CDC IIS Functional Standards, HIPAA requirements, and applicable state-level regulations.

In Maryland, VAULT implemented and continues to support a statewide deployment of PrepMod, which integrates immunization workflows, school-based health programs, and public health reporting. The system supports high-volume operations (more than 2 million patient records), real-world public health operations, including patient registration, vaccine administration tracking, and reporting across a wide network of providers and public health stakeholders. This implementation required coordination across multiple agencies and compliance with state and federal requirements. This implementation supports tens of thousands of users and high-volume vaccination workflows across a statewide network of providers, demonstrating VAULT's ability to operate at scale in a production public health environment.

In Alaska, VAULT previously supported the PrepMod platform as part of the State's public health infrastructure. This work included system configuration, stakeholder collaboration, and alignment with CDC standards and jurisdictional requirements. This experience reflects VAULT's ability to support geographically complex environments and adapt solutions to unique public health needs.

These experiences directly align with West Virginia's environment, which includes a distributed provider network, high-volume data exchange, and the need for coordinated public health reporting across agencies and regions.

These implementations demonstrate VAULT's ability to design, deploy, and operate systems that meet the needs of public health agencies while maintaining compliance with regulatory requirements.
These systems are not theoretical implementations—they are actively used in production environments to support public health operations and decision-making.

Demonstrated Compliance with Regulatory Requirements
VAULT's solutions are developed and operated in compliance with applicable federal and state regulations, including HIPAA, CDC IIS Functional Standards, and NIST-aligned security practices. VAULT has experience operating within environments that require strict data privacy protections, auditability, and secure data exchange.

VAULT's platforms support secure data handling, role-based access control, audit logging, and interoperability with external systems such as EHRs and public health reporting systems. These capabilities ensure that the system meets both operational and compliance requirements.

Experience Within Required Timeframe
VAULT's relevant project experience falls within the required five-year timeframe and includes both active and recently completed engagements. This ensures that VAULT's experience reflects current technologies, standards, and best practices.

VAULT's work in Maryland and its prior work in Alaska demonstrate both implementation capability and the ability to support systems through evolving public health requirements.

Exceeding Mandatory Requirements

VAULT exceeds the mandatory qualification requirements through:

- Experience supporting both implementation and ongoing operations
- Proven ability to support multi-stakeholder environments, including providers, schools, and public health agencies
- Experience integrating with federal and external systems to support interoperability
- Demonstrated success in high-volume, real-world public health scenarios
- Ability to adapt solutions to diverse jurisdictional and operational needs

Summary

VAULT Technologies satisfies and exceeds the mandatory requirement to demonstrate organizational experience with Immunization Information Systems and large-scale public health data systems.

Through its work in jurisdictions such as Maryland and Alaska, VAULT has delivered and operated production systems that support high-volume public health workflows, regulatory compliance, and multi-agency coordination.

This experience directly aligns with the needs of West Virginia and demonstrates VAULT's readiness to successfully implement and support a modern, scalable IIS.

Immunization Information System (IIS) Baseline Requirements Traceability Matrix (RTM)
Update Released July 2025

This requirements traceability matrix (RTM) contains draft baseline functional and non-functional requirements for an immunization information system (IIS). The requirements clarify minimum expectations for what IIS technology must do and how it must operate to support IIS Functional Standards and programmatic and immunization stakeholder needs. The functional requirements describe intended behaviors of an IIS to support business processes and tasks, by function and capability. The non-functional requirements convey technical requirements related to how a system must operate, by attribute and sub-characteristic. An embedded IIS Functional Model presents a visual depiction of the core functions, capabilities and attributes of IIS and serves as a companion to the requirements.

This RTM is intended to be used by immunization programs as a starting point for the procurement of an IIS platform, module or enhancement. The RTM should be used throughout the system development life cycle (SDLC) to ensure requirements are met in a final product or system. Immunization programs and IIS may also use the IIS Functional Model and the requirements within this RTM to help assess and identify gaps in current IIS functions, capabilities and technical quality and provide a roadmap for future development within or across jurisdictions.

Contents

This RTM was developed by the Public Health Informatics Institute, in partnership with AIRA and CDC and with financial support from CDC under Cooperative Agreement number 6 NH23IP922664-01. Questions, comments and suggestions are welcomed at iis@phii.org.

Guidance for leveraging the RTM workbook in a procurement

Return to Cover Page

Suggested steps and helpful hints for immunization programs and IIS when using the IIS Functional Model and requirements within this RTM as part of a procurement and system development life cycle.

1. Identify the scope of the procurement
-- Are you looking to procure an IIS platform or a specific module or enhancement?
-- Identify which functions and capabilities within the IIS Functional Model may relate to your project scope.
-- What technologies/systems do you have access to within your jurisdiction that will fulfill certain functions/capabilities/requirements?
-- What technologies/systems will need to be integrated with the procured solution?
-- Use the RTM to identify the requirements in scope.

2. Identify stakeholders/representatives to be included in the requirements review and validation process (and will be included in user acceptance testing)
-- Include people that do the work, i.e., staff from across the IIS and immunization program who will be using the system/module/enhancement being procured.
-- Include representatives from IT, as appropriate, e.g., a jurisdictional IT security officer.
-- Consider validating requirements with end users to ensure completeness and accuracy and to inform prioritization.
-- Engage with the procurement office early in the process to fully understand jurisdictional requirements, policies, templates, approval processes, and timelines.

3. Gather existing business process documentation for reference
-- Gather standard operating procedures, documented workflows, business process analysis documents, help desk and tickets.
-- These materials will assist in the review and validation of the requirements within the RTM.

4. Kickoff the requirements review and validation process
-- Identify reviewers for the functions and requirements within scope, considering individuals' subject matter expertise.
-- Schedule and conduct a meeting with all stakeholders/representatives to discuss the requirement review and validation plan.
-- Introduce the Functional Model functions, capabilities and/or attributes in scope.
-- Orient the group to the RTM format and contents, including the glossary of terms.
-- Review the project schedule and individual responsibilities.

5. Review and validate requirements
-- Review the requirements by tab with the appropriate program staff and/or impacted stakeholders (consider daily facilitated review sessions). Review the requirements based on current issues, concerns, challenges to ensure/mitigate current issues, concerns, etc. (using documentation gathered in step 3).
-- Discuss and define jurisdiction-specific needs and requirements. In particular, consider requirements that include 'as per jurisdictional policy,' those indicating 'user-defined parameters,' and non-functional requirements where jurisdiction-specific values should be entered.
-- Validate the requirements in terms of their:
   * Completeness and accuracy: add jurisdiction-specific requirements in a separate tab (included in the RTM workbook) or as additional rows in the appropriate existing tab.
   * Clarity: offer clarifications as comments in the "Comments" column. CDC strongly recommends not altering the wording of the requirements in the RTM.
   * Priority: CDC strongly recommends that values listed in the "Priority: E, O (essential, optional)" column remain as is unless jurisdictional law/policy says otherwise.

6. Approve the final set of requirements
-- Gain approval of the final requirements from program and jurisdictional IT leadership, as appropriate.
-- Use the "Req. #" column on each tab to assign a unique identifier, which will facilitate traceability throughout the development lifecycle.

7. Include the requirements in the solicitation to inform vendor selection.
-- Conduct a final re-validation of the requirements: what has changed? Are the requirements still accurate and relevant? Have any priorities changed?
-- Work with your procurement office to ensure your requirements are incorporated into your solicitation. Attach or otherwise incorporate the RTM or requirements listing based on jurisdictional policy.
-- Provide instructions for solicitation respondents to comment on each requirement, using the "Vendor Response" and "Vendor Comments" columns.
-- Review responses and conduct due diligence to determine a solution/vendor that best meets your needs.

8. Work with the selected vendor on configuration and specifications, as needed.
-- Ensure that your essential requirements are met.
-- Review vendor system documentation to determine potential gaps for future consideration.

9. Test the delivered solution to ensure requirements are met.
-- Refer to the vendor documentation to control the quality and completeness of the procured solution in meeting the requirements within the RTM.
-- Add columns to the RTM for further traceability of the requirements through the SDLC. For example, 'Script #' and 'Tester' columns can be included to ensure each requirement has a corresponding test and tester during user acceptance testing.
-- Identify individuals who will be involved in user acceptance testing; ensure these staff are prepared for the testing process and know how to document testing results.

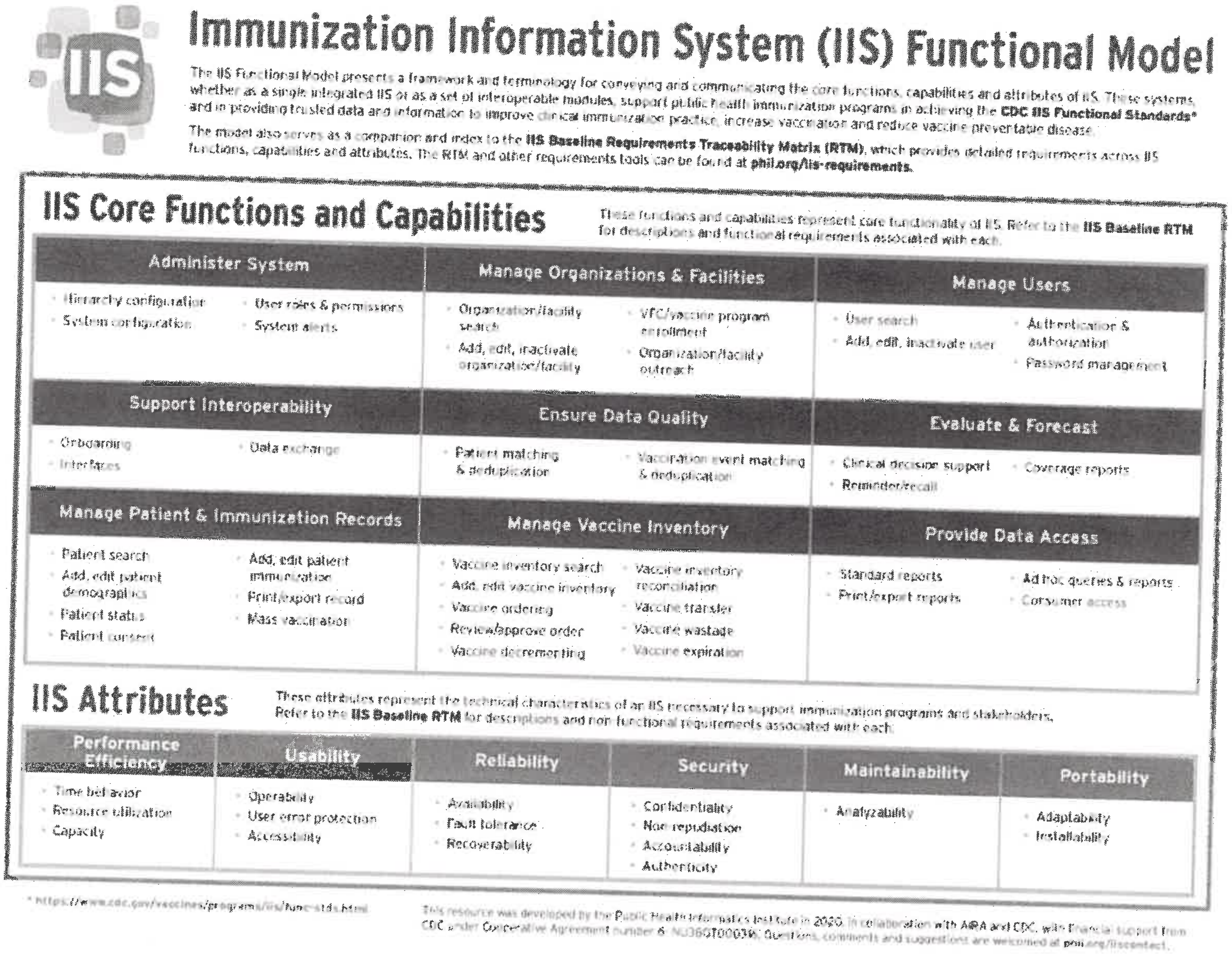
10. Update business processes & documentation, as needed
-- Update standard operating procedures to reflect and refine staff interaction with the new technology.

-- Be sure to train internal staff as well as external end-users.

Helpful Hints and Notes

-- The RTM can be used in conjunction with requirements definition tools, such as task flow diagrams. (For more information on PHII's Collaborative Requirements Development
-- On each tab, high-level requirements are shaded in blue; rows beneath each high level requirement provide further detail.
jurisdiction name.
-- Tabs can be added to the RTM to encompass business processes or business rules within the workbook.
-- Columns can be added to the RTM for further traceability of the requirements through the design, build, test and release activities. For example, a 'Script #' column can be
-- To be most effective in tracking a solution that meets program requirements, the RTM must be maintained throughout the system development life cycle.
differentiate those required for Day 1 and those that could be delivered in future releases.
-- Consider using an additional priority designation of 'R' for 'Required by Law' to indicate requirements that stem from jurisdictional laws/administrative rules. Provide a

Return to Cover Page



Immunization Information System (IIS) Functional Model

The IIS Functional Model presents a framework and terminology for conveying and communicating the core functions, capabilities and attributes of IIS. These systems, whether as a single integrated IIS or as a set of interoperable modules, support public health immunization programs in achieving the **CDC IIS Functional Standards*** and in providing trusted data and information to improve clinical immunization practice, increase vaccination and reduce vaccine preventable disease.

The model also serves as a companion and index to the **IIS Baseline Requirements Traceability Matrix (RTM)**, which provides detailed requirements across IIS functions, capabilities and attributes. The RTM and other requirements tools can be found at **phii.org/iis-requirements.**

IIS Core Functions and Capabilities

These functions and capabilities represent core functionality of IIS. Refer to the **IIS Baseline RTM** for descriptions and functional requirements associated with each.

Administer System

- Hierarchy configuration
- System configuration
- User roles & permissions
- System alerts

Manage Organizations & Facilities

- Organization/facility search
- Add, edit, inactivate organization/facility
- VFC/vaccine program enrollment
- Organization/facility outreach

Manage Users

- User search
- Add, edit, inactivate user
- Authentication & authorization
- Password management

Support Interoperability

- Onboarding
- Interfaces
- Data exchange

Ensure Data Quality

- Patient matching & deduplication
- Vaccination event matching & deduplication

Evaluate & Forecast

- Clinical decision support
- Reminder/recall
- Coverage reports

Manage Patient & Immunization Records

- Patient search
- Add, edit patient demographics
- Patient status
- Patient consent
- Add, edit patient immunization
- Print/export record
- Mass vaccination

Manage Vaccine Inventory

- Vaccine inventory search
- Add, edit vaccine inventory
- Vaccine ordering
- Review/approve order
- Vaccine decrementing
- Vaccine inventory reconciliation
- Vaccine transfer
- Vaccine wastage
- Vaccine expiration

Provide Data Access

- Standard reports
- Print/export reports
- Ad hoc queries & reports
- Consumer access

IIS Attributes

These attributes represent the technical characteristics of an IIS necessary to support immunization programs and stakeholders. Refer to the **IIS Baseline RTM** for descriptions and non-functional requirements associated with each.

Performance Efficiency	Usability	Reliability	Security	Maintainability	Portability
Time behavior Resource utilization Capacity	Operability User error protection Accessibility	Availability Fault tolerance Recoverability	Confidentiality Non-repudiation Accountability Authenticity	Analyzability	Adaptability Installability

* https://www.cdc.gov/vaccines/programs/iis/func-stds.html

This resource was developed by the Public Health Informatics Institute in 2020, in collaboration with AIRA and CDC, with financial support from CDC under Cooperative Agreement number 6 NU38OT000316. Questions, comments and suggestions are welcomed at phii.org/iiscontact.

IIS Functional Model descriptions

Return to Cover Page

Tab Name	# of Reqs	Function	Function Description	Capability	Capability Description
Admin System	61	Administer System	Management of global system settings and alerts, including set up of user roles and permissions.	Hierarchy Configuration	-- ability to create hierarchy that informs the association between geographical levels within the jurisdiction and among organizations, facilities, providers
				System Configuration	-- ability to define system-wide settings, such as management of code tables
				User Roles and Permissions	-- ability to define and manage user roles and use role permissions to perform a function, activity or task
				System Alerts	-- ability to broadcast communication to IIS users viewable upon logging into the system
Manage Orgs	83	Manage Organizations and Facilities	Management of organizations and facility accounts.	Organization/Facility Search	-- ability to look up and retrieve an organization or facility account
				Add, Edit, Inactivate	-- ability to add, edit or inactivate an organization or facility; ability for an organization to initiate enrollment and re-enrollment in the IIS
				VFC/Vaccine Program	-- ability to enroll and re-enroll a provider organization in VFC and/or other vaccine program(s)
				Organization/Facility	-- ability to communicate with organization/facility representatives
Manage Users	35	Manage Users	Management of user accounts.	User Search	-- ability to define parameters to look up and retrieve a user account
				Add, Edit, Inactivate User	-- ability to add, edit or inactivate a user account
				Authentication and	-- ability to validate a user's identity, entity and system permissions
				Password Management	-- ability to administer, change and reset user passwords
Interop	65	Support Interoperability	Manage interfaces to exchange data between the IIS and other systems.	Onboarding	-- ability to establish/re-establish/modify an interface with another information system for the electronic exchange of demographic and/or immunization
				Interfaces	-- ability to facilitate electronic data exchange with other information systems, including EHRs, VTrckS, jurisdictional vital records, and the IZ Gateway
				Data Exchange	-- ability to exchange data electronically and monitor and troubleshoot data exchange
Data Quality	32	Ensure Data Quality	Deduplication and consolidation of records	Patient Matching and	-- ability to identify and manage duplicate and potential duplicate patient records
				Vaccination Event Matching	-- ability to identify and manage duplicate and potential duplicate vaccination entries
Eval Forecast	64	Evaluate and Forecast	Determine the validity of past immunizations administered as a basis for determining	Clinical Decision Support	-- ability to evaluate and forecast immunizations for a patient per ACIP guidelines and in alignment with CDSi specifications
				Reminder/Recall	-- ability to identify and notify patients who are due for upcoming immunizations (reminder) and/or are past due (recall)
				Coverage Reports	-- ability to create reports to support immunization coverage assessment at the provider and geographic levels including reports for the CDC's VFC
Manage Pt Iz Record	83	Manage Patient and Immunization Records	Manage patient demographics and patient immunization record.	Patient Search	-- ability to look up and retrieve a patient record
				Add, Edit Patient	-- ability to add, edit or inactivate a patient record
				Patient Status	-- ability to manage the assignment of a specific patient to a provider organization or jurisdiction
				Patient Consent	-- ability to manage patient agreement to participate in the IIS in accordance with jurisdictional policy
				Add, Edit Patient	-- ability to add, edit an immunization record
				Print/Export Report	-- ability to print or export either a patient or immunization record
				Mass Vaccination	-- ability to capture a large volume of demographic and immunization data in emergency situations
Manage Vaccine Inv	87	Manage Vaccine Inventory	Order publicly-purchased vaccine and manage vaccine inventory.	Vaccine Inventory Search	-- ability to look up and retrieve vaccine doses in inventory
				Add, Edit Vaccine Inventory	-- ability to manage vaccine inventory, including ordering, storing and handling, and reconciliation of vaccine doses
				Vaccine Ordering	-- ability to order publicly funded vaccines as authorized
				Review/Approve Order	-- ability to review, edit, and authorize an organization's vaccine order for approval, submission and fulfillment
				Vaccine Dose Decrementing	-- ability to automatically decrement vaccine doses from inventory when matched vaccine doses are reported as administered
				Vaccine Inventory	-- ability to maintain an accurate count of vaccine doses available based on doses administered, wasted, transferred, and expired
				Vaccine Transfer	-- ability to transfer vaccine from one VFC provider organization to another in certain situations
				Vaccine Wastage	-- ability to manage nonviable vaccine reporting
				Vaccine Expiration	-- ability for notification and management of vaccine inventory expired and due to expire
Data Access	65	Provide Data Access	Provision of access to data and information.	Standard Reports	-- ability to generate pre-configured reports available and accessible in the IIS
				Ad Hoc Queries and Reports	-- ability to create, save and schedule data queries and customized reports on demand
				Print/Export Report	-- ability to generate data to print or use in other systems
				Consumer Access	-- ability for authorized consumers to directly access IIS data for which they are authorized

Tab Name	# of Reqs	Attribute	Description	Sub-Characteristic	Description
Non-functional	99	Performance	Performance efficiency relative to the amount of resources used under stated conditions.	Time behavior	-- degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements
				Resource utilization	-- degree to which the amounts and types of resources used by a product or system, when performing its functions, meet requirements
				Capacity	-- degree to which the maximum limits of a product or system parameter meet requirements
		Usability	Degree to which a product or system can be used by specified users to achieve specified goals	Operability	-- degree to which a product or system has attributes that make it easy to operate and control
				User error protection	-- degree to which a system protects users against making errors
				Accessibility	-- degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a
		Reliability	Degree to which a system, product or component performs specified functions under specified	Availability	-- degree to which a system, product or component is operational and accessible when required for use
				Fault tolerance	-- degree to which a system, product or component operates as intended despite the presence of hardware or software faults
				Recoverability	-- degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired
		Security	Degree to which a product or system protects information and data so that persons or other products or systems have the	Confidentiality	-- degree to which a product or system ensures that data are accessible only to those authorized to have access
				Non-repudiation	-- degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later
				Accountability	-- degree to which the actions of an entity can be traced uniquely to the entity
				Authenticity	-- degree to which the identity of a subject or resource can be proved to be the one claimed

IIS Functional Model descriptions

Return to Cover Page

Tab Name	# of Reqs	Function	Function Description	Capability	Capability Description
		Maintainability	Degree of effectiveness and	**Analyzability**	-- degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its
		Portability	Degree of effectiveness and efficiency with which a system,	**Adaptability**	-- degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or
				Installability	-- degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment
	674				

RTM Format

Return to Cover Page

Status	Req. #*	Capability/Attribute	***Requirement: The IIS must/should have...	Comments	Reviewer notes	Priority: E, O (essential, optional)**	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Updated from the previous version of the RTM or newly added.	[Req. ID]	[Capability/attribute name, e.g., "System Configuration"]	[high-level requirement]	--Suggested recommendations for the requirement. --Indication of relationship to a priority cross-functional need such as mass vaccination or school reports.	[Reviewer notes related to: -- Organization of the requirement (in terms of its associated capability and/or function) -- Wording of the requirement -- Misc thoughts]	[Draft priority designation, e.g. "E"]		
Updated from the previous version of the RTM or newly added.	[Req. ID]	[Capability/attribute name, e.g., 'System Configuration']	[detailed requirement]	--Suggested recommendations for the requirement. --Indication of relationship to a priority cross-functional need such as mass vaccination or school reports.	[Reviewer notes related to: -- Organization of the requirement (in terms of its associated capability and/or function) -- Wording of the requirement -- Misc thoughts]	[Draft priority designation, e.g. "E"]		

*Numbering/identification of individual requirements will occur at the very end of the review and revision process, once requirements are final.

**Priority designations:
E: Essential: Baseline, critical requirement reflective of core functionality/attribute for a viable IIS as defined by CDC.
O: Optional: Not essential for all IIS as defined by CDC.

*** Rows highlighted in blue indicate a high-level requirement

Function: Administer System

Return to Cover Page

Capability	Requirement: The IIS must/should...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: indicate the anticipated cost and timeline for development and release.
Hierarchy Configuration	ability to establish the IIS hierarchy to associate and manage relationships between entities	E	Yes	
Hierarchy Configuration	ability to associate user(s) to a facility	E	Yes	
Hierarchy Configuration	ability to associate clinician(s) to a facility	E	Yes	
Hierarchy Configuration	ability to associate facility/facilities to an organization	E	Yes	
Hierarchy Configuration	ability to establish geographic jurisdictional hierarchy	E	Yes	
Hierarchy Configuration	ability to aggregate data across user-defined hierarchies	E	Yes	
System Configuration	ability to maintain inventory availability in IIS visible to authorized users	E	Yes	
System Configuration	ability for jurisdictional admin to maintain separate VFC supplied inventory in the IIS	E	Yes	
System Configuration	ability for jurisdictional admin to maintain separate jurisdiction supplied inventory	E	Yes	
System Configuration	ability for jurisdictional admin to maintain separate private stock inventory	E	Yes	
System Configuration	ability for jurisdictional admin to manage code sets	E	Yes	
System Configuration	ability for jurisdictional admin to update NDC codes	E	Yes	
System Configuration	ability for jurisdictional admin to update CVX codes	E	Yes	
System Configuration	ability for jurisdictional admin to update MVX codes	E	Yes	
System Configuration	ability to configure default values to minimize data input	E	Yes	
System Configuration	ability to display an error message in the user interface when minimum information required is not complete	E	Yes	
System Configuration	ability to standardize addresses per US Postal conventions and codes	E	Yes	
System Configuration	ability to verify validity of addresses (as valid USPS addresses) in the IIS through electronic means (e.g., SmartyStreets)	E	Yes	
System Configuration	ability to geocode addresses	E	Yes	
System Configuration	ability to validate accurate assignment of address to an individual through electronic means (e.g., LexisNexis)	O	Yes	
System Configuration	ability for jurisdictional admin to modify facility types according to immunization program descriptions and CDC VFC Program descriptions	E	Yes	
System Configuration	ability for jurisdictional admin to configure rules governing data validation of incoming HL7 messages	E	Yes	
System Configuration	ability to configure an authorization agreement as per jurisdictional policy	O	Yes	
System Configuration	ability to configure a user agreement as per jurisdictional policy	O	Yes	
System Configuration	ability to display age in year/month/day format in all age display fields (e.g., 2 years, 4 months, 3 days)	E	Yes	
System Configuration	ability to provide optional calendar to select a date in a web client	O	Yes	
System Configuration	ability to add patient priority group indicators	E	Yes	
System Configuration	ability to modify patient priority group indicators	E	Yes	
System Configuration	ability for jurisdictional admin to manage business rules related to data quality	E	Yes	
System Configuration	ability for jurisdictional admin to specify business rules for monitoring data quality	E	Yes	
System Configuration	ability for jurisdictional admin to modify business rules for monitoring data quality	E	Yes	
System Configuration	ability to configure the organization enrollment form	E	Yes	
System Configuration	support rules-based logic to suggest approval or rejection of enrollment form based on review of completed fields	E	Yes	
System Configuration	ability to manage rules-based logic for approval or rejection of enrollment form	E	Yes	
System Configuration	ability for jurisdictional admin to create enrollment forms based on program requirements	E	Yes	
System Configuration	ability for jurisdictional admin to modify an enrollment form	E	Yes	
System Configuration	ability to auto-populate existing user information in the IIS with the information on the enrollment form when creating a new facility in the IIS	O	Yes	
System Configuration	ability to auto-populate the organization information in the IIS with information on the enrollment form when creating a new organization in the IIS	O	Yes	
System Configuration	ability for jurisdictional admin to configure vaccine forecasting business rules	E	Yes	
System Configuration	ability to apply effective dates to vaccine rules	O	Yes	
System Configuration	ability to incorporate new vaccines per ACIP into the forecasting algorithm	E	Yes	
System Configuration	ability to support a record search algorithm to return "best matches"	E	Yes	
System Configuration	ability for jurisdictional admin to configure the number of search results to be displayed per jurisdictional policy	E	Yes	
System Configuration	ability for jurisdictional admin to modify required parameters for patient searches	E	Yes	
System Configuration	ability to restrict certain data from being included in reports such as sensitive demographic information e.g , address, phone number, mother's maiden name, Medicaid ID	E	Yes	
System Configuration	ability to open multiple screens simultaneously within the application	O	Yes	
User Roles and Permissi	ability for jurisdictional admin to manage user roles and permissions by task per jurisdictional policy	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to add user roles with distinct permissions	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to modify user roles with distinct permissions	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to inactivate user roles	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to modify permissions to IIS processes and data for specific user roles	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to restrict system functionality by user role	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to restrict authorized user access to data based on user role	E	Yes	
User Roles and Permissi	ability for jurisdictional admin to enable access to standard reports based on user role	E	Yes	
User Roles and Permissi	ability to automatically update all users assigned to a role based on changes made to the "master" role attributes	E	Yes	
System Alerts	ability for jurisdictional admin to manage system alerts	E	Yes	
System Alerts	ability to view global messages upon logging into the application	E	Yes	
System Alerts	ability for jurisdictional admin to add system alerts for specific IIS users to view when logging into application	O	Yes	
System Alerts	ability for jurisdictional admin to add global messages	E	Yes	
System Alerts	ability for jurisdictional admin to edit global messages	E	Yes	
System Alerts	ability for jurisdictional admin to inactivate global messages	E	Yes	

Function: Manage Organizations and Facilities

turn to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: indicate the anticipated cost and timeline for development and release.
Organization/Facility	ability to search organization/facility information stored in the IIS	E	Yes	
Organization/Facility	ability for jurisdictional admin to search organizations/facilities by user-defined parameters	E	Yes	
Organization/Facility	ability to clear and re-enter search criteria when searching for an organization/facility	E	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized (non-participating/enrolled) organization to enroll electronically for participation in the IIS	E	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized organization to add IIS enrollment information online	E	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized org to submit IIS enrollment information online	E	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized org to save partially complete IIS enrollment information	O	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized org to return to a partially complete IIS enrollment information	O	Yes	
Add, Edit, Inactivate	ability to prevent submission of incomplete IIS enrollment information when required field(s) are missing	E	Yes	
Add, Edit, Inactivate	ability to electronically notify the applicant of incomplete IIS enrollment information specifying the missing required fields	E	Yes	
Add, Edit, Inactivate	ability to electronically notify applicant that IIS enrollment information has been submitted	E	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized org to edit rejected IIS enrollment information	E	Yes	
Add, Edit, Inactivate	ability for applicant from unauthorized org to resubmit a rejected IIS enrollment	E	Yes	
Add, Edit, Inactivate	ability to capture electronic signature for enrollment, for an authorization agreement	O	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to manage organization/facility IIS enrollment	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to manage organization/facility IIS enrollment status	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to inactivate an organization	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to reactivate an organization	E	Yes	
Add, Edit, Inactivate	ability to store IIS enrollment status for an organization/facility	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to inactivate a facility	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to reactivate a facility	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to electronically approve IIS enrollment	E	Yes	
Add, Edit, Inactivate	ability to include reason for rejecting IIS enrollment of an organization	E	Yes	
Add, Edit, Inactivate	ability to electronically notify the organization that the submitted enrollment was rejected along with the reason	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to manage organization and facility records within the IIS	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to add an organization	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to modify an organization record	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to add a facility	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to modify a facility record	E	Yes	
Add, Edit, Inactivate	ability to automatically generate unique facility IIS ID	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to associate a facility to an organization	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to edit association between a facility an organization	E	Yes	
Add, Edit, Inactivate	ability to store multiple unique facility site IDs associated with a particular facility (to facilitate matching of facilities between the IIS and other data systems)	E	Yes	
Add, Edit, Inactivate	ability to capture a facility's mailing address	E	Yes	
Add, Edit, Inactivate	ability to capture a facility's shipping address	E	Yes	
Add, Edit, Inactivate	ability to enter contact information for the facility contact	E	Yes	
Add, Edit, Inactivate	ability to enter contact information for an optional contact	E	Yes	
Add, Edit, Inactivate	ability to indicate if an organization/facility is a site where immunizations are administered	E	Yes	
Add, Edit, Inactivate	ability to indicate if an organization/facility is a site where vaccines are stored for redistribution	O	Yes	
Add, Edit, Inactivate	ability to save documents (i.e., enrollment/onboarding documents, storage and handling, borrowing, temperature logs, wastage, etc.) to specific organization/facility file folder per policy	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to retrieve electronic files from provider file folder	E	Yes	
Add, Edit, Inactivate	ability for jurisdictional admin to record notes related to a organization/facility	E	Yes	
Add, Edit, Inactivate	ability to flag an organization as participating in VFC and/or other user-defined vaccine program(s)	E	Yes	
Add, Edit, Inactivate	ability to retrieve organization/facility information from scanned forms and automatically fill required data fields with retrieved information	O	Yes	
VFC/Vaccine Program	ability for an organization to submit vaccine program enrollment information electronically	E	Yes	
VFC/Vaccine Program	ability to capture electronic signature for vaccine program enrollment	E	Yes	
VFC/Vaccine Program	ability to access the vaccine program agreement in a separate window from the vaccine program enrollment	E	Yes	
VFC/Vaccine Program	ability to provide link to the blank formatted vaccine program enrollment form	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to assign a VFC pin number to a newly enrolled VFC site	E	Yes	
VFC/Vaccine Program	ability to select the type of certified monitoring device being used to record temperatures	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to document that a facility has a certificate of calibration for the temperature monitoring device	O	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to approve a vaccine program enrollment	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to enter an expiration date for a vaccine program enrollment	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to document that the vaccine program facility has a routine and emergency vaccine management plan	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to document that a facility participating in VFC has a VFC Coordinator annual training certificate	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to document that a facility participating in VFC has a Backup Coordinator annual training certificate	E	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to add comments during the vaccine program enrollment approval process	O	Yes	
VFC/Vaccine Program	ability to require the vaccine program facility to indicate the number of vaccine storage units being monitored	O	Yes	
VFC/Vaccine Program	ability to require the vaccine program facility to indicate the types of vaccine storage units being monitored	O	Yes	
VFC/Vaccine Program	ability to require the vaccine program facility to indicate whether they store Varicella and MMRV vaccine	E	Yes	
VFC/Vaccine Program	ability to enter contact information for the facility Primary Vaccine Coordinator	E	Yes	
VFC/Vaccine Program	ability to enter contact information for the facility Backup Vaccine Coordinator	E	Yes	
VFC/Vaccine Program	ability to enter contact information for the facility vaccine program Agreement Signatory	E	Yes	
VFC/Vaccine Program	ability to capture the day of the week that a vaccine program facility may receive vaccine shipments	E	Yes	
VFC/Vaccine Program	ability to capture the time that a vaccine program facility may receive vaccine shipments	E	Yes	
VFC/Vaccine Program	ability to automatically turn off vaccine ordering capabilities for a facility that does not have an up-to-date vaccine program enrollment	E	Yes	
VFC/Vaccine Program	ability to capture required information for VFC clinician: last name, first name, title, medical license number, NPI number, still active with facility, are they a signatory, specialty (FP, Peds) during the enrollment process	E	Yes	
VFC/Vaccine Program	ability to attach VFC documentation (in multiple formats) such as: VFC training certification, certificate of calibration, medical license, floor design diagram and other documents	E	Yes	
VFC/Vaccine Program	ability for IIS staff to retrieve electronic files from organization/facility file folder	O	Yes	
VFC/Vaccine Program	ability to automatically validate clinician license number against Professional Licensing Agency record database	O	Yes	
VFC/Vaccine Program	ability to submit vaccine program re-enrollment data electronically	E	Yes	

Function: Manage Organizations and Facilities

turn to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization, indicate the anticipated cost and timeline for development and release.
VFC/Vaccine Program	ability to electronically notify a facility VFC/vaccine program coordinator of an upcoming need for VFC/vaccine program re-enrollment	O	Yes	
VFC/Vaccine Program	ability for the jurisdictional vaccine program admin to modify the date for online renewal electronic notifications for each vaccine program facility	E	Yes	
VFC/Vaccine Program	ability to suspend ordering capabilities for a facility pending approval of vaccine program enrollment	E	Yes	
VFC/Vaccine Program	ability to re-activate ordering capabilities for a facility when a vaccine program enrollment is approved	E	Yes	
Organization/Facility	ability to send electronic communications to organization/facility contacts	E	Yes	
Organization/Facility	ability to send a final electronic notification reminder, re: renewal, to all VFC facilities that have not completed the renewal by their expiration date	E	Yes	
Organization/Facility	ability to send electronic communications directly from the IIS	O	Yes	
Organization/Facility	ability to send electronic communications directly from the IIS to multiple recipients	O	Yes	
Organization/Facility	ability to notify more than one user at a participating vaccine program facility of any vaccine program notification	O	Yes	
Organization/Facility	ability for the jurisdictional vaccine program admin to customize vaccine program enrollment alerts to participating vaccine program facilities when needed	O	Yes	
Organization/Facility	ability for the jurisdictional vaccine program admin to modify the date for online renewal electronic notifications for each participating vaccine program facility	O	Yes	
Organization/Facility	ability to electronically notify the jurisdictional vaccine program admin of vaccine program follow-up activities for a new vaccine program facility enrolled for 6 months	O	Yes	

Function: Manage Users

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
User Search	ability for jurisdictional admin to search for user accounts by user-defined criteria	E	Yes	
User Search	ability for jurisdictional admin to view all user accounts	E	Yes	
User Search	ability for organization admin to search all user accounts associated with their organization	E	Yes	
User Search	ability for organization admin to view all user accounts associated with their organization	E	Yes	
User Search	ability to sort users by user defined-criteria	O	Yes	
Add, Edit, Inactivate User	ability for admin to manage user accounts	E	Yes	
Add, Edit, Inactivate User	ability to track the progress of a new user registration	O	Yes	
Add, Edit, Inactivate User	ability for admin to add new users	E	Yes	
Add, Edit, Inactivate User	ability for admin to modify user accounts	E	Yes	
Add, Edit, Inactivate User	ability for admin to inactivate user accounts	E	Yes	
Add, Edit, Inactivate User	ability for jurisdictional admin to inactivate multiple accounts in one transaction	O	Yes	
Add, Edit, Inactivate User	ability for organization admin to inactivate user accounts associated with their organization	E	Yes	
Add, Edit, Inactivate User	ability to store reason for inactivation of user account	E	Yes	
Add, Edit, Inactivate User	ability for jurisdictional admin to reactivate an inactivated account	E	Yes	
Add, Edit, Inactivate User	ability to electronically notify a user that their account is locked (inaccessible) as per jurisdictional security policy	O	Yes	
Add, Edit, Inactivate User	ability to electronically notify a user that their account is inactive	O	Yes	
Add, Edit, Inactivate User	capture clinician activity status (out of state, loss of certification, change of practice status, other)	O	Yes	
Add, Edit, Inactivate User	ability for jurisdictional admin to assign a role to authorized users	E	Yes	
Add, Edit, Inactivate User	ability for organization admin to assign a role to authorized users within their organization	E	Yes	
Authentication & Authorization	ability to authenticate user	E	Yes	
Authentication & Authorization	ability to access the system through an authorized username and password	E	Yes	
Authentication & Authorization	ability to support access via single-sign in for jurisdictional users	O	Yes	
Authentication & Authorization	ability to switch between multiple organizations	O	Yes	
Authentication & Authorization	ability to view jurisdictional policy agreements	E	Yes	
Authentication & Authorization	support multi-factor authentication per jurisdictional policy	O	Yes	
Password Management	ability to generate electronic notification to authorized user of account credentials	E	Yes	
Password Management	ability to electronically notify authorized users of their username	E	Yes	
Password Management	ability to electronically notify authorized users of their temporary password in a separate notification	E	Yes	
Password Management	ability to generate electronic notification at periodic intervals to authorized users of their pending account password expiration	E	Yes	
Password Management	ability for jurisdictional admin to configure the periodic intervals for generation of notifications to authorized users of their pending account password expiration	O	Yes	
Password Management	ability to support temporary password which will be required to change during initial log in	E	Yes	
Password Management	ability to support temporary password which will expire in X number of days determined by policy	E	Yes	
Password Management	ability for users to change their own passwords per program/jurisdiction security policy	E	Yes	
Password Management	ability for users to reset their password per program/jurisdiction security policy	E	Yes	
Password Management	ability to prompt users to change their password at time intervals per program/jurisdiction security policy	E	Yes	

Function: Support Interoperability

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Onboarding	ability to onboard organizations/facilities to facilitate electronic data exchange	E	Yes	
Onboarding	ability to track an organization's/facility's progress through the onboarding process	O	Yes	
Onboarding	ability to capture EHR system specification details	E	Yes	
Onboarding	ability to create a unique username to assign to the organizations/facilities during the test phase	E	Yes	
Onboarding	ability to create a unique password to assign to the organizations/facilities during the test phase	E	Yes	
Onboarding	ability to electronically alert the vendor/organization when the certificate for transport is going to expire in X time period	E	Yes	
Onboarding	ability to store digital certificate information	E	Yes	
Onboarding	ability to validate that the transport layer between the test site and IIS is functional	E	Yes	
Onboarding	ability to validate system connectivity prior to the submission of test data	E	Yes	
Onboarding	ability to identify data formatting errors during testing	E	Yes	
Onboarding	ability to provide test message submission summary report to the EHR vendor	E	Yes	
Onboarding	ability for EHR vendor to view details regarding the processing of test data in terms of errors and warnings in the messages	E	Yes	
Onboarding	ability for IIS authorized staff to review and approve onboarding forms	E	Yes	
Onboarding	ability for IIS staff to review and reject onboarding forms	E	Yes	
Onboarding	ability for applicant to edit a rejected onboarding application	E	Yes	
Onboarding	ability for applicant to save a rejected onboarding application	E	Yes	
Onboarding	ability for applicant to resubmit a rejected onboarding application	E	Yes	
Onboarding	ability to compare onboarding application information to current records to determine most current data	E	Yes	
Interfaces	ability to interface with other systems to facilitate electronic data sharing/exchange per jurisdictional policy	E	Yes	
Interfaces	ability to interface with electronic health record systems	E	Yes	
Interfaces	ability to interface with the Immunization Gateway	E	Yes	
Interfaces	ability to interface with an application that facilitates patient scheduling	E	Yes	
Interfaces	ability to exchange data with CDC Vaccine Tracking System (VTrckS) based on most current CDC ExIS Specifications	E	Yes	
Interfaces	ability to order vaccine via electronic interface with VTrckS	E	Yes	
Interfaces	ability to receive vaccine inventory/shipping information	E	Yes	
Interfaces	ability to batch export vaccine inventory for submission to VTrckS	E	Yes	
Interfaces	ability to batch export vaccine ordering information for submission to VTrckS	E	Yes	
Interfaces	ability to batch export facility information	E	Yes	
Interfaces	ability to export vaccine return and wastage data to VTrckS	E	Yes	
Interfaces	ability to use the VTrckS-API for file exchange between the IIS and VTrckS based on CDC requirements and API file specifications	O	Yes	
Interfaces	ability to receive data through an interface with jurisdictional vital records system	E	Yes	
Interfaces	ability to update IIS data from Vital Records for birth events	E	Yes	
Interfaces	ability to update IIS data from Vital Records for death events	E	Yes	
Interfaces	ability to update IIS data from Vital Records for adoption events	E	Yes	
Interfaces	ability to update IIS data from Vital Records for name change events	E	Yes	
Interfaces	ability to detect if a newborn record is a potential duplicate in the IIS	E	Yes	
Interfaces	ability to use new Vital Record data for matched records to update patient demographic data	E	Yes	
Interfaces	ability to update the IIS with date of death from Vital Records data	E	Yes	
Interfaces	ability to prevent updates to IIS records	O	Yes	
Data Exchange	ability to support real-time data exchange per the CDC HL7 implementation guide	E	yes	
Data Exchange	ability to process an HL7 message	E	Yes	
Data Exchange	ability to respond to an HL7 message	E	Yes	
Data Exchange	ability to create an HL7 message	E	Yes	
Data Exchange	ability to capture IIS Core Data Elements	E	Yes	
Data Exchange	ability to store IIS Core Data Elements	E	Yes	
Data Exchange	ability to accept last prior version of HL7 messages	E	Yes	
Data Exchange	ability to manually correct a submitted record and resubmit for processing	O	Yes	
Data Exchange	ability to support data exchange in non-HL7 format	E	Yes	
Data Exchange	ability to import bulk patient demographic information into IIS	E	Yes	
Data Exchange	ability to import bulk immunization information into IIS	E	Yes	
Data Exchange	ability to export routine, seasonal, and emergency vaccination files (aggregate and de-identified)	E	Yes	
Data Exchange	ability to export routine, seasonal, and emergency vaccination files (aggregate and de-identified) automatically via CDC approved	O	Yes	
Data Exchange	ability to monitor and troubleshoot data exchange	E	Yes	

Function: Support Interoperability

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Data Exchange	ability to view VXU messages submitted by an organization	E	Yes	
Data Exchange	ability to view HL7 messages for an organization within a defined date range per jurisdictional policy	E	Yes	
Data Exchange	ability to view HL7 ACK messages generated for an organization	E	Yes	
Data Exchange	ability to view incoming HL7 QBP messages submitted by an organization	E	Yes	
Data Exchange	ability to view RSP messages generated for an organization	E	Yes	
Data Exchange	ability to log acknowledgement messages indicating warnings and errors	E	Yes	
Data Exchange	ability to retrieve error messages within a specified date range by organization	E	Yes	
Data Exchange	ability to retrieve acknowledgment messages within a specified date range by organization	E	Yes	
Data Exchange	ability to filter error messages	E	Yes	
Data Exchange	ability to filter acknowledgement messages	E	Yes	
Data Exchange	ability to sort error messages	E	Yes	
Data Exchange	ability to sort acknowledgement messages	E	Yes	

Function: Ensure Data Quality

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release
Patient Matching &	ability to prevent duplicate patient records in the IIS database	E	Yes	
Patient Matching &	ability to automatically identify incoming patient records as potential duplicates	E	Yes	
Patient Matching &	ability to automatically identify existing patient records as potential duplicates	E	Yes	
Patient Matching &	ability to automatically consolidate two or more duplicate records	E	Yes	
Patient Matching &	ability to generate electronic notification of potential duplicates for manual review	E	Yes	
Patient Matching &	ability to automatically match an incoming patient record with existing records to avoid a duplicate record being created	E	Yes	
Patient Matching &	ability to set thresholds for patient matching	E	Yes	
Patient Matching &	ability to view all potential duplicate patient records for an individual patient simultaneously	E	Yes	
Patient Matching &	ability for jurisdictional admin to edit thresholds to increase the probability of a match	E	Yes	
Patient Matching &	ability for jurisdictional admin to edit thresholds to reduce the probability of a match	E	Yes	
Patient Matching &	ability to flag potential duplicate patient records for manual review that cannot be resolved automatically	E	Yes	
Patient Matching &	ability to view all potential duplicate patient records simultaneously	E	Yes	
Patient Matching &	ability for admin to manually merge patient records	E	Yes	
Patient Matching &	ability for organizational/facility user to manually merge patient records from their own organization/facility	E	Yes	
Patient Matching &	ability to manually flag two or more patient records as potential duplicates	E	Yes	
Patient Matching &	ability to prevent manual review of records previously indicated as "not a duplicate"	E	Yes	
Patient Matching &	ability to flag a patient as "not a duplicate" during manual review	E	Yes	
Patient Matching &	ability to maintain "not a duplicate" flag for resolved patient records	E	Yes	
Patient Matching &	ability to select data elements from the patient records to maintain within the consolidated record	E	Yes	
Patient Matching &	ability to retain "pre-merged" records for reference	E	Yes	
Patient Matching &	ability to separate patient records that were incorrectly merged	E	Yes	
Vaccination Event	ability to prevent potential duplicate vaccination events at the immunization level	E	Yes	
Vaccination Event	ability to automatically identify incoming vaccination event as potential duplicates	E	Yes	
Vaccination Event	ability to automatically select the most accurate vaccination event based on deduplication rules	E	Yes	
Vaccination Event	ability to automatically identify existing vaccination events as potential duplicates	E	Yes	
Vaccination Event	ability to manually flag potential duplicate vaccination events for manual review	E	Yes	
Vaccination Event	ability to display potential duplicate vaccine records for an individual patient	E	Yes	
Vaccination Event	ability to manually merge a duplicate vaccination event	E	Yes	
Vaccination Event	ability to manually delete a duplicate vaccination event	E	Yes	
Vaccination Event	ability to automatically consolidate two or more duplicate vaccination events	E	Yes	
Vaccination Event	ability to retain "pre-merged" or "pre-consolidated" vaccination events for reference	E	Yes	
Vaccination Event	ability to separate vaccination events that were incorrectly merged or consolidated	E	Yes	

Function: Evaluate and Forecast

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Clinical Decision Support	**ability to provide immunization clinical decision support according to ACIP recommendations**	E	Yes	
Clinical Decision Support	ability to support a vaccine clinical decision support algorithm aligned with the CDC CDSi logic specifications	E	Yes	
Clinical Decision Support	ability for jurisdictional admin to update the CDS rules	E	Yes	
Clinical Decision Support	ability to evaluate a patient's' immunization history according to the ACIP Child and Adolescent	E	Yes	
Clinical Decision Support	ability to evaluate a patient's' immunization history according to the ACIP Recommended Catch-up	E	Yes	
Clinical Decision Support	ability to evaluate a patient's' immunization history according to the ACIP Adult Immunization Schedule	E	Yes	
Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Child and Adolescent Immunization Schedule and	E	Yes	
Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Recommended Catch-up Immunization Schedule	E	Yes	
Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Adult Immunization Schedule and a patient's	E	Yes	
Clinical Decision Support	ability to display and highlight vaccines that are due	E	Yes	
Clinical Decision Support	ability to display and highlight vaccines that are overdue	E	Yes	
Clinical Decision Support	ability to display an indication when a vaccine series is complete	E	Yes	
Clinical Decision Support	ability to display vaccine-specific contraindications according to CDC lists of vaccine contraindications	O	Yes	
Clinical Decision Support	ability to take into account contraindications and precautions in the vaccine forecast	E	Yes	
Clinical Decision Support	ability to take into account evidence of immunity in the vaccine forecast	E	Yes	
Clinical Decision Support	ability to generate a forecast of specific vaccines required for individuals who travel outside the US	O	Yes	
Clinical Decision Support	ability to maintain historical records of effective dates of previous forecast schedules	O	Yes	
Clinical Decision Support	ability to review an immunization schedule that was appropriate at the time of administration	O	Yes	
Clinical Decision Support	ability to apply an immunization schedule that was appropriate at the time of administration	O	Yes	
Clinical Decision Support	ability to account for immune globulins in vaccine forecasting	E	Yes	
Clinical Decision Support	ability to create test cases for reuse during user acceptance testing	E	Yes	
Clinical Decision Support	ability to save test cases for reuse during user acceptance testing	E	Yes	
Clinical Decision Support	ability to compare the expected results of the forecasting test case to the actual results observed by the	E	Yes	
Reminder/Recall	**ability to generate patient-specific reminder/recall notifications**	E	Yes	
Reminder/Recall	ability to select one or more vaccines for generating reminder/recall notifications	E	Yes	
Reminder/Recall	ability to view the date the reminder/recall notice was sent to a patient	O	Yes	
Reminder/Recall	ability to generate lists of patients in need of a reminder or recall notification by organization	E	Yes	
Reminder/Recall	ability to generate reminder/recall notifications per consent designation	E	Yes	
Reminder/Recall	**ability to generate patient-specific reminder/recall notices by user-defined parameters**	E	Yes	
Reminder/Recall	ability to generate reminder/recall in user-defined format	E	Yes	
Reminder/Recall	ability to select the age of the cohort when generating reminder/recall notifications	E	Yes	
Reminder/Recall	ability to print patient-specific reminder/recall notices by user-defined parameters	E	Yes	
Reminder/Recall	ability to generate patient specific reminder/recalls in a user-defined format	E	Yes	
Reminder/Recall	ability for an end user to generate patient specific reminder/recalls in accordance with HIPAA and	E	Yes	
Reminder/Recall	ability for an end user to print patient specific reminder/recalls in accordance with HIPAA and jurisdictional	E	Yes	
Reminder/Recall	ability to generate vaccine recall notices by facility based on vaccine name, vaccination date range, and lot	O	Yes	
Reminder/Recall	ability to generate vaccine recall notices by administering provider based on vaccine name, vaccination date	O	Yes	
Reminder/Recall	ability to set the limit/number of times a patient will receive a reminder/recall	O	Yes	
Reminder/Recall	ability to modify the limit/number of times a patient will receive a reminder/recall	O	Yes	
Reminder/Recall	ability to exclude a patient who has met the limit/number of times to receive a reminder/recall	O	Yes	
Reminder/Recall	ability to generate a list of phone numbers for patients needing reminder/recall	O	Yes	
Reminder/Recall	**ability to manually review a patient list for a reminder/recall notification**	E	Yes	
Reminder/Recall	ability to flag patients to exclude before sending a reminder/recall notification	O	Yes	
Reminder/Recall	ability to establish a time interval between reminder recall notices (e.g., 90 days or 60 days)	O	Yes	
Reminder/Recall	ability to generate a reminder/recall notifications for patients with an active status for their organization	E	Yes	
Reminder/Recall	ability to generate reports that include reminder/recall history for specific date range	O	Yes	
Reminder/Recall	ability to make all reminder/recall data accessible to authorized users for a predetermined period of time	O	Yes	
Reminder/Recall	ability to aggregate multiple notices going to the same address into one notification	O	Yes	

Function: Evaluate and Forecast

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Coverage Reports	ability to generate report(s) displaying information on immunization coverage rate(s) among select	E	Yes	
Coverage Reports	ability to generate report(s) for organizations and facilities per CDC Immunization Quality Improvement for	E	Yes	
Coverage Reports	ability to generate report(s) on immunization coverage for a user-defined geographic area	E	Yes	
Coverage Reports	ability to generate report(s) on immunization coverage for a patient cohort	E	Yes	
Coverage Reports	ability to view and modify list of patients to be included in immunization coverage report	O	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage trends over time, over a selected timeframe	E	Yes	
Coverage Reports	ability to generate report(s) that display the number of missed opportunities for vaccination	E	Yes	
Coverage Reports	ability to generate report(s) displaying the number of patients late up-to-date for immunization who are up-	E	Yes	
Coverage Reports	ability to generate report(s) that display the number of invalid vaccine doses	E	Yes	
Coverage Reports	ability to generate report(s) displaying vaccine exemption rates	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by user-defined parameters	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by vaccine type	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by age range	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by ethnicity	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by race	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by patient sex	O	Yes	

Function: Manage Patient and Immunization Records

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Patient Search	**ability to search for patient records**	E	Yes	
Patient Search	ability to search patient record based on one or multiple user-defined parameters	E	Yes	
Patient Search	ability to re-search for a patient record by modifying existing search parameters	E	Yes	
Patient Search	ability to display the list of returned possible patient matches per jurisdictional policy	E	Yes	
Patient Search	ability to select a patient record from the list of possible patient matches	E	Yes	
Add, Edit Patient	**ability to add demographic information to a patient record**	E	Yes	
Add, Edit Patient	ability to create a new patient record	E	Yes	
Add, Edit Patient	ability to edit demographic information in a patient record	E	Yes	
Add, Edit Patient	ability to insert permanent comments in a patient's record that can be viewed based on	E	Yes	
Add, Edit Patient	ability to display the user who created the permanent comment in a patient's record	E	Yes	
Add, Edit Patient	ability to prevent a patient record from being saved unless required fields are completed, per	E	Yes	
Add, Edit Patient	ability to automatically notify a user when attempting to submit an incomplete patient record	E	Yes	
Add, Edit Patient	ability to store CDC-endorsed core data elements for all patient records	E	Yes	
Add, Edit Patient	ability to store multiple of reported names for each patient to include: first name, middle name, last	E	Yes	
Add, Edit Patient	ability to store multiple patient addresses	O	Yes	
Add, Edit Patient	ability to support multiple patient address type designations (e.g. primary address, vacation address)	O	Yes	
Add, Edit Patient	ability to identify effective dates for use of a patient address	O	Yes	
Add, Edit Patient	ability to store all historic addresses for a patient	O	Yes	
Add, Edit Patient	ability to store country information related to where the patient was born	O	Yes	
demographics	SmartyStreets)	O	Yes	
Add, edit patient	SmartyStreets)	O	Yes	
Add, Edit Patient	ability to automatically create a unique patient ID number	E	Yes	
Add, Edit Patient	ability to automatically associate patient ID number to the patient's record	E	Yes	
Add, Edit Patient	ability to track patients of all ages per jurisdictional law or policy	E	Yes	
Add, Edit Patient	ability to store mother's HBsAg status for a patient	O	Yes	
Add, Edit Patient	ability to store a patient's occupation	E	Yes	
Add, Edit Patient	ability to designate patient as belonging to a priority group for vaccination	O	Yes	
Add, Edit Patient	ability to store multiple patient identifiers	E	Yes	
Add, Edit Patient	ability to assign patient records to a cohort	E	Yes	
Add, Edit Patient	ability to assign patient records to multiple cohorts	E	Yes	
Add, Edit Patient	ability to view patient records by cohort	E	Yes	
Add, Edit Patient	ability to remove patient records from a cohort	E	Yes	
Patient Status	**ability to manage patient status at the organization/facility level**	E	Yes	
Patient Status	ability to store active patient status at the organization/facility level	E	Yes	
Patient Status	ability to store inactive patient status at the organization/facility level	E	Yes	
Patient Status	ability to edit active patient status at the organization/facility level	E	Yes	
Patient Status	ability to edit inactive patient status at the organization/facility level	E	Yes	
Patient Status	ability to store reason for inactive status of patients at the organizational/facility level	E	Yes	
Patient Status	ability to edit multiple patients status in one action	O	Yes	
Patient Status	**ability to manage patient status at the geographic jurisdictional level**	E	Yes	
Patient Status	ability to store active patient status at the geographic jurisdiction level	E	Yes	
Patient Status	ability to store inactive patient status at the geographic jurisdictional level	E	Yes	
Patient Status	ability to edit active patient status at the geographic jurisdictional level	E	Yes	
Patient Status	ability to edit inactive patient status at the geographic jurisdictional level	E	Yes	
Patient Status	ability to store reason for inactive status of patients at the geographic jurisdictional level	O	Yes	
Patient Status	ability to restrict access to patient records that have been placed in an inactive status	O	Yes	

Function: Manage Patient and Immunization Records

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Patient Status	ability to restrict edits to patient records that have been placed in an inactive status	O	Yes	
Patient Consent	**ability to manage patient consent per jurisdictional policy**	E	Yes	
Patient Consent	ability to update patient consent on a patient's record	E	Yes	
Patient Consent	ability to opt out a patient from participating in the IIS	E	Yes	
Patient Consent	ability to opt in a patient for participation in the IIS	E	Yes	
Patient Consent	ability to enable access to a patient record per consent designation	E	Yes	
Patient Consent	ability to enable updates to a patient record per consent designation	E	Yes	
Add, Edit Patient	**ability to add vaccination event information to a patient record**	E	Yes	
Add, Edit Patient	ability to edit vaccine information in a patient record	E	Yes	
Add, Edit Patient	ability to mark vaccine information in a patient record for deletion	O	Yes	
Add, Edit Patient	ability to add reason for deletion of vaccine information in a patient record	O	Yes	
Add, Edit Patient	ability to capture vaccine eligibility by vaccine dose for publicly purchased vaccine	E	Yes	
Add, Edit Patient	ability to store vaccine eligibility by vaccine dose for publicly purchased vaccine	E	Yes	
Add, Edit Patient	ability to report multiple doses administered to the same patient on the same administration date	E	Yes	
Add, Edit Patient	ability to store all CDC-endorsed core data elements related to vaccine events	E	Yes	
Add, Edit Patient	ability to enter vaccination substandard or otherwise compromised flag	E	Yes	
Add, Edit Patient	ability to view submitted vaccination event information on a patient's record	E	Yes	
Add, Edit Patient	ability to store adverse reactions in accordance with Vaccine Recommendations and Guidelines of	E	Yes	
Add, Edit Patient	ability to flag an adverse reaction as having been reported to VAERS	E	Yes	
Add, Edit Patient	ability to store patient vaccination event funding eligibility information	E	Yes	
Add, Edit Patient	ability to print form for signature of vaccine refusal by patient for each individual vaccine antigen	O	Yes	
Add, Edit Patient	ability to ensure that the default lot number is from the oldest lot when entering an administered	E	Yes	
Add, Edit Patient	ability to record administration of vaccination regardless if vaccine has since expired in inventory	E	Yes	
Add, Edit Patient	ability to track vaccinations that require adjuvant	E	Yes	
Print/Export Record	**ability to securely print a patient immunization record**	E	Yes	
Print/Export Record	ability to include evaluated history in the printable version of the patient record	E	Yes	
Print/Export Record	ability to include the forecast in the printable version of the patient record	E	Yes	
Print/Export Record	ability to include immunity in the printable version of the patient record	E	Yes	
Print/Export Record	**ability to securely export a patient immunization record**	E	Yes	
Print/Export Record	ability to export a patient record in user-defined format	O	Yes	
Mass Vaccination	**ability to support mass vaccination operations**	E	Yes	
Mass Vaccination	ability to rapidly capture patient demographic information offline during mass vaccination clinic for	E	Yes	
Mass Vaccination	ability to rapidly capture vaccine information offline during mass vaccination clinic for later	E	Yes	
Mass Vaccination	ability to support rapid capture of patient demographic information during mass vaccination clinic	E	Yes	
Mass Vaccination	ability to support rapid capture of vaccine information during mass vaccination clinic	E	Yes	
Mass Vaccination	ability to administer vaccines during public health emergency without impacting the patient's status	O	Yes	
Mass Vaccination	ability for jurisdictional admin to flag/indicate org/facility participation in mass vaccination event	O	Yes	

Function: Manage Vaccine Inventory

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Vaccine Inventory	ability to search inventory by user-defined parameters	E	Yes	
Vaccine Inventory	ability to search the inventory by funding source	E	Yes	
Vaccine Inventory	ability to search inventory by vaccine type	E	Yes	
Vaccine Inventory	ability to search inventory by vaccine lot number	E	Yes	
Vaccine Inventory	ability to search inventory by vaccine NDC code	E	Yes	
Add, Edit Vaccine	ability to manage vaccine inventory	E	Yes	
Add, Edit Vaccine Inventory	ability to support visualization of current vaccine inventory	E	Yes	
Add, Edit Vaccine	ability to edit inventory funding source at the lot level	E	Yes	
Add, Edit Vaccine	ability to edit inventory funding source at the vaccine level	E	Yes	
Add, Edit Vaccine	ability to add vaccine information to inventory	E	Yes	
Add, Edit Vaccine	ability to support barcode scanning system to electronically upload vaccine inventory to the IIS	O	Yes	
Add, Edit Vaccine	ability to view current inventory list by facility	E	Yes	
Add, Edit Vaccine	ability to view current inventory list by organization	E	Yes	
Add, Edit Vaccine	ability for jurisdictional admin to edit organization/facility inventory	E	Yes	
Add, Edit Vaccine	ability to manage vaccine borrowed from lots belonging to one funding source to lots belonging to another funding source	O	Yes	
Add, Edit Vaccine	ability to reclassify funding source of borrowed vaccine from private to public or vice versa for replacement cases	O	Yes	
Add, Edit Vaccine	ability to view storage capability	E	Yes	
Add, Edit Vaccine	ability to document vaccine storage and handling events such as temperature excursions	E	Yes	
Add, Edit Vaccine	ability to store storage capability	E	Yes	
Vaccine Ordering	ability for rule based logic to recommend vaccine order quantity	E	Yes	
Vaccine Ordering	ability to alert user when "reorder recommendation" inventory level is reached	O	Yes	
Vaccine Ordering	ability to pre-populate order with recommended quantities based on inventory, doses reported as administered to IIS	E	Yes	
Vaccine Ordering	ability to edit pre-populated order quantity	E	Yes	
Vaccine Ordering	ability to order vaccines	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to activate vaccines available for ordering	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to inactivate vaccines available for ordering	E	Yes	
Vaccine Ordering	ability to order publicly-purchased vaccines	E	Yes	
Vaccine Ordering	ability to view all orders by user-defined parameters	O	Yes	
Vaccine Ordering	ability to update delivery hours to receive shipments	E	Yes	
Vaccine Ordering	ability to enter a reason for vaccine orders outside the recommended order quantity	E	Yes	
Vaccine Ordering	ability to search and view past vaccine orders by facility within a specified timeframe	E	Yes	
Vaccine Ordering	ability to verify contact information during each order without leaving ordering workflow	E	Yes	
Vaccine Ordering	ability to update contact information during each order without leaving ordering workflow	E	Yes	
Vaccine Ordering	ability to save an unsubmitted order	E	Yes	
Vaccine Ordering	ability to update organization/facility contact information before submitting a vaccine order	E	Yes	
Vaccine Ordering	ability to cancel unsubmitted or unprocessed vaccine orders	E	Yes	
Vaccine Ordering	ability to edit unsubmitted or unprocessed vaccine orders	E	Yes	
Vaccine Ordering	ability to save an unsubmitted order after rejection	E	Yes	
Vaccine Ordering	ability to verify order information before order submitted	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to reject a vaccine order	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to select a reason code when rejecting an order	E	Yes	
Vaccine Ordering	ability to edit an order after rejection	E	Yes	
Vaccine Ordering	ability to resubmit an order after rejection	E	Yes	
Vaccine Ordering	ability to electronically notify the facility of a rejected order	E	Yes	
Vaccine Ordering	ability to track the shipping status of orders	E	Yes	
Vaccine Ordering	ability to verify packing slip information after order is shipped	O	Yes	
Vaccine Ordering	ability to receive electronic notification when order quantity received does not match vaccine order	O	Yes	
Vaccine Ordering	ability to receive electronic notification when vaccine order received is damaged	O	Yes	
Vaccine Ordering	ability to request shipping label(s) for nonviable vaccine subject to return	O	Yes	
Vaccine Ordering	ability to search for past vaccine returns within a specified timeframe	E	Yes	
Vaccine Ordering	ability to view past vaccine returns within a specified time frame	E	Yes	
Vaccine Ordering	ability to pre-book vaccine orders	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to allocate vaccine inventory per user defined parameters	E	Yes	
Vaccine Ordering	ability to activate vaccine ordering functionality for all designated organizations/facilities during a public health emergency	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to create order sets	E	Yes	

Function: Manage Vaccine Inventory

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release
Review/Approve Order	ability for jurisdictional admin to review order	E	Yes	
Review/Approve Order	ability to support a rules-based decision logic to approve or reject order if above or below recommended order quantity	O	Yes	
Review/Approve Order	ability for jurisdictional admin to approve order	E	Yes	
Review/Approve Order	ability for jurisdictional admin to adjust order	E	Yes	
Review/Approve Order	ability for jurisdictional admin to electronically accept VFC vaccine into inventory	E	Yes	
Review/Approve Order	ability to accept each vaccine product in the IIS after shipment is received	E	Yes	
Vaccine Dose	ability to automatically decrement vaccine doses from inventory when matched vaccine doses are reported as administered	E	Yes	
Vaccine Dose	ability to automatically match vaccine doses reported as administered to vaccine doses in inventory to facilitate dose decrementing	E	Yes	
Vaccine Dose	ability to automatically decrement vaccine inventory in real-time via HL7 messaging	E	Yes	
Vaccine Dose	ability to automatically decrement vaccine inventory in real-time via UI data entry	E	Yes	
Vaccine Inventory	ability to reconcile vaccine doses currently in physical storage with vaccine doses reflected in system inventory	E	Yes	
Vaccine Inventory	ability to document reductions in vaccine inventory due to outgoing vaccine transfers	E	Yes	
Vaccine Inventory	ability to electronically document reductions in vaccine inventory due to outgoing vaccine wastage	E	Yes	
Vaccine Inventory	ability to enter current number of vaccine doses on-hand in physical storage	E	Yes	
Vaccine Inventory	ability to track and manage doses for vaccines: on hand, administered, wasted, expired, ordered, recalled, returned, transferred	E	Yes	
Vaccine Inventory	ability to enable removal of recalled lots from active inventory	E	Yes	
Vaccine Inventory	ability to print a reconciliation worksheet	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to approve vaccine transfers	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to initiate VFC vaccine transfers	O	Yes	
Vaccine Transfers	ability to accept VFC vaccine transfers	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to reject vaccine transfers	O	Yes	
Vaccine Transfers	ability to search and view past vaccine transfers within a specified timeframe	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to allow for direct vaccine transfer between facilities without jurisdictional pre-approval, but with jurisdictional visibility/oversight.	O	Yes	
Vaccine Wastage	ability to manage vaccine wastage	E	Yes	
Vaccine Wastage	ability to determine the total cost of wasted vaccine by user-defined parameters	E	Yes	
Vaccine Wastage	ability for jurisdictional admin to modify inventory quantity to reflect wastage	E	Yes	
Vaccine Wastage	ability for jurisdictional admin to assign reason for inventory wastage	E	Yes	
Vaccine Wastage	ability to determine the total doses of vaccine wasted by user-defined parameters	E	Yes	
Vaccine Expiration	ability to manage vaccine expiration	E	Yes	
Vaccine Expiration	ability to alert users to vaccine nearing expiration	O	yes	
Vaccine Expiration	ability to provide alerts for inventory already expired	O	Yes	
Vaccine Expiration	ability for jurisdictional admin to modify inventory quantity removed from available inventory	E	Yes	

Function: Provide Data Access

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Standard Reports	ability to generate a report that includes history and forecast	E	Yes	
Standard Reports	ability to generate a data quality report displaying information on the quality of submitted data	E	Yes	
Standard Reports	ability to generate a report that provides information on patient and vaccine matching and deduplication	E	Yes	
Standard Reports	ability to generate a report that provides information on data quality of data at rest	E	Yes	
Standard Reports	ability to generate data quality reports for HL7 submissions	E	Yes	
Standard Reports	ability to generate VFC reports	E	Yes	
Standard Reports	ability to generate a practice-level patient data report for VFC enrolled sites	E	Yes	
Standard Reports	ability to generate a doses administered report to support accountability for publicly-purchased vaccine	E	Yes	
Standard Reports	ability to generate a doses administered report for VFC enrolled sites	E	Yes	
Standard Reports	ability to generate VFC provider practice profiles	E	Yes	
Standard Reports	ability to generate a report showing the total number of select vaccines administered each month by facility	E	Yes	
Standard Reports	ability to generate a report displaying a change in vaccine administration patterns over a selected timeframe	E	Yes	
Standard Reports	ability to generate duplicate/merge record reports	E	Yes	
Standard Reports	ability to generate reports about IIS users	E	Yes	
Standard Reports	ability to generate vaccine management reports	E	Yes	
Standard Reports	ability to generate a report listing/identifying patients who received a recalled vaccine	E	Yes	
Standard Reports	ability to generate a report of patients declining or refusing vaccinations	O	Yes	
Standard Reports	ability to generate a report to calculate a facility's average vaccine usage	O	Yes	
Standard Reports	ability to generate VFC accountability reports for managing VFC inventories and orders	E	Yes	
Standard Reports	ability to generate vaccine inventory reports	E	Yes	
Standard Reports	hand	E	Yes	
Standard Reports	transactions	E	Yes	
Standard Reports	ability to generate report(s) that display information about vaccine order history	O	Yes	
Standard Reports	ability to generate report(s) that display information about vaccine wastage and returns	E	Yes	
Standard Reports	specific timeframe	E	Yes	
Standard Reports	ability to generate a report providing information about influenza pre-book orders	E	Yes	
Standard Reports	ability to query vaccine ordering patterns over a selected timeframe to indicate trends	O	Yes	
Standard Reports	ability to generate reports that provide information about organizations and facilities	O	Yes	
Standard Reports	ability for jurisdictional admin to generate report that lists immunizing facilities	O	Yes	
Standard Reports	ability for jurisdictional admin to generate a report that provides information on	O	Yes	
Standard Reports	ability for jurisdictional admin to access utilization of report/usage statistics	O	Yes	
Standard Reports	ability to generate reports that provide information about students and their immunization	E	Yes	
Standard Reports	ability to generate report of student exemptions by type (medical, religious)	E	Yes	
Standard Reports	ability to generate a record of students' immunizations for school purposes	E	Yes	
Standard Reports	ability to generate exclusion letters stating which vaccine(s) a student needs to come into	E	Yes	
Standard Reports	ability to generate reports for individuals vaccinated during a mass vaccination event	E	Yes	
Standard Reports	ability to generate doses administered reports for priority groups during a public health	E	Yes	
Standard Reports	ability to generate a report that provides information about the status of the system in	E	Yes	
Ad Hoc Queries &	ability to generate queries and reports based on user-defined parameters	E	Yes	

Function: Provide Data Access

Return to Cover Page

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Ad Hoc Queries &	ability to schedule an ad hoc query to run on a predetermined interval (i.e., daily, weekly,	E	Yes	
Ad Hoc Queries &	ability to generate reports with a user-defined report format	E	Yes	
Ad Hoc Queries &	ability to generate reports across geographic hierarchy levels	E	Yes	
Ad Hoc Queries &	ability to generate data to inform the public via website dashboards or similar means	E	Yes	
Ad Hoc Queries &	ability to store saved report templates	E	Yes	
Ad Hoc Queries &	ability to modify saved report templates	E	Yes	
Ad Hoc Queries &	ability to inactivate (archive) saved report templates	E	Yes	
Ad Hoc Queries &	ability to modify a query	E	Yes	
Ad Hoc Queries &	ability to delete a query	E	Yes	
Ad Hoc Queries &	ability to save an ad hoc query	E	Yes	
Ad Hoc Queries &	ability to create a map using geocodes for statistical reporting	O	Yes	
Print/Export Reports	**ability to export IIS data for use in other systems**	E	Yes	
Print/Export Reports	ability to export data in user-defined formats	E	Yes	
Print/Export Reports	ability to export aggregate level de-identified data	E	Yes	
Print/Export Reports	ability to export record level de-identified data	E	Yes	
Print/Export Reports	**ability to print reports**	E	Yes	
Consumer Access	**ability for authorized consumers to access personal IIS data per jurisdictional policy**	E	Yes	
Consumer Access	ability for authorized consumer to print forecast	O	Yes	
Consumer Access	ability for authorized consumer to print patient immunization record	E	Yes	
Consumer Access	ability for authorized consumer to print an official immunization history	E	Yes	
Consumer Access	ability for authorized consumer to retrieve a verifiable digital vaccine credential without	E	Yes	
Consumer Access	ability for authorized consumer to view immunization forecast	E	Yes	
Consumer Access	ability for authorized consumer to view patient information	E	Yes	
Consumer Access	ability for authorized consumer to view patient immunization record	E	Yes	
Consumer Access	ability for patient/patient representative to opt in for reminder/recall notifications	O	Yes	
Consumer Access	ability for patient/patient representative to opt out of reminder/recall notifications	O	Yes	

Non-functional

Return to Cover Page

Attribute	Sub Characteristic	Requirement: The IIS must/should...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: Indicate the anticipated cost and timeline for development and release.
Performance	Time Behavior	support a responsive user interface	E	Yes	
Performance	Time Behavior	support application launch, i.e. time between user initiation and application start, in less than 10 seconds	E	Yes	
Performance	Time Behavior	support response to a user navigation action (e.g., mouse movement, keypresses, navigation) in less than 1	E	Yes	
Performance	Time Behavior	support response to process submitted information via direct data entry in less than 4 seconds	E	Yes	
Performance	Time Behavior	support generation of a standard, pre-configured report in less than 30 seconds	E	Yes	
Performance	Time Behavior	support responsive data exchange system interfaces	E	Yes	
Performance	Time Behavior	support electronic response to a submitted HL7 message in 5 seconds or less, 95% of the time	E	Yes	
Performance	Capacity	support up to 1000 concurrent users of the user interface without performance degradation	E	Yes	
Performance	Capacity	support multiple users viewing the same data at the same time	E	Yes	
Performance	Capacity	support users using the same function at the same time without degrading IIS performance	E	Yes	
Performance	Resource	support resource-intensive tasks without degrading IIS performance	E	Yes	
Performance	Resource	support user queries via the user interface without degrading IIS performance	E	Yes	
Performance	Resource	support generation of ad hoc reports without degrading IIS performance	E	Yes	
Performance	Resource	support data extracts without degrading IIS performance	E	Yes	
Performance	Capacity	support efficient processing of HL7 messages without performance degradation, as per jurisdictional capacity	E	Yes	
Performance	Capacity	support processing of up to 200 of HL7 VXU messages per hour without performance degradation	E	Yes	
Performance	Capacity	support processing of up to 8000 of HL7 QBP messages per hour without performance degradation	E	Yes	
Performance	Capacity	support permanent storage of records as per jurisdictional policy	E	Yes	
Performance	Capacity	support storage of unlimited number of organization records	E	Yes	
Performance	Capacity	support storage of unlimited number of user records	E	Yes	
Performance	Capacity	support storage of unlimited number of patient records	E	Yes	
Performance	Capacity	support storage of unlimited number of patient immunization records	E	Yes	
Usability	Accessibility	meet the United States Access Board Section 508 Standards	E	Yes	
Usability	Operability	support best practices for web application session management (e.g., cookies, cache) as recommended by the	E	Yes	
Usability	Operability	ability to execute Boolean searches	E	Yes	
Usability	Operability	ability to execute a wildcard searches	E	Yes	
Usability	User error	minimize data entry errors	E	Yes	
Usability	User error	assist in entering data correctly via pick-lists, drop-down boxes, or other easy-to-use options such as predictive	E	Yes	
Usability	User error	indicate required fields for data entry	E	Yes	
Usability	User error	ability to provide alert when required fields are left blank	E	Yes	
Usability	User error	support cross-field checks to ensure accuracy of information where dependencies exist (e.g., warning that a	E	Yes	
Usability	User error	support spell check functionality with medical terminology for all free text fields	O	Yes with customization	Time to develop 2 weeks, time to release 1 week at no additional cost
Usability	User error	and error messages (error must be fixed prior to continuing)	E	Yes	
Usability	User interface	support alerts related to user interface response time	O	Yes	
Usability	User Interface	support user feedback with a simple indicator for response times between 2-4 seconds	O	Yes	
Usability	User interface	support user feedback with expected response time and percent-done indicator for response times greater	O	Yes	
Usability	User interface	support users in stopping an operation expected to take longer than 10 seconds	O	Yes with customization	Time to develop 1 week, time to release 1 week at no additional cost
Usability	User interface	support users in performing other tasks while waiting for the system to complete tasks expected to take longer	O	Yes	
Reliability	Availability	support availability of the system as per jurisdictional needs	E	Yes	
Reliability	Availability	support access to the web application 99.9% of the time	E	Yes	
Reliability	Availability	support processing of and response to HL7 messages 99.9% of the time	E	Yes	
Reliability	Recoverability	ability to backup the IIS data as per jurisdictional policy	E	Yes	
Reliability	Recoverability	support redundancy of the IIS as per jurisdictional recovery plan	E	Yes	
Reliability	Recoverability	support real-time failover	E	Yes	
Reliability	Recoverability	support the recovery of backed up data as needed	E	Yes	
Reliability	Recoverability	support the restoration of IIS data after an outage or loss	E	Yes	
Reliability	Fault tolerance	support the efficient roll back of software changes as needed	E	Yes	
Security	Non-repudiation	support audit logs for security purposes	E	Yes	
Security	Integrity	ability to electronically notify the system administrator of unauthorized activity	E	Yes	
Security	Authenticity	ability to track all attempted accesses that fail identification, authentication and authorization requirements	E	Yes	
Security	Authenticity	ability to track all accesses that successfully comply with identification, authentication and authorization	E	Yes	
Security	Non-repudiation	ability to maintain audit logs for specified time per jurisdictional policy	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by function performed	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by date and time period	E	Yes	

Non-functional

Return to Cover Page

Attribute	Sub Characteristic	Requirement: The IIS must/should...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s) If Yes with customization: indicate the anticipated cost and timeline for development and release.
Security	Non-repudiation	ability for jurisdictional admin to search audit log by date range	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by user defined parameters	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by patient identifiers	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to filter audit log search by user defined parameters	O	Yes	
Security	Non-repudiation	ability for jurisdictional admin to sort audit log search results	O	Yes	
Security	Integrity	store audit data related to user access/viewing of patient records in the system	E	Yes	
Security	Integrity	store date of user access to a patient record	E	Yes	
Security	Integrity	store time of user access to a patient record	E	Yes	
Security	Integrity	store user ID of user access to a patient record	E	Yes	
Security	Non-repudiation	store audit data related to data changes in the system	E	Yes	
Security	Non-repudiation	store 'date received' for data modified in the system	E	Yes	
Security	Non-repudiation	store 'time received' for data modified in the system	E	Yes	
Security	Non-repudiation	store 'date updated' for data modified in the system	E	Yes	
Security	Non-repudiation	store 'time updated' for data modified in the system	E	Yes	
Security	Non-repudiation	store user associated with data modified in the system	E	Yes	
Security	Integrity	automatically enforce session timeout for a user when idle period is reached	E	Yes	
Security	Integrity	ability for automatic session timeout to be customized per jurisdictional policy	O	Yes	
Security	Integrity	ability to notify the user the session will expire	O	Yes	
Security	Confidentiality	support masking of passwords as they are typed or entered into the user interface	E	Yes	
Security	Integrity	ability for system administrator to terminate user connections	E	Yes	
Security	Confidentiality	Safeguard electronic personally identifiable information by implementing the appropriate technical best	E	Yes	
Security	Confidentiality	ability to encrypt personally identifiable information at rest	E	Yes	
Security	Confidentiality	ability to decrypt personally identifiable information at rest	E	Yes	
Security	Confidentiality	ability to encrypt personally identifiable information during transmission	E	Yes	
Security	Confidentiality	ability to decrypt personally identifiable information during transmission	E	Yes	
Security	Integrity	ability to maintain firewalls per AIRA's Security Guidance Considerations for Immunization Information Systems	E	Yes	
Security	Integrity	ability to maintain firewalls for protection of the hosting network	E	Yes	
Security	Integrity	ability to maintain firewalls for protection of the hosting environment	E	Yes	
Security	Integrity	ability to electronically notify the system admin of unauthorized activity	E	Yes	
Security	Integrity	ability to support anti-virus protection at current critical patch levels in the hosting environment	E	Yes	
Maintainabili	Analyzability	support event logging	E	Yes	
Maintainabilit	Analyzability	ability for system admin to enable event logging on all servers	O	Yes	
Maintainabilit	Analyzability	ability for system admin to enable event logging on all devices	O	Yes	
Maintainabilit	Analyzability	ability for system admin to disable event logging on all devices	O	Yes with customization	Time to develop 1 week, time to release 1 week at no additional cost
Maintainabilit	Analyzability	ability for system admin to limit access to event logs, including System, Application, Web and Database logs	O	Yes with customization	Time to develop 1 week, time to release 1 week at no additional cost
Portability	Adaptability	support use of web browsers per jurisdictional policy	E	Yes	
Portability	Adaptability	support use of current version of web browsers	E	Yes	
Portability	Adaptability	support use of last prior version of web browsers	E	Yes	
Portability	Adaptability	support a responsive design that renders properly on multiple devices	E	Yes	
Portability	Adaptability	support web client use on a desktop	E	Yes	
Portability	Adaptability	support web client use on a laptop	E	Yes	
Portability	Adaptability	support web client use on a tablet	E	Yes	
Portability	Adaptability	support web client use on a smartphone	E	Yes	
Portability	Installability	be containerized (e.g., Docker or Kubernetes) to support easy installation and system updates	E	Yes	
Portability	Installability	be containerized for cloud based environments	O	Yes	

Glossary of Terms

Terms and definitions used within requirements. Note: For definitions of general terms related to immunizations, see the CDC Vaccines and Immunizations Glossary

Return to Cover Page

For definitions of general terms related to IIS, see the AIRA MIROW Common Vocabulary resources.

Term	Definition
Admin	Refers to a jurisdictional admin and organizational admin.
Associate (verb)	Establish a relationship between entities. Synonymous with "link."
At rest	Used to refer to data in storage within the IIS.
Audit log	Also referred to as an audit trail. Used to refer to the tracking of information about system activity and changes, used for security purposes.
Authorization agreement	Formal or legal agreement between an organization submitting and/or using immunization data and the jurisdiction that outlines terms for participating in the IIS per jurisdictional policy (e.g., data use agreements, user agreements).
Authorized consumer	A consumer authorized to access IIS records such as their personal vaccination records or those for individuals for whom they are guardians/care-takers.
Authorized user	Individual authorized to access the system based on their role and affiliation with an IIS-authorized organization.
Automatically	Ability for the system to take action without manual intervention.
Capture	Ability to enter data via user interface (UI) or data exchange interface for immediate usage. Does not necessarily imply storage.
Clinician	A clinician or health care professional who orders and/or administers vaccines (e.g., vaccine ordering provider, vaccine administering provider).
Cohort	A group of patients of particular interest to an organization and/or facility (e.g., a group of health plan members, a group of students, group of individuals with the same age).
Containerization	Containerization packages an application along with all its necessary configuration files, libraries, and dependencies, ensuring it runs efficiently and without bugs across various computing environments.
Delete	Process by which data are removed from the IIS system, including removal from data table(s). Synonymous with "purge."
During transmission	Used to refer to data being transmitted or actively moved from one location to another.
Edit	Global term to reflect ability to modify, update, and change data. For a particular field, this also includes the ability to delete field-level data that is no longer accurate.
Electronic notification	Communication/message sent to a user without manual intervention.
Electronic response	The IIS returns a final resolution, or outcome, of processing the HL7 message with a conformant HL7 (Health Level Seven) message.
Enroll	Process by which an organization or a facility is authorized to participate in an IIS and/or in a jurisdictional Vaccines for Children (VFC) program,
Event log	Tracking (i.e., storing) information about system activity and changes, used for IT support and maintenance.
Facility	A sub-organizational unit for organizations with multiple locations. May also be synonymous for "organization" for organizations with one
Immunization Information System	Refers to the application, data and staff that record all immunization doses administered by participating providers to individuals within a given
Inactivate	To make inoperable.
Interface (noun)	Connection between two or more systems for transmission of data.
Interface (verb)	Act of securely exchanging data to facilitate data use.
Interoperate	Data are transmitted from one system to be consumed by another.
Jurisdictional admin	Jurisdictional IIS staff authorized to enter and modify information in the IIS.
Jurisdictional vaccine program admir	Jurisdictional vaccine program staff authorized to enter and modify VFC- and vaccine program-related information in the IIS.

Glossary of Terms

Terms and definitions used within requirements. Note: For definitions of general terms related to immunizations, see the CDC Vaccines and Immunizations Glossary

Return to Cover Page

For definitions of general terms related to IIS, see the AIRA MIROW Common Vocabulary resources.

Term	Definition
Manage	Global term used to refer to the ability to add, edit, or otherwise modify information.
Notification	A push communication to an authorized user.
Order set	A standardized group of supply items that can ordered at one time that create efficiencies in the ordering process.
Organization	An entity that may provide data to an IIS and/or may consume IIS data and information (e.g., provider organization, school). An organization
Organizational admin	Staff within the organization (e.g., clinic, facility, LHD) responsible for maintaining the organization/facility information in the IIS, including
Patient	Used to refer to an individual. Synonymous with "client."
Personally identifiable information	”Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an
Process	The IIS reads the incoming data and takes appropriate action based on the data submitted and previously known information already in the IIS.
Provider	A vaccinating or non-vaccinating health care professional authorized to submit, access and/or use IIS data.
Provider organization	A type of organization that has any combination of the following characteristics: provides vaccination services, responsible for an entity that
Query	A question posed of the IIS data.
Recall	A notification sent to individuals who are overdue for a vaccination.
Re-enroll	Process by which a previously enrolled organization or facility is re-authorized to participate in an IIS and/or in a jurisdictional VFC program, per
Reminder	A notification sent to individuals who are due to receive a vaccination soon.
Report	System generated data or information available in suitable formats, which may include outputs of queries.
Store	Maintenance of data for potential future use. Note: use of "store" also implies data capture.
System admin	Jurisdictional administrator responsible for oversight of the IIS technology, typically an IT role.
System alert	A communication broadcast to authorized users.
Track	Follow the steps of a process to note a modification.
User	Individual associated with an organization authorized to access the IIS system to submit and/or consume IIS data and information (e.g., clinic
User agreement	Agreement between a representative(s) of an organization and the jurisdiction, outlining terms for participation in the IIS, per jurisdictional
User-defined parameter	An element selected by a user to define the scope of a particular process or activity.
Vaccines for Children (VFC) provider	A type of provider organization, specifically, a provider organization that is enrolled in the VFC program.
Vaccine program	A program managed and administered by a jurisdiction to provide specified vaccine(s) to specified organizations or facilities (e.g., Vaccines for

Functional Standards: https://www.cdc.gov/iis/functional-standards/resource.html

Return to Cover Page

Draft IIS Functional Standards, v5.0			IIS Functional Model Functions									IIS Functional Model Attributes					
Goal	Standard	Guidance Statement	Administer System	Manage Organizations and Facilities	Manage Users	Support Interoperability	Ensure Data Quality	Evaluate and Forecast	Manage Patient and Immunization Records	Manage Vaccine Inventory	Provide Data Access	Performance	Usability	Reliability	Security	Maintainability	Portability
A. Establish and maintain a secure, confidential Immunization Information System.	1.0 The IIS is physically and digitally secured in accordance with policies and industry standards for protected health information, security, and encryption.				x							x	x	x	x	x	x
		1.1 The IIS establishes, documents, and updates policies and procedures to manage the collective functions, capabilities, and attributes of an IIS.										x	x	x	x	x	x
		1.2 The IIS establishes and maintains the technical infrastructure to securely capture, store, and process patient demographic and vaccination data consistent with established policies and procedures.										x	x	x	x	x	x
		1.3 The IIS provides ongoing training to ensure awareness of and to promote adherence to policies and procedures.			x										x		
	2.0 The IIS is physically and digitally secured in accordance with industry standards for disaster avoidance, mitigation, and recovery.													x	x		
		2.1 The IIS establishes and maintains the infrastructure needed for disaster avoidance.												x	x		
		2.2 The IIS establishes and tests recovery plans to mitigate system downtime.												x	x		
	3.0 The IIS defines service expectations between the program and the entities providing information technology support to ensure system availability and uninterrupted data flow.											x	x	x	x	x	x
		3.1 The IIS implements service-level agreements between the program and the entities providing information technology and support.										x	x	x	x	x	x
		3.2 The IIS implements and maintains the infrastructure to fulfill service-level agreements.										x	x	x	x	x	x
B. Continuously improve IIS data quality.	4.0 The IIS validates patient demographic and vaccination data.		x			x	x	x	x		x		x				
		4.1 The IIS supports the identification, prevention, and resolution of duplicate and fragmented patient demographic and vaccination data in accordance with policies and procedures.					x										
		4.2 The IIS monitors data quality within the IIS in accordance with policies and procedures.	x			x	x	x	x		x						
		4.3 The IIS uses electronic tools to standardize and/or validate addresses in the IIS.	x						x								
		4.4 The IIS delivers feedback and training to IIS partners and providers to ensure complete, timely, and accurate patient demographic and vaccination records.															
		jurisdictional data quality					x	x			x		x				

IIS Functional Standards: https://www.cdc.gov/iis/functional-standards/resource.html

Return to Cover Page

Draft IIS Functional Standards, v5.0

			IIS Functional Model Functions									IIS Functional Model Attributes					
Goal	Standard	Guidance Statement	Administer System	Manage Organizations and Facilities	Manage Users	Support Interoperability	Ensure Data Quality	Evaluate and Forecast	Manage Patient and Immunization Records	Manage Vaccine Inventory	Provide Data Access	Performance	Usability	Reliability	Security	Maintainability	Portability
C. Promote electronic data exchange between the IIS and its partners and providers.	5.0 Manage interfaces for exchange and integration of data electronically between the IIS and other information systems in accordance with federal and jurisdictional standards.					x	x				x	x	x	x			
		accordance with current				x											
		enrolls, and onboards IIS				x						x					
		evaluates data submitted via				x	x				x		x				
		resolves electronic data				x						x	x	x			
D. Ensure the delivery of immunization services reflects current ACIP recommendations.	6.0 The IIS supports pediatric, adolescent, and adult immunization forecasts consistent with Advisory Committee on Immunization Practices (ACIP) recommendations.							x									
		maintains Clinical Decision						x									
		maintains Clinical Decision						x									
E. Ensure appropriate user access to data.	7.0 The IIS ensures authorized users have access to patient demographic and vaccination data based on user roles and permissions.		x	x	x				x		x		x		x		
		confidentiality policies that													x		
		comprehensive account													x		
		attributes for the set up and	x	x	x												
		in accordance with policies and			x												
		IIS partners' and providers'	x	x	x										x		
		covers accessing patient									x						
		inactivates user and site	x	x	x				x				x				
	8.0 The IIS supports authorized public access to official immunization records.										x				x		x
		with direct access to									x				x		x
F. Support the generation and use of IIS data through various channels and formats.	9.0 The IIS supports the reporting needs of federal and jurisdictional immunization programs.										x						
		and ad hoc reports to meet									x						
	10.0 The IIS supports ad-hoc queries of patient demographic and vaccination data.										x				x		
		access for internal authorized									x				x		
		data for data visualization,									x						
	11.0 The IIS supports investigation and reporting of vaccine adverse events.								x								
		adverse event investigation.							x								
		appropriate resources to							x								
	12.0 The IIS supports the ability to generate coverage reports that users can access without assistance from IIS staff.							x	x		x						
		data to assess vaccination									x						
		status at provider site and							x								
		training on accessing,									x						
		compliance with immunization						x			x						
	13.0 The IIS supports reminder/recall activities.							x	x								
		conducting reminder/recall						x	x								
G. Support federal and jurisdictional vaccine program requirements.	14.0 The IIS supports management and quality assurance functions for federal and jurisdictional vaccine programs.								x	x	x		x				
		program procedures in											x				
		tracking of eligibility at the dose							x								
		listing patients that received a									x						
		listing provider sites that								x	x						
	15.0 The IIS supports vaccine inventory management and reconciliation according to federal and jurisdictional vaccine program requirements.									x	x						
		inventory management,								x	x						
		vaccine orders and monitoring								x	x						
		vaccine returns and wastage.								x	x						
		decrements administered doses								x	x						
	16.0 The IIS supports data exchange with the national Vaccine Tracking System (VTrckS).					x											
		exchange with VTrckS in				x											
		to ExIS functionality following				x											
		automated data exchange with				x											

IIS Functional Standards: https://www.cdc.gov/iis/functional-standards/resource.html

Return to Cover Page

Draft IIS Functional Standards, v5.0			IIS Functional Model Functions										IIS Functional Model Attributes					
Goal	Standard	Guidance Statement	Administer System	Manage Organizations and Facilities	Manage Users	Support Interoperability	Ensure Data Quality	Evaluate and Forecast	Manage Patient and Immunization Records	Manage Vaccine Inventory	Provide Data Access	Performance	Usability	Reliability	Security	Maintainability	Portability
H. Support response efforts for vaccine-preventable disease outbreaks and other public health emergencies.	17.0 The IIS supports partner and provider onboarding and vaccine management during vaccine-preventable disease response and/or public health emergencies.		x	x	x	x			x		x		x				
		coordinates, and executes											x				x
		17.2 The IIS supports expedited communication and onboarding with partners to capture patient demographic and vaccination data in an emergency.	x	x	x												
		onboarded partners.		x													
		administration functionality to							x								
		integration with tools for				x											x
		health immunization reporting									x						
I. Participate in and prioritize emerging technologies and standards.	18.0 The IIS participates in modernization initiatives and emerging technologies.															x	
		modernization efforts.														x	
		efforts that align IIS initiatives														x	
		initiatives to develop standards														x	

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1874842

Doc Description: REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)

Reason for Modification:

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2026-02-03	2026-03-10 13:30	CRFP 0506 MIS2600000001	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : VAULT Technologies, LLC

Address :

Street : 1 Reservoir Circle, Suite 101

City : Pikesville

State : MD **Country :** USA **Zip :** 21208

Principal Contact : Tiffany Tate

Vendor Contact Phone: 888-862-2920 **Extension:** 1

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X **FEIN#** 92-0384326 **DATE** 03/24/26

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, DEPARTMENT OF HEALTH, BUREAU OF PUBLIC HEALTH- EPIDEMIOLOGY SERVICES, IS SOLICITING PROPOSALS TO ESTABLISH AN OPEN-END CONTRACT FOR AN IMMUNIZATION INFORMATION SYSTEM (IIS) PER THE ATTACHED DOCUMENTS.

ONLINE RESPONSES ARE PROHIBITED FOR THIS SOLICITATION

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

INVOICE TO	SHIP TO
HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US	HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Software				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
See attached Cost Sheet - Attachment A.

Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**** Online responses have been prohibited for this solicitation. Follow all bidding instructions.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2026-02-17

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1874842

Doc Description: REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)

Reason for Modification:
ADDENDUM 1
TO ADD PRICING PAGES THAT WERE INADVERTENTLY NOT INCLUDED

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2026-02-03	2026-03-10 13:30	CRFP 0506 MIS2600000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : VAULT Technologies, LLC

Address :

Street : 1 Reservoir Circle, Suite 101

City : Pikesville

State : MD **Country :** USA **Zip :** 21208

Principal Contact : Tiffany Tate

Vendor Contact Phone: 888-862-2920 **Extension:** 1

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X **FEIN#** 92-0384326 **DATE** 03/24/26

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, DEPARTMENT OF HEALTH, BUREAU OF PUBLIC HEALTH- EPIDEMIOLOGY SERVICES, IS SOLICITING PROPOSALS TO ESTABLISH AN OPEN-END CONTRACT FOR AN IMMUNIZATION INFORMATION SYSTEM (IIS) PER THE ATTACHED DOCUMENTS.

ONLINE RESPONSES ARE PROHIBITED FOR THIS SOLICITATION

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

INVOICE TO	SHIP TO
HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US	HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Software				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

See attached Cost Sheet - Attachment A.

Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**** Online responses have been prohibited for this solicitation. Follow all bidding instructions.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2026-02-17

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1874842			**Reason for Modification:** ADDENDUM 2 TO PROVIDE REVISED ATTACHMENT B
Doc Description: REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)			
Proc Type: Central Master Agreement			
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2026-02-10	2026-03-10 13:30	CRFP 0506 MIS2600000001	3

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : VAULT Technologies, LLC

Address :

Street : 1 Reservoir Circle, Suite 101

City : Pikesville

State : MD **Country :** USA **Zip :** 21208

Principal Contact : Tiffany Tate

Vendor Contact Phone: 888-862-2920 **Extension:** 1

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X **FEIN#** 92-0384326 **DATE** 03/24/26

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, DEPARTMENT OF HEALTH, BUREAU OF PUBLIC HEALTH- EPIDEMIOLOGY SERVICES, IS SOLICITING PROPOSALS TO ESTABLISH AN OPEN-END CONTRACT FOR AN IMMUNIZATION INFORMATION SYSTEM (IIS) PER THE ATTACHED DOCUMENTS.

ONLINE RESPONSES ARE PROHIBITED FOR THIS SOLICITATION

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

INVOICE TO	SHIP TO
HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US	HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Software				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

See attached Cost Sheet - Attachment A.

Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**** Online responses have been prohibited for this solicitation. Follow all bidding instructions.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2026-02-17

	Document Phase	Document Description	Page 3
MIS2600000001	Final	REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1874842

Doc Description: REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)

Proc Type: Central Master Agreement

Reason for Modification:
ADDENDUM 3
TO EXTEND OPENING DATE

Date Issued	Solicitation Closes	Solicitation No	Version
2026-03-02	2026-03-24 13:30	CRFP 0506 MIS2600000001	4

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : VAULT Technologies, LLC

Address :

Street : 1 Reservoir Circle, Suite 101

City : Pikesville

State : MD **Country :** USA **Zip :** 21208

Principal Contact : Tiffany Tate

Vendor Contact Phone: 888-862-2920 **Extension:** 1

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X **FEIN#** 92-0384326 **DATE** 03/24/26

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, DEPARTMENT OF HEALTH, BUREAU OF PUBLIC HEALTH- EPIDEMIOLOGY SERVICES, IS SOLICITING PROPOSALS TO ESTABLISH AN OPEN-END CONTRACT FOR AN IMMUNIZATION INFORMATION SYSTEM (IIS) PER THE ATTACHED DOCUMENTS.

ONLINE RESPONSES ARE PROHIBITED FOR THIS SOLICITATION

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

INVOICE TO	SHIP TO
HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US	HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Software				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
See attached Cost Sheet - Attachment A.

Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**** Online responses have been prohibited for this solicitation. Follow all bidding instructions.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2026-02-17

	Document Phase	Document Description	Page 3
MIS2600000001	Final	REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1874842

Doc Description: REQUEST FOR PROPOSAL - IMMUNIZATION INFORMATION SYSTEM (IIS)

Proc Type: Central Master Agreement

Reason for Modification:
ADDENDUM 4
TO PROVIDE ANSWERS TO
VENDOR QUESTIONS

Date Issued	Solicitation Closes	Solicitation No	Version
2026-03-09	2026-03-24 13:30	CRFP 0506 MIS2600000001	5

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : VAULT Technologies, LLC

Address :

Street : 1 Reservoir Circle, Suite 101

City : Pikesville

State : MD **Country :** USA **Zip :** 21208

Principal Contact : Tiffany Tate

Vendor Contact Phone: 888-862-2920 **Extension:** 1

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X Tiffany Tate **FEIN#** 92-0384326 **DATE** 03/24/26

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, DEPARTMENT OF HEALTH, BUREAU OF PUBLIC HEALTH- EPIDEMIOLOGY SERVICES, IS SOLICITING PROPOSALS TO ESTABLISH AN OPEN-END CONTRACT FOR AN IMMUNIZATION INFORMATION SYSTEM (IIS) PER THE ATTACHED DOCUMENTS.

ONLINE RESPONSES ARE PROHIBITED FOR THIS SOLICITATION

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

INVOICE TO	SHIP TO
HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US	HEALTH AND HUMAN RESOURCES BUREAU FOR PUBLIC HEALTH CENTRAL FINANCE 350 CAPITOL ST, RM 206 CHARLESTON WV 25301-3717 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Software				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
See attached Cost Sheet - Attachment A.

Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**** Online responses have been prohibited for this solicitation. Follow all bidding instructions.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2026-02-17

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: MIS2600000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[✓] Addendum No. 1

[✓] Addendum No. 2

[✓] Addendum No. 3

[✓] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

VAULT Technologies, LLC
Company

Authorized Signature

3/20/26
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.