

Technical Proposal Title Page

Request for Proposals (RFP)

RFP Subject: Immunization Information System (IIS)

RFP Number: CRFP MIS2700000001

Submitted by

Vendor Name: Gainwell Technologies LLC

Business Address: 225 East John Carpenter Freeway, Suite 500, Irving, TX 75062

Primary Contact

Name: Adam Moyer, Account General Manager

Telephone Number: 712-308-0598

Fax Number: N/A

Email Address: amoyer@gainwelltechnologies.com

Authorized Signature

Signature:  _____

Printed Name: Mark Knickrehm

Title: President and Chief Executive Officer

Date: August 19, 2026

Contents

RFP Certification Signature Pages	1
Technical Proposal Title Page	4
Executive Summary	7
Additional Considerations	8
Section 4: Project Specifications	9
4.1 Background and Current Operating Environment.....	9
4.2 Project Goals and Mandatory Requirements	10
4.2.1 CDC-Based Goals and Objectives	10
4.2.2. West Virginia Specific Goals and Objectives	51
4.2.3. Mandatory Project Requirements	82
4.3. Qualifications and Experience	129
4.3.1. Qualifications and Experience Information	129
4.3.2. Mandatory Qualification/Experience Requirements.....	139
Appendix A – Contract Exceptions and Clarifications	141
Appendix B – Bidder Certification and Authorization	146
Appendix C – Designated Contact and Certification Signature	147
Appendix D – Federal Funds Addendum	148

List of Tables

Table 1. Core IIS Modernization Capabilities	11
Table 2. State and Gainwell Responsibilities	63
Table 3. Gainwell Non-Confidential Planning Roadmap Baseline	80
Table 4. Proposed Staff Roles	100
Table 5. Reference 1 – Maryland	137
Table 6. Reference 2 – North Carolina	137
Table 7. Reference 3 – New York	138
Table 8. Gainwell Contract Exceptions and Clarifications	141



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
2026-07-15	2026-08-19 13:30	CRFP 0506 MIS2700000001	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 000000166458

Vendor Name : Gainwell Technologies LLC

Address :

Street : 225 East John Carpenter Freeway, Suite 500

City : Irving

State : Texas

Country : United States

Zip : 75062

Principal Contact : Adam Moyer, Account General Manager

Vendor Contact Phone: 712-308-0598

Extension: N/A

FOR INFORMATION CONTACT THE BUYER

Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor
Signature X

FEIN# 27-1510177

DATE August 18, 2026

offers subject to all terms and conditions contained in this solicitation



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: 2009980

Doc Description: IMMUNIZATION INFORMATION SYSTEM (IIS)

Reason for Modification:

ADDENDUM 1
TO PROVIDE ANSWERS TO
VENDOR QUESTIONS AND
REVISED ATTACHMENT B

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2026-08-04	2026-08-19 13:30	CRFP 0506 MIS2700000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 000000166458

Vendor Name: Gainnwell Technologies LLC

Address:

Street :225 East John Carpenter Freeway, Suite 500

City : Irving

State : Texas

Country : United States

Zip : 75062

Principal Contact : Adam Moyer, Account General Manager

Vendor Contact Phone: 712-308-0598

Extension:

FOR INFORMATION CONTACT THE BUYER

Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor
Signature X

FEIN# 27-1510177

DATE August 18, 2026

All offers subject to all terms and conditions contained in this solicitation

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: MIS2700000001

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. 6
☐ Addendum No. 2	☐ Addendum No. 7
☐ Addendum No. 3	☐ Addendum No. 8
☐ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ 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.

Gainwell Technologies LLC

Company

Authorized Signature

August 19, 2026
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

Executive Summary

Gainwell Technologies LLC (Gainwell) is pleased to submit this proposal response to the State of West Virginia (State) for the modernization and ongoing operation of its Immunization Information System (IIS). The State seeks a secure, compliant, and future-ready platform that strengthens immunization tracking, supports public health decision-making, and enables seamless data exchange across providers, partners, and federal systems. Gainwell's proposed solution, Gainwell Assist™, is purpose-built to meet these objectives and provides a scalable foundation that evolves with national standards and public health needs.

West Virginia's IIS plays a critical role in safeguarding public health by managing millions of patient and vaccination records, supporting statewide reporting, and enabling rapid response during public health emergencies. Gainwell Assist is a cloud-hosted, Software-as-a-Service (SaaS) solution designed to securely collect, store, and manage immunization data in alignment with **the Centers for Disease Control and Prevention (CDC) IIS Functional Standards, Advisory Committee on Immunization Practices (ACIP) recommendations**, and applicable federal and state security requirements. Gainwell Assist solution supports high-volume transactions, robust interoperability, and comprehensive reporting without compromising performance or data integrity.

Security and compliance are foundational to Gainwell's approach. Gainwell Assist is hosted in a federally compliant cloud environment and incorporates layered physical, technical, and administrative safeguards to protect sensitive health information. Gainwell Assist aligns with standards including the Federal Risk and Authorization Management Program (FedRAMP), National Institute of Standards and Technology (NIST), System and Organization Controls (SOC) 2, Health Insurance and Portability Act (HIPAA), and Federal Information Processing Standards (FIPS). Safeguards include comprehensive audit logging, role-based access controls, encryption of data at rest and in transit, and resilient disaster recovery capabilities that support confidentiality, integrity, availability, and auditability of IIS throughout the system lifecycle.

Gainwell's solution promotes high-quality data through automated validation, deduplication, and governance practices aligned with CDC and AIRA guidance. Real-time interoperability using Health Level Seven (HL7) Version 2.5.1, readiness for Fast Healthcare Interoperability Resources (FHIR), and integration with national systems such as the CDC Immunization Gateway and VTrckS support accurate, timely, and standards-based information sharing. These capabilities help providers, public health officials, and partners deliver coordinated immunization services and meet federal reporting obligations.

The proposed IIS supports a wide range of program and stakeholder needs, including vaccine inventory management, coverage and population-level reporting, exemption tracking, reminder and recall activities, and consumer access to immunization records. Optional modules, such as Oral Health, allow the State to extend the platform to support additional public health initiatives while maintaining a unified and secure system architecture.

Built for West Virginia's Public Health Mission

- **Purpose Built for IIS Compliance.**
Designed to meet CDC IIS Functional Standards, ACIP guidance, and AIRA proven practices supporting West Virginia's immunization goals.
- **Secure, Standards Driven, and Future Ready.** Cloud-hosted SaaS aligned with NIST, SOC 2, and HIPAA, with proven HL7 v2.5.1 and a FHIR-ready architecture.
- **Lower Risk and Predictable Delivery.**
A configuration-first approach with included compliance updates reduces implementation risk, controls cost, and limits long term maintenance burden.

Role-based training, user-centered design, and configurable workflows promote adoption across providers, schools, and public health users statewide.

Gainwell proposes a proven phased implementation methodology that supports a smooth transition from the current IIS to the modernized platform. The approach includes collaborative planning, agile configuration, rigorous data migration and testing, comprehensive training, and structured go-live readiness. A proposed 12-month implementation timeline balances speed with risk mitigation and positions the State for a successful deployment with minimal disruption to ongoing operations. After implementation, Gainwell provides proactive maintenance, quarterly compliance updates aligned with CDC and AIRA requirements, and ongoing operational support to sustain long-term success.

With decades of experience supporting large-scale public health and Medicaid systems nationwide, Gainwell brings deep domain expertise, disciplined delivery practices, and a strong record of partnership with federal and state agencies. Gainwell *Assist* offers West Virginia a secure, interoperable, and adaptable IIS that strengthens public health outcomes, supports regulatory compliance, and delivers lasting value to West Virginians.

Additional Considerations

At the end of the Contract, Gainwell will grant the State, without additional license fees, a perpetual license to Gainwell *Assist*, subject to Gainwell's current license terms and conditions and exclusive of licenses to third-party embedded components or third-party software required for the operation of Gainwell *Assist*, solely for the State's internal government business purposes. Continued maintenance and support services, including updates if offered by Gainwell, will be provided pursuant to Gainwell's then-current terms and conditions for such services, including applicable maintenance and support fee(s). The continued use of Gainwell *Assist* is contingent upon the State obtaining required third-party software licenses and paying associated third-party license fees as necessary for the operation of the module.

Section 4: Project Specifications

RFP Reference: Section 4, p. 30

4.1 Background and Current Operating Environment

Background and Current Operating Environment: The West Virginia Department of Health operates an Immunization Information System (IIS) that manages statewide immunization records, supports public health reporting, and enables data exchange between healthcare providers, pharmacies, and public health agencies. The current solution is vendor-hosted in a remote cloud environment, providing centralized storage, access control, and secure transmission of vaccination data required for program management and mandatory federal reporting. The IIS maintains unique identifiers for 2,946,001 Patient Records, 31,929,498 Vaccination Records, and 14,164 User Accounts (Front End and HL7 no login users) to ensure accurate data linkage, auditability, and role-based access across all system modules.

Gainwell understands and acknowledges the information contained in the 4.1 Background and Current Operating Environment section above.

4.2 Project Goals and Mandatory Requirements

Project Goals and Mandatory Requirements: The agency desires an Immunization Information System (IIS) to securely collect, store, and manage vaccination records within its jurisdiction. The goal is to improve immunization tracking, enhance vaccination coverage, and support data-driven public health decision-making. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

Gainwell affirms and understands the above requirements. The State of West Virginia (the State) seeks a modern, cloud-hosted Immunization Information System (IIS) that is secure, confidential, and compliant with required federal and state security standards, including Federal Risk and Authorization Management Program (FedRAMP) Moderate or High authorization, Federal Information Processing Standards (FIPS) encryption, System and Organization Controls (SOC) 2 auditing, and six-year audit log retention.

The State requires an IIS that aligns with the Centers for Disease Control and Prevention (CDC) IIS Functional Standards and supports Advisory Committee on Immunization Practices (ACIP) guidelines and forecasting requirements. The IIS must improve data quality through deduplication and consolidation and enable seamless electronic data exchange using standards such as Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR), and integrations with electronic health record systems, vital records, and the CDC Vaccine Tracking System (VTrckS).

The State further prioritizes robust reporting and analytics for coverage assessments, reminder and recall, exemption tracking, and support for large-scale or emergency vaccination efforts. Additional objectives include comprehensive vaccine inventory management across Vaccines for Children (VFC), jurisdictional, and private stock; improved ordering and reconciliation workflows; and readiness for public-health emergencies supported by National Institute of Standards and Technology (NIST) SP 800-34-aligned business continuity and disaster recovery capabilities. Gainwell's proposal details the approach and methodology we will use to deliver a secure, interoperable IIS that advances data quality, improves immunization program operations, and fulfills the goals outlined in the Request for Proposal (RFP).4.2.1. CDC-Based Goals and Objectives.

4.2.1 CDC-Based Goals and Objectives

CDC-Based Goals and Objectives - The following goals and objectives are derived from the CDC's IIS Functional Standards and related guidance documents. While not mandatory for contract award, these capabilities reflect nationally recognized best practices and support long-term compliance, interoperability, and public health impact. The Vendor should address these items to demonstrate alignment with CDC goals and readiness for future federal initiatives.

Gainwell has reviewed and understands the CDC-based goals and objectives outlined by the State. Our capabilities align directly with these goals and with the State's readiness for future federal initiatives. This submission demonstrates how the Gainwell *Assist* solution aligns with nationally recognized standards and proven practices to improve immunization program performance and public health impact.

Gainwell *Assist* positions the State to meet CDC-based expectations by delivering an IIS built for continuous improvement and modernization. Gainwell *Assist* incorporates proven practices reflected in the CDC IIS Functional Standards and is designed to adapt as national expectations evolve, supporting future enhancements in interoperability, data, quality, forecasting, and public-health reporting. It enables the State to incorporate new CDC guidance and emerging federal

requirements without disruption. The table below summarizes key IIS capabilities that support the State's modernization objectives and the value each capability provides.

Table 1. Core IIS Modernization Capabilities

Capability Area	How Gainwell Assist Supports	Value to State
Data Quality Advancement	Uses the American Immunization Registry Association (AIRA) Data Quality Framework and configurable Public Health Information Network Vocabulary Access and Distribution System (PHIN-VADS) code sets to maintain accurate, complete, and timely data aligned with national IIS standards.	Improves data accuracy and validation, reduces errors, and confirms alignment with national IIS quality expectations.
Continuous Improvement	Teams participate in AIRA workgroups and adopt updated AIRA guidance and test cases, enabling the IIS to evolve alongside national standards.	Provides continuous system improvement aligned with national IIS evolution.
Evolving CDC Standards	Supports rapid adoption of updated HL7, FHIR, and AIRA Implementation Guide updates through a flexible interface engine.	Keep the IIS aligned with CDC and AIRA standards without delays or costly redevelopment.
Modernization and Scalability	Uses cloud, event-driven pipelines to support high message volumes and scalable IIS operations.	Enables the IIS to grow and perform reliably as statewide data exchange increases.
Future Federal Expectations	Aligns system capabilities with AIRA's forward-looking modernization workgroups to anticipate and accommodate federal policy shifts.	Reduces redesign risk and keeps the IIS ready for emerging CDC and federal requirements.
Long-Term Adaptability	Uses modular rules, configurable code sets, and adaptable mapping layers to support long-term IIS evolution without disruptive redevelopment.	Provides a future-proof IIS that adapts to new workflows, data types, and program changes.
Interoperability Evolution	Adopt an API-first and FHIR-ready design while supporting scalable HL7 message processing aligned with AIRA interoperability guidance.	Improves statewide connectivity and prepares West Virginia for next-generation data exchange models.

These capabilities provide West Virginia with a forward-looking IIS that remains aligned with national direction, supports long-term compliance, and strengthens the State's ability to evolve its immunization program as public-health priorities change.

Gainwell Assist also supports CDC-based expectations through ACIP-aligned clinical decision logic and forecasting capabilities that enhance the accuracy and consistency of immunization recommendations across the jurisdiction. These capabilities allow the IIS to evolve with clinical guidelines and improve data-driven program decisions as national standards advance. By integrating these functions within a scalable, adaptable platform, Gainwell Assist enables the State to maintain alignment with CDC objectives and continue improving immunization program performance as public health needs evolve.

4.2.1.1. Establish and Maintain a Secure, Confidential Immunization Information System

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.1.1. The IIS is physically and digitally secured in accordance with policies and industry standards for protected health information, security, and encryption.

4.2.1.1.1.1. The IIS establishes, documents, and updates policies and procedures to manage the collective functions, capabilities, and attributes of an IIS.

4.2.1.1.1.2. 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.

4.2.1.1.1.3. The IIS provides ongoing training to ensure awareness of and to promote adherence to policies and procedures.

4.2.1.1.2. The IIS is physically and digitally secured in accordance with industry standards for disaster avoidance, mitigation, and recovery.

4.2.1.1.2.1. The IIS establishes and maintains the infrastructure needed for disaster avoidance.

4.2.1.1.2.2. The IIS establishes and tests recovery plans to mitigate system downtime.

4.2.1.1.3. The IIS defines service expectation between the program and the entities providing information technology support to ensure system availability and uninterrupted data flows.

4.2.1.1.3.1. The IIS implements service-level agreements between the program and the entities providing information technology and support.

4.2.1.1.3.2. The IIS implements and maintains the infrastructure to fulfill service-level agreements.

Gainwell affirms its commitment to establishing and maintaining a secure, confidential Immunization Information System (IIS). The sections below describe how our proposed system achieves the Functional Standards outlined in the RFP.

4.2.1.1.1. Physical and Digital Security of Protected Health Information

The Gainwell Assist solution is a Software-as-a-Service (SaaS) system hosted in the Amazon Web Services (AWS), a cloud platform that maintains a broad portfolio of industry-recognized security certifications and compliance attestations. Gainwell will adhere to the State's Disaster Recovery (DR) frequency expectations, typically annually. AWS provides robust built-in security capabilities and services to increase privacy and control network access. These include:

- Next-generation firewalls within Amazon Virtual Private Cloud (VPC) with integrated Web Application Firewall (WAF) capabilities to manage private network traffic and control access to applications
- Encryption for data at rest and in transit across services using Transport Layer Security (TLS)
- Private connectivity options that support dedicated, secure communication between system components
- Automatic encryption of traffic across AWS global and regional networks between secured AWS facilities

AWS enables clients to operate securely in the cloud by providing an infrastructure designed and managed in alignment with federal, state, and industry security frameworks.

The AWS cloud environment supports compliance with regulations and standards such as Health Insurance and Portability Act (HIPAA), the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline, and multiple National Institute of Standards and Technology (NIST) security and control frameworks. AWS maintains more than 1,800 security controls across its services and offers a comprehensive suite of security capabilities, including access control, encryption, logging and monitoring, and threat-detection services to support security and compliance needs.

Our modern, commercial-off-the-shelf (COTS) solution supports Secure Sockets Layer (SSL) connectivity through Internet Protocol Security (IPsec) virtual private network (VPN) as the primary external link. External connections pass through a VPN gateway before entering the VPC. The architecture uses multiple AWS Availability Zones so that if one Availability Zone becomes unavailable, the other Availability Zone can continue to process information. These Availability Zones are located in separate geographic areas, and the databases are replicated in real time between database servers in each Availability Zone to reduce the risk of downtime and data loss. Gainwell provides secure hosting and backup services that meet the State's security requirements, including regular backups of State data and systems hosted in the AWS cloud.

4.2.1.1.1. Policies and Procedures for Managing IIS Functions and Capabilities

The IIS establishes, documents, and updates policies and procedures to manage its functions, capabilities, and operational attributes through a structured set of strategies. These strategies confirm the IIS operates effectively, maintains data quality, and remains aligned with applicable standards and policies. The sections below summarize how Gainwell Assist supports these governance and operational needs.

Data Governance and Support for Internal Policy and Procedures. Gainwell applies a proven approach to data governance that supports the development, documentation, and management of defined data entities, attributes, data models, and relationships. This approach promotes consistent interpretation and use of program data and aligns with State Data Governance standards.

Key features include the use of normalized or de-normalized tables for efficient operations, controls over relationships among database tables, and safeguards to prevent duplicate or orphan records.

Data Integrity Support. Data integrity is maintained through coordinated database management, application controls, documented procedures, and security measures. Gainwell's database administrators manage the information model according to established processes, including data-element naming standards, mapping to logical and physical data models, value enforcement, and validation algorithms. To protect data in transit, the system employs strong encryption methods and public/private key pairs to support secure web transactions and prevent unauthorized modifications.

Managing Additional Requirements. Gainwell is equipped to support new or evolving governance and compliance requirements by conducting targeted gap analyses to identify necessary controls. We update or develop policies and procedures to address new specifications; establish operational processes and controls to support compliance, including staff training and workflow integration; and collaborate with stakeholders to confirm the implementation aligns with program priorities and expectations.

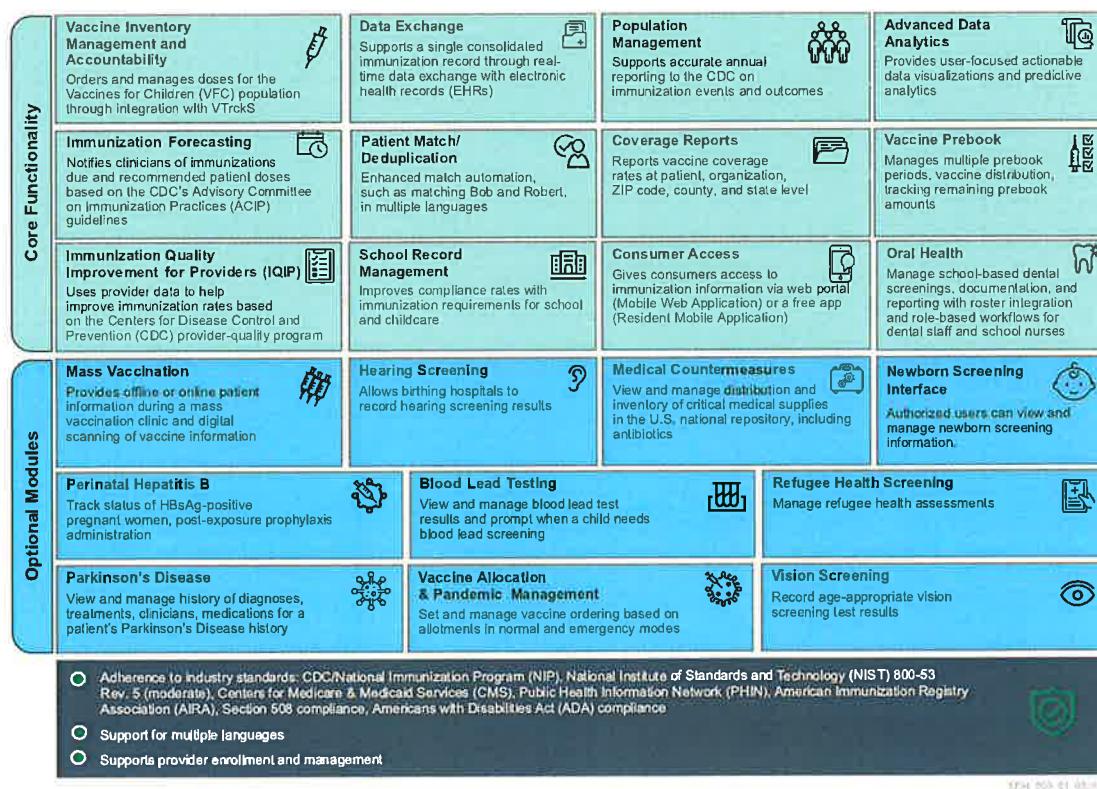
4.2.1.1.1.2. Technical Infrastructure for Secure IIS Data Capture and Processing

On the infrastructure side, our Gainwell Assist Solution is deployed in a **multi-available zones AWS cloud environment** with disaster recovery capabilities. This architecture maintains continuity of service even in the rare event of a Availability Zone outage. Security and compliance are foundational; our solution aligns with **NIST 800-53 Rev. 5, SOC 2 Type 2, and HIPAA standards**.

Together, these capabilities provide the State more than an immunization registry. They deliver a **secure, resilient, and user-centered platform that supports public health leaders, providers, and individuals, while promoting equity and reliability across the State**.

The figure below provides an overview of our proposed Gainwell Assist solution for the State. The core functionality shown will be delivered as part of the base immunization system. Optional modules (blue color) are available for future expansion and can be incorporated through a change order. Since these modules are already developed, the State can readily leverage them as new needs arise. Gainwell will apply relevant standards consistently across the base solution and other supported modules.

Figure 1. Proposed Gainwell Assist Solution



Cloud Solution Architecture

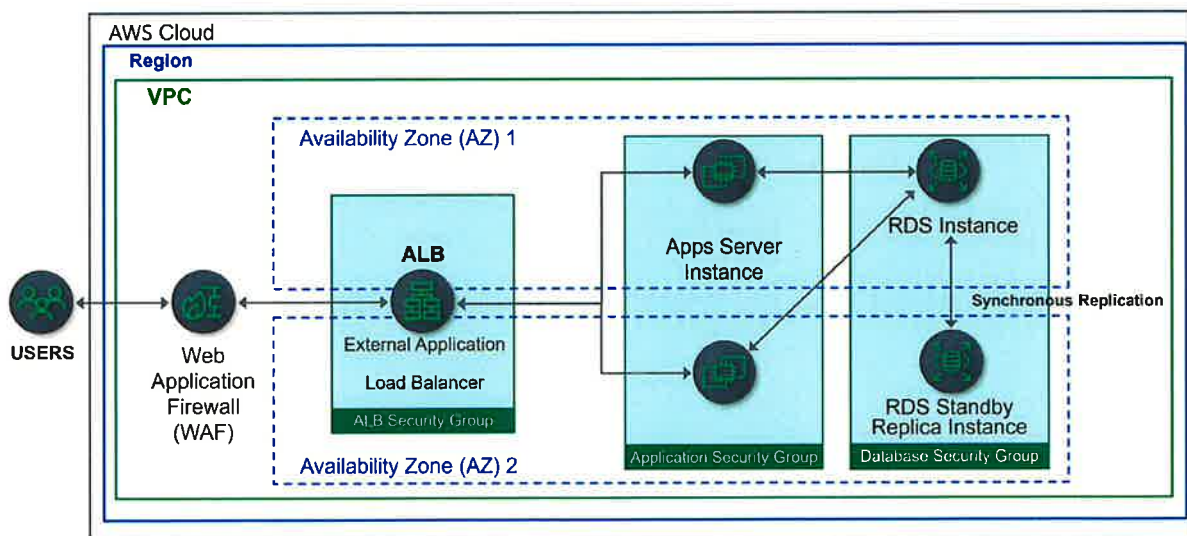
Gainwell Assist adapts for reliable operations. Infrastructure virtualization enables Gainwell Assist to meet capacity and throughput without degradation of performance. We also incorporated comprehensive physical and system security protocols into the IIS infrastructure that reduce the risk of threat from malicious attacks.

Gainwell Assist is deployed using an AWS cloud environment that delivers improved throughput and performance relative to legacy platforms. It combines the benefits of COTS/SaaS with single-tenant design, providing the security and flexibility needed for West Virginia-specific operational scheduling and controls.

The front-end application servers run on Amazon Elastic Compute Cloud (EC2) instances. Traffic is distributed across multiple EC2 instances using Amazon Application Load Balancers to confirm efficient load handling. The application database uses PostgreSQL, operated through Amazon Relational Database Services (RDS). Amazon RDS for PostgreSQL simplified database administration by managing hardware provisioning, database setup, patching, backups, and scaling, allowing the system to maintain reliable performance with reduced operational overhead.

As the following diagram illustrates, Gainwell Assist's standards-compliant cloud architecture provides firewall protection, load balancing, redundancy, and synchronous replication to keep the system running smoothly. In the rare event of a server or application issue, the architecture uses multiple AWS Availability Zones, each with independent power and networking, to enable seamless failover. This resilient design protects against data loss and minimizes downtime, delivering continuous availability for West Virginia.

Figure 2. AWS Architecture Diagram



Key elements in each environment include the Application Server instance and the RDS that manages database servers in the cloud, with traffic orchestrated using an External Application Load Balancer. At the database instance level, we have designed Gainwell Assist with the RDS reporting instance separate from the transaction RDS instance, providing even more power and resource balancing than within a shared RDS instance. We use advanced monitoring tools to track throughput and performance and scale the database accordingly. This will help the State gain both operational efficiency and financial predictability.

Security is built into each layer of the architecture. The system uses multi-layered physical, system, and network protections, aligned with NIST 800-53, HIPAA, and Internal Revenue Service (IRS) Pub 1075 standards, to safeguard protected health information against malicious threats. These protections are continuously monitored, and automated patching and upgrades allow the State to benefit from the latest safeguards without the burden of manual intervention.

Gainwell Assist provides the State with a future-proof IIS. Its cloud design supports growth and adaptation as the State's immunization program evolves, while maintaining consistent, uninterrupted service across communities.

Gainwell establishes and maintains the technical infrastructure to securely capture, store, and process patient demographic and vaccination data through several measures:

- **Role-Based Access and Single Sign-on (SSO).** Defines user access based on role and supports SSO to applications, verifying users have the appropriate permissions through integration with identity and access management solutions.
- **Data Security and Encryption.** Protects data using industry proven practices, including encryption at rest and in transit with advanced encryption standards (AES-256), helping safeguard information from unauthorized access and maintains compliance with applicable standards.
- **Security Policies and Compliance.** Maintains security policies aligned with International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and NIST guidelines, covering access control, data protection, and incident response. Conducts regular audits and assessments to support compliance with regulations such as HIPAA.
- **Data Integrity and Management.** Enforces data integrity through database and application management, policies, procedures, and security measures. This includes protections against modification of data in transit, strong encryption methods, and maintaining audit logs to track changes.
- **Risk Management and Incident Response.** Conducts regular risk assessments to identify threats and vulnerabilities and implements mitigation strategies. A defined incident response plan outlines procedures for detecting, reporting, and responding to security incidents, supported by continuous monitoring and logging.
- **Data Governance and Compliance.** Promotes data governance throughout the data-lifecycle, supporting implementation and operations to meet internal and external requirements, including reporting, regulatory compliance, and privacy policies, working in alignment with governance frameworks and councils.

4.2.1.1.1.3. Ongoing Training to Support Policy and Procedure Compliance

Gainwell implements its comprehensive role-based Training Plan before go-live. By offering multiple training formats (online, guided seminar, recorded) and providing clear, plain-language user manuals, we help users feel confident and prepared. A successful implementation depends on user readiness, and our methodology trains users effectively while preparing systems and processes for a smooth go-live.

- **Role-based Training Program.** We develop and deliver a comprehensive training program tailored to the needs of each user group. Using a mix of guided online seminars, recorded sessions, and detailed user manuals, we confirm each user is confident and capable in using the new IIS.
- **Operational Readiness Review (ORR).** Before go-live, we conduct a thorough ORR to validate that the technical, operational, and organizational components are in place. This includes confirming system performance, support-staff readiness, and workflow validation. We provide a final ORR report with a clear go/no-go recommendation to support a confident and successful launch.

4.2.1.1.2. Physical and Digital Security for Disaster Avoidance, Mitigation, and Recovery

Gainwell *Assist* is deployed in **the East Region of AWS' cloud environment**. Security and compliance are foundational; we are compliant with **NIST 800-53 Rev. 5, SOC 2 Type 2, and HIPAA standards**. Our team's deployment across multiple AWS Availability Zones provides a resilient environment that guards against downtime and data loss.

Gainwell employs a comprehensive approach to physical and digital security for the IIS, following industry standards for disaster avoidance, mitigation, and recovery. Gainwell's security measures are built to exceed standard expectation and provide strong protection and confidentiality for IIS data, as described below.

- **Risk Management Assessment.** Regular risk assessments identify potential threats and vulnerabilities and evaluate the likelihood and impact of security risks. Mitigation strategies are developed from these assessments to reduce risks to acceptable levels.
- **Policy and Governance.** Gainwell develops and maintains security policies aligned with standards such as ISO/IEC 27001 and NIST guidelines. These policies address access control, data protection, and incident response. Compliance with HIPAA and other legal requirements is supported through regular audits and assessments.
- **Access Control and Identity Management.** Role-Based Access Control (RBAC) grants access based on the principle of least privilege, and Multi-Factor Authentication (MFA) adds a second layer of verification before accessing sensitive systems.
- **Data Protection.** Data is encrypted in transit and at rest using advanced encryption standards (AES-256) protections. Sensitive information is masked or anonymized as needed, especially for testing and analytics activities.
- **Incident Response and Management.** Gainwell maintains a detailed incident response plan that defines procedures for identifying, reporting, and addressing security incidents. Continuous monitoring and logging of network and system activity support early identification of potential issues. Security Information and Event Management (SIEM) tools support efficient incident handling.
- **Continuous Improvement.** Security audits and penetration tests are conducted regularly to identify vulnerabilities and remediate them. Client-facing reports from these evaluations promote transparency and shared improvement of security controls.
- **Business Continuity and Disaster Recovery.** Gainwell's business continuity and disaster recovery (BC/DR) approach uses a production architecture designed for reliability and resiliency without single points of failure. AWS Cloud capabilities provide redundancy and fault tolerance through Availability Zones, allowing operations to continue even if one zone becomes unavailable.
- **Physical Security.** AWS data centers apply multiple levels of physical protection, including badge and PIN access, cameras, fire suppression systems, uninterruptible power supply (UPS) resources, and backup generators. Cameras monitor critical access points with recordings retained for 30 days, and windows are equipped with alarmed glass-break sensors. Networks and servers are protected by firewalls and monitored for intrusion detection.

4.2.1.1.2.1. Infrastructure Needed for Disaster Avoidance

The IIS maintains the infrastructure needed for disaster avoidance through the strategies and technologies described below. Together, these capabilities support a resilient environment that delivers continuous availability and protects against potential disruptions.

- **AWS Cloud.** The infrastructure is architected using AWS Cloud, which supports rapid deployment of additional servers, memory, and storage as needed. This flexibility supports ongoing capacity needs and helps maintain business continuity.
- **High-Availability Architecture for Disaster Recovery.** The production environment is designed for reliability and resiliency with no single point of failure. AWS provides redundancy and fault tolerance using multiple AZs within a region. If one AZ goes down, operations can continue in another AZ, providing continuous availability.

4.2.1.1.2.2. Establish and Test Recovery Plans

The IIS establishes and tests recovery plans to mitigate system downtime through a comprehensive Business Continuity and Disaster Recovery (BC/DR) framework. This framework complies with NIST SP 800-34 Contingency Planning Guide for Federal Information Systems standards. Key elements include:

- **BC/DR Plan.** A BC/DR Plan is provided, identifying core business processes included in the Gainwell Assist Solution in accordance with the State's requirements.

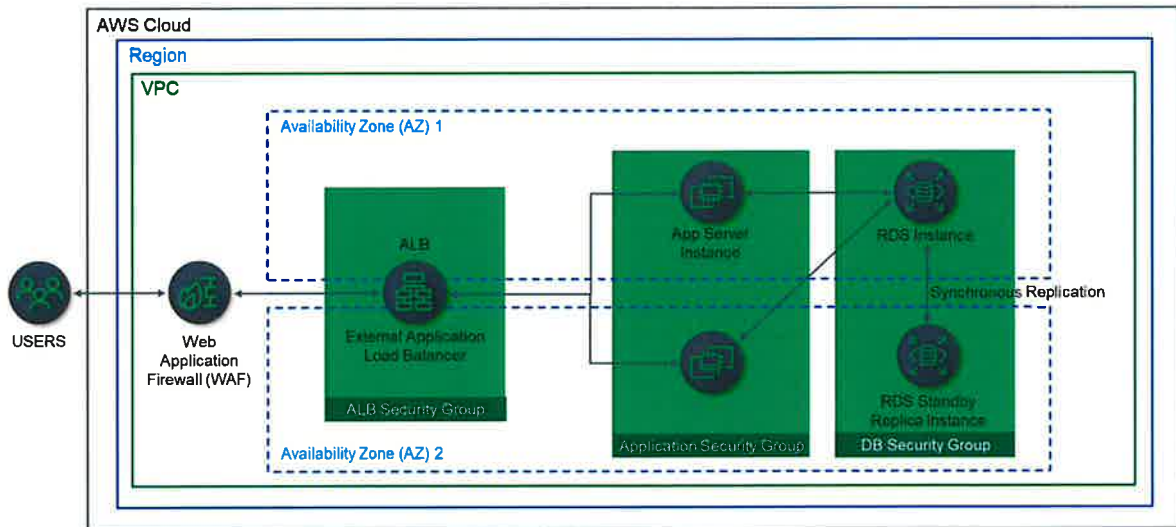
The plan supports recovery of critical services and includes a notification process in the event of a disaster. It is updated at least annually to incorporate new functionality.

- **BC/DR Testing.** BC/DR Plan testing is conducted as part of operational readiness and performed annually to demonstrate compliance with service level agreements (SLAs). Gainwell works with State stakeholders to determine DR test dates. Testing includes collaboration with State partners to validate connectivity and interoperability for integrated applications. Test reports are delivered within five business days of the exercise, and BC/DR Plan updates are provided within one business day when deficiencies are identified. Lessons learned are documented and incorporated into the Continuous Improvement Plan.
- **Backup and Restore Procedures.** Gainwell's backup and restore procedures for data hosted in the AWS Cloud support the State's backup and retention requirements in accordance with SLAs.

4.2.1.1.3 Service Expectation to Confirm System Availability and Uninterrupted Data Flows

Gainwell Assist's standards-compliant cloud architecture provides a firewall, load balancing, redundancy, and synchronous replication to confirm the system is running smoothly. In the rare event of a server or application issue, our architecture leverages multiple AWS Availability Zones, each with independent power and networking, to enable seamless failover. This resilient design protects against data loss and minimizes downtime, delivering continuous availability to the State. The following diagram illustrates security and data flows within our system architecture.

Figure 3. AWS Architecture Diagram



Key elements in each environment include the Application Server instance and the RDS that manages database servers in the cloud, with traffic routed through an External Application Load Balancer. At the database layer, Gainwell Assist uses a dedicated RDS reporting instance separate from the primary transactional RDS instance, providing stronger performance and more balanced resource usage than a shared configuration. Advanced monitoring tools track throughput and performance and allow the database tier to scale as needed. This approach supports both operational efficiency and financial predictability for the State.

Security is embedded throughout the architecture. The system applies multiple layers of physical, system, and network protections aligned with NIST 800-53 controls, HIPAA, and IRS Pub 1075 standards. These protections are continuously monitored, and automated patching and upgrades help the State benefit from the latest safeguards without manual effort.

Gainwell Assist provides the State with a future-proof IIS by delivering a secure scalable cloud-based Software as a Service (SaaS) solution that can adapt as the State's immunization program evolves while maintaining uninterrupted service across communities.

Gainwell monitors the performance of the Gainwell Assist solution and maintains processes and procedures to restore systems in the event of partial or full failure, support capacity planning, and address security risks and vulnerabilities.

4.2.1.1.3.1. and 4.2.1.1.3.2. Service-Level Agreement Implementation

We regularly track performance indicators such as response time, resource availability, central processing unit (CPU) utilization, network load, memory usage, and application performance to identify conditions that may affect SLAs or system stability. AWS provides continuous monitoring of the underlying cloud environment, which complements Gainwell's oversight. Gainwell is fully committed to meeting or exceeding each SLA specified in Attachment C of the RFP.

4.2.1.2. Continuously Improve IIS Data Quality

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.2.1. The IIS validates patient demographic and vaccination data.

4.2.1.2.1.1. The IIS supports the identification, prevention, and resolution of duplicate and fragmented patient demographic and vaccination data in accordance with policies and procedures.

4.2.1.2.1.2. The IIS monitors data quality within the IIS in accordance with policies and procedures.

4.2.1.2.1.3. The IIS uses electronic tools to standardize and/or validate addresses in the IIS.

4.2.1.2.1.4. The IIS delivers feedback and training to IIS partners and providers to ensure complete, timely, and accurate patient demographic and vaccination records.

4.2.1.2.1.5. The IIS meets federal and jurisdictional data quality metrics.

Gainwell verifies continuous improvement of the IIS' data quality. We describe how our proposed system achieves the Functional Standards listed in the RFP below.

4.2.1.2.1. Validation of Patient Demographic and Vaccination Data

Gainwell *Assist* supports data exchange with national systems such as VTrckS via an External Information System (ExIS) interface, which is part of our Vaccine Inventory Management and Accountability functional area. Further demonstrating our collaboration with external partners, our solution complies with CDC IIS Functional Standards and incorporates guidance from AIRA. Gainwell *Assist* adheres to data requirements, technical guidance for data transport and deduplication, and Clinical Decision Support for immunizations (CDSi), also known as vaccine forecasting. Our approach to data quality aligns with the CDC's IIS Data Quality Blueprint and AIRA's IIS Best Practices Community of Practice, focusing on data availability, completeness, and timeliness.

Data quality is built into the system. Through **automated deduplication, identity resolution, and real-time validation of addresses and provider records**, Gainwell *Assist* maintains clean, accurate, and reliable immunization data for the State and reduces common data integrity challenges.

Through Quality Assurance activities, Gainwell develops and executes test plans, manages defect resolution, and verifies deliverables meet acceptance criteria. Debriefs and joint action plan sessions with the State accelerate feedback and translate findings into measurable improvements.

Quality and security are integrated throughout our methodology. From secure coding practices based on MITRE recommendations and robust testing cycles to a proactive approach to HIPAA compliance, we protect the integrity and confidentiality of the State's critical immunization data. Gainwell is a dedicated partner in supporting the State's pursuit of future CDC and Office of the National Coordinator for Health Information Technology (ONC) Data Quality Certification (once available), providing both the tools and expertise need to achieve these goals:

- **Proactive data quality management** that reduces errors and provides real-time feedback
- **Transparent reporting** based on CDC and AIRA metrics that highlights improvement opportunities
- **Expert guidance** from experienced subject matter experts (SMEs), supported by high-quality documentation

Product Improvement, Service Delivery, and Client Satisfaction Processes

Alongside our implementation methodology, Gainwell Voice™ and Gainwell Assure™ provide self-monitoring and self-correcting mechanisms that strengthen product quality, service delivery, and client satisfaction. To support continuous improvement, high-quality service, and strong client satisfaction, Gainwell uses two key tools:

- **Gainwell Voice.** Activities include executive-level engagement, client satisfaction interviews, customer surveys, IIS product user groups, and participation in executive councils.
- **Gainwell Assure.** Independent, in-depth quality and risk reviews performed by account and delivery leaders. During implementation, these reviews occur once per project phase; during maintenance and operations (M&O), they occur annually or more frequent upon request.

Comprehensive Testing and Quality Assurance

Gainwell's rigorous, multilayered testing strategy identifies and resolves defects early so we can deliver a high-quality, reliable, and performant system. We execute the Test Management Plan and complete multiple cycles of system, integration, interface, and regression testing. We fully support the State throughout User Acceptance Testing (UAT), including a dedicated UAT environment and detailed test cases and scripts.

User Adoption and Training

Low adoption by providers, school nurses, and other users can reduce the value of a new system and affect data quality. Gainwell implements its comprehensive role-based Training Plan 90 days before go-live. By offering multiple training formats (online, guided seminar, and recorded modules) and developing clear, plain-language user manuals, we help users feel confident and prepared.

The IIS validates patient demographic and vaccination data through the following mechanisms:

- **Data Integrity Support.** Data integrity is maintained through database and application management, policies, procedures, and security controls. Database administrators manage the information model following documented processes that include naming conventions, alignment to logical and physical data models, valid-value enforcement, and defined validation rules. Protections include preventing modification of data in transit using strong encryption and public/private key pairs for secure web transactions. Audit logs track inbound and outbound files and record applied changes to maintain data integrity. Original files are retained for extended periods for reprocessing when needed, and data is stored in normalized transactional databases to minimize redundancy and preserve accuracy. Controls prevent duplicate or orphan records.
- **Data Transmissions and Standards.** Data transmissions follow agreed-upon content, format, metadata, and reference-data exceptions using defined layouts and delivery methods. The services framework is built for maximum interoperability and follows industry standards for communications, security, and data formats, including Simple Object Access Protocol (SOAP), Representational State Transfer (REST) web services, Secure File Transfer Protocol (SFTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Council for Affordable Quality Healthcare (CAQH) guidelines, Extensible Markup Language (XML), JavaScript Object Notation (JSON), and delimited and positional text files.
- **Data Dictionaries and Reference Data.** Clear data dictionaries, data rules, and standard reference data are used across system modules. Master Data Management (MDM) practices govern reference data, standard data elements, and consistent definitions in alignment with

the State. This approach supports the State's data lake integrity by aligning data and reference standards across as directed and aligning with reference data standards within the data lake to verify reporting is accurate across environments.

4.2.1.2.1.1. Identification and Resolution of Duplicate and Fragmented IIS Records

The IIS supports the identification, prevention, and resolution of duplicate or fragmented patient demographic and vaccination data through the methods described below. Together, these capabilities promote data integrity and accuracy in accordance with established policies and procedures.

Data Integrity Support. Gainwell maintains data integrity through comprehensive database and application management, documented procedures, and strong security controls. Database administrators manage the information model using established processes that guide the end-to-end lifecycle, including data-element naming conventions, alignment to logical and physical data models, valid-value enforcement, and defined validation algorithms.

Safeguards protect data in transit through strong encryption techniques and the use of public and private key pairs for secure web transactions. Audit logs document inbound and outbound files and record applied changes to maintain the integrity of healthcare data. Original files are retained for extended periods to support reprocessing when needed, and data is stored in normalized transactional databases to reduce redundancy and preserve accuracy. Relationships among tables are managed carefully to prevent duplicate or orphan records.

Data Governance and Support. Gainwell applies a proven approach to data governance that supports internal policies and procedures for documenting, developing, managing defined data entities, attributes, models, and relationships. This framework promotes consistent use of data and aligns with the State's Data Governance standards.

Governance practices guide the structure of data tables, relationships, and definitions across the IIS to maintain accuracy and meaning throughout the system.

Database Structures and Controls: Module components are supported by database structures that set and control data relations using foreign key constraints. The relationships of data elements within and across business components are enforced by these foreign keys, preventing data entry without the proper relationships existing first. Additionally, primary keys are used to prevent internal duplication of data, and orphaned rows are prevented with foreign key table relationships.

Issue Identification and Resolution. Gainwell uses management and monitoring tools, the State's service portal, and escalations from the State's enterprise call solution to identify and diagnose support needs. We investigate and resolve issues through a structured process that incorporates both application and database review. These activities help verify data relationships are functioning as expected and that system behavior aligns with established policies and procedures.

4.2.1.2.1.2. Monitoring of IIS Data Quality

The IIS monitors data quality in accordance with State policies and procedures through several mechanisms:

- **Data Governance and Integration.** Gainwell coordinates with the State to align existing governance processes and procedures with the State's Governance Framework. Activities include applying data standards, sharing metadata, managing data quality, usage, and security for data management within each module and sharing with external modules and

vendors. Gainwell contributes to the State's Data Governance initiatives such as enterprise data modeling, data dictionaries, ETL mappings, and other source-to-target mappings to record and maintain enterprise data assets. We also establish working relationships with the State's governance bodies for review of Data Governance policies, deliverables, metadata, and interface deliverables.

- **Data Integrity and Security.** Gainwell maintains data integrity to validate key identifiers and protect the accuracy of data, including referential integrity. We establish standards for data masking and de-identification for testing, define AWS settings for intrusion detection and prevention, unauthorized access, disruptions, and disclosures, and define role-based access to data while facilitating Single Sign-on (SSO) to applications with the State's security management. In addition, Gainwell defines rules and security for data archiving and purging.
- **Data Storage and Compliance.** Data is stored, archived, retrieved, and purged according to the State's security policies, procedures, and standards, with a minimum retention period of 10 years for application, network, system, and perimeter data including logs, files, and records. Gainwell schedules security and data assessment activities supporting Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0, NIST 800-53 management, and maintains compliance with updated State Data Policies and Standards.
- **Data Catalogs and Metadata Management.** Gainwell creates and maintains data catalogs according to the State's standards and captures metadata, including business and technical metadata, supporting the Enterprise Metadata Repository. We work with Integration Services Layer (ISL) vendors to establish standards for data sharing, maintenance, interfacing, and reference data usage.
- **Audit Logs and Monitoring.** Gainwell uses tools such as SIEM, Amazon CloudWatch, and CloudTrail to manage logs.

Audit logs and data files used for process and system databases are based on user-defined auditable events and backed up daily to maintain ready access to system data.
- **Technology Standards and Reporting.** We support standard reporting, dashboard, and SLA/KPI reporting and visualizations for member-related data. Gainwell verifies compliance with industry standards and integrates data for advanced analytics and reporting.

4.2.1.2.1.3. *Electronic Address Standardization and Validation in the IIS*

Data exchange is **seamless and standards-driven**, with support for HL7 v2.5.1 and integration with the CDC's Immunization Gateway and provider EHRs. This enables real-time, two-way information sharing that supports coordinated care.

Data quality is built into the system. Through **automated deduplication, identity resolution, and real-time validation of addresses and provider records**, Gainwell Assist maintains clean, accurate, and reliable immunization data for the State.

Gainwell Assist supports data exchange through both flat-file interfaces and HL7 web services. It is fully compliant with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, and leverages SOAP-based transport using the standard CDC and Immunization Gateway (IZ Gateway) Web Services Description Language (WSDL). We collaborate with the State to define and implement the required integration with the Master Client Index (MCI). Through this integration, Gainwell Assist exchanges demographic records to verify records are accurately registered, matched, and merged. We have extensive experience integrating across multiple states, delivering reliable interoperability and accurate client identity management.

Smarty, a Coding Accurate Support System (CASS)-certified service, is used to standardize address fields to the United States Postal Service (USPS) format. It validates and cleanses new address data by cross-checking entries against a comprehensive reference database and applying data-cleansing algorithms to verify accuracy and standardize formatting. Smarty corrects issues such as misspelled street names, incorrect postal codes, or incomplete addresses when possible. It also performs real time validation during data entry and provides batch validation for imported or migrated data. In addition, Smarty's embedded geocoding classifies addresses by geographic region and can recognize and correct or reject invalid postal codes and counties.

4.2.1.2.1.4. Feedback and Training for Complete and Accurate IIS Records

The IIS delivers feedback and training to partners and providers to support complete, timely, and accurate patient demographic and vaccination records through a comprehensive training approach. This approach includes evaluating training needs, identifying appropriate participants, and developing materials that meet user expectations. Gainwell provides qualified training staff to design, organize, and lead training and education activities, including train-the-trainer sessions. Training is offered through multiple formats such as in-person and remote instructor-led sessions, webinars, on-demand video modules, online help, and user documentation.

These resources document technical processes and identifies subject matter expert contacts for additional support. Training materials and learning path inputs are incorporated into the Learning Management System (LMS), drawing on proven materials from similar projects. The training experience is continuously monitored, evaluated, and refined using feedback collected through post-training surveys. This feedback identifies topics that may need to be revisited and informs ongoing improvements to training content and delivery.

4.2.1.2.1.5. Federal and Jurisdictional Data Quality Metrics

Our data management frameworks are built on principles of security, quality, and governance. We apply rigorous data cleansing, validation, and deduplication processes to maintain a high-integrity single source of truth. Data is managed in compliance with federal and State regulations, including HIPAA and NIST standards, and we bring a strong record of collaboration with federal partners such as CMS, CDC, ONC, and AIRA.

The IIS meets federal and jurisdictional data quality metrics through the methods listed below. These methods help the system maintain data integrity, alignment, and compliance with industry standards.

Data Dictionaries and Standards. Clear data dictionaries, data rules, and standard reference data are used to support consistent and accurate data management.

Master Data Management (MDM). Gainwell applies Master Data Management practices for reference data, standard data elements, and definitions to verify data quality and integrity. This confirms reporting accuracy across environments and supports the State's data lake integrity.

HL7. Most IIS systems operating in the United States rely on HL7 v2.5.1, guided by AIRA and CDC implementation guides. This version is optimized for high-volume, transactional immunization workflows. Key characteristics include:

- Vaccination Update (VXU) messages for reporting administered doses.
- Query by Parameter (QBP) messages for requesting a patient's immunization history.
- Response (RSP) messages returning the IIS record.

- Acknowledgement (ACK) messages confirming receipt and identifying errors.
- Standard code sets including Clinical Vaccine Administered (CVX), Manufacturer Vaccine Code (MVX), and National Drug Code (NDC).

HL7 v2.5.1 is highly structured and predictable, making it ideal for large-scale IIS operations.

Why HL7 Matters for Modern Immunization Systems

HL7 is foundational because it enables:

- Nationwide interoperability across thousands of electronic health records (EHRs) and providers.
- Scalability during outbreaks, pandemics, and high-volume reporting.
- Consistency in vaccine coding, patient identity, and clinical detail.
- Adaptability as new vaccines, schedules, and reporting requirements emerge.
- Future readiness for FHIR-based Application Programming Interfaces (APIs) and modern data exchange models.

HL7 is both the backbone of today's IIS and the bridge to tomorrow's immunization data ecosystem.

Data Integration Solutions. The module is configured with the ISL to support required data exchanges, providing secure and accurate data exchange among business associates, the State, and federal entities.

Monitoring Tools. Gainwell uses environment monitoring tools that enable compliance with the State's technology stack and technical requirements.

4.2.1.3 Promote Electronic Data Exchange Between the IIS and its Partners and Providers

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.3.1. Manage interfaces for exchange and integration of data electronically between the IIS and other information systems in accordance with federal and jurisdictional standards.

4.2.1.3.1.1. The IIS exchanges data in accordance with current interoperability standards endorsed by CDC for message content, format, and transport.

4.2.1.3.1.2. The IIS actively recruits, enrolls, and onboards IIS partners and providers for electronic data exchange.

4.2.1.3.1.3. The IIS actively monitors and evaluates data submitted via electronic data exchange.

4.2.1.3.1.4. The IIS investigates and resolves electronic data exchange errors and anomalies with IIS partners and providers.

Gainwell currently serves more than 40 state agencies and 175 Managed Care Organizations (MCOs).

To perform our coordination of benefits (COB) and payment integrity (PI) services, we have established data exchange agreements with more than 1,700 trading partners, including commercial insurance carriers and third-party administrators. We manage an average of 800,000 electronic data file exchanges each month, a testament to our deep integration and collaboration with a wide array of national and regional organizations. Below are additional details about our data exchange system.

4.2.1.3.1. Management of Interfaces for Exchange and Integration of Data

The Gainwell team is deeply versed in the critical frameworks and initiatives shaping the future of public health data. Our solutions fully support and comply with federal and jurisdictional standards.

CDC Message Mapping Guides (MMGs)

Our team has direct, hands-on experience implementing and maintaining systems that conform to CDC MMGs for immunizations (HL7 2.5.1, VXU, QBP) and other public health reporting. Data exchanged with the CDC and other partners is structured correctly, facilitating accurate national reporting and surveillance.

Gainwell *Assist* complies fully with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5. It uses SOAP-based transport with the standard CDC and Immunization (IZ) Gateway Web Services Description Language (WSDL) and supports flat-file import and vital records file submission. **This compliance continues as part of our product roadmap. We deliver quarterly compliance releases aligned with CDC's roadmap, keeping West Virginia current without extra cost or change orders, a distinct advantage of Gainwell *Assist*.**

In addition to standards compliance, Gainwell's interface management approach emphasizes scalability, resiliency, and operational continuity. The proposed approach employs a structured, collaborative, and risk-mitigated methodology to support high-volume HL7 message processing while maintaining efficient error management and continuity of data flow. Through near-real-time validation, monitoring, and configurable reprocessing workflows, the solution supports the timely identification and resolution of messaging errors without impeding overall system operations. This design aligns with the State's published peak-load assumptions and is intended to minimize disruption, support continuity of operations, and maintain system performance during normal operations, peak usage periods, and seasonal surges.

4.2.1.3.1.1. Standards-Based IIS Data Exchange

Building on this standards-compliant foundation, data exchange is seamless and standards-driven, with support for HL7 v2.5.1 and integration with the CDC's Immunization Gateway and EHRs. This enables real-time, two-way information sharing that supports coordinated care.

Further, data quality is built into the system. Through **automated deduplication, identity resolution, and real-time validation of addresses and provider records**, Gainwell *Assist* helps maintain clean, accurate, and reliable immunization data for the State. This eliminates many data integrity challenges.

Gainwell *Assist* is designed with **users in mind**. A responsive interface supports rural bandwidth limitations, while dashboards give providers, schools, and public health staff easy-to-use tools for decision-making.

For the State, **the system provides** users convenient, secure access to their immunization records. This is a key step in improving consumer empowerment and public trust.

We collaborate with the State to define and implement the required integration. Through this integration, our solution exchanges demographic records to confirm client records are accurately registered, matched, and merged. We have extensive experience in integrating with MCIs across multiple states, delivering reliable interoperability and accurate client identity management.

4.2.1.3.3.1.2. IIS Partner Recruitment and Onboarding

Collaborating with Partners

Our project methodology is inherently collaborative. We have decades of experience working within the intricate ecosystem of public health, fostering strong partnerships with government agencies; data exchange networks; and national and State to achieve shared goals. We collaborate with state public health leaders, bringing firsthand knowledge of the State's partnership environment.

- **Government Agencies.** We serve as a trusted technology partner to numerous State public health departments, Medicaid agencies, and federal bodies such as the Centers for Medicare and Medicaid Services (CMS) and the CDC. This work involves constant communication, joint planning, and a deep understanding of government program objectives and regulatory landscapes.
- **Data Exchange Networks.** We have successfully integrated our systems with a wide array of Health Information Exchanges (HIEs), Immunization (IZ) Gateways, and other data exchange partners.
- **National Organizations.** We align our work with guidance from national standards-setting bodies and organizations such as the American Immunization Registry Association (AIRA), the Public Health informatics Institute (PHII), and HL7 International. This alignment keeps our solutions compliant and forward-thinking, moving with the future direction of public health IT.

Gainwell brings a strong record of collaboration with federal partners such as CMS, CDC, and ONC ecosystems. Gainwell Assist includes an evidence-based immunization decision support solution that aligns with the latest CDC Clinical Decision Support for Immunization (CDSi) materials. It is test-driven and continually validated through national benchmarking via AIRA. Gainwell Assist features a forecasting component that imports immunization schedules directly from the CDC, enabling near-real-time vaccine forecasting without the need for developer or business analyst support to update the system.

We have managed large-scale, multi-stakeholder implementations, demonstrating our ability to align technology, governance, and data across complex agency and vendor environments.

Gainwell Assist supports data exchange with national systems via an External Information System (ExIS) interface, which is part of our Vaccine Inventory Management and Accountability functional area. Further demonstrating our collaboration with external partners, Gainwell Assist complies with CDC IIS Functional Standards and incorporates guidance from AIRA. In addition, Gainwell Assist adheres to data requirements, technical guidance for data transport and deduplication, and Clinical Decision Support for immunizations (CDSi), also known as vaccine forecasting. Our approach to data quality aligns with the CDC's IIS Data Quality Blueprint and AIRA's IIS Best Practices Community of Practice, focusing on data availability, completeness, and timeliness.

Gainwell Assist exchanges data with health information systems in accordance with current interoperability standards endorsed by the CDC and follows AIRA's guidance for acknowledgement (ACK) messages. It fully complies with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging and supports multiple data exchange options, including Simple Object Access Protocol (SOAP)-based transport and flat-file import. Gainwell Assist is architected on the Fast Healthcare Interoperability Resources (FHIR) framework, providing compatibility with future deployments once CDC and AIRA publish an IIS FHIR Implementation Guide 2.

Gainwell Assist captures the Core Data Elements for IIS Functional Standards v5.0, along with the mandatory and optional requirements defined by the CDC and AIRA joint requirements traceability matrix (RTM). This includes capturing required Facility Identifier Data Elements and Provider Data Elements as part of the primary vaccination event record.

Our Product Team includes leaders with experience in state agencies responsible for immunization registries and with strong relationships with the CDC and AIRA. Our long-standing working relationship with CMS and CDC demonstrates our ability to serve as a **trusted integrator** across public health and federal health initiatives, experience that uniquely positions us to support West Virginia's IIS modernization within a broader health ecosystem. For West Virginians, this means we are prepared to align with the CDC and AIRA and work seamlessly with national partners to confirm the IIS modernization succeeds within West Virginia's overall health ecosystem.

4.2.1.3.1.3. IIS Electronic Data Exchange Monitoring

The IIS actively monitors and evaluates data submitted via electronic data exchange through several mechanisms, as described below. These mechanisms verify that data submitted via electronic data exchange is actively monitored, validated, and managed to maintain data integrity and quality.

- **Integration Gateway Monitoring.** Gainwell's Integration Gateway and service framework monitor data file exchanges and record data inbound and outbound metrics. This includes monitoring the flow of data, applying data validation to inbound and outbound files, and retaining full files for a defined timeframe for potential reprocessing in the event of errors. CloudWatch is used to monitor the flow of data and detect errors that may trigger.
- **Automated File Processing.** File processing is fully automated and monitored. Submitting and receiving solutions must pass data validation testing before receiving approval for production status. The Integration Gateway continually applies data validation to validate data quality.
- **Data Validation and Interface Control.** Interface Control Documents (ICDs) are established for Integration Gateway users for nonstandard data exchange. Data partner agreements are captured and stored for access and retrieval. The system performs initial validations on data inbound into the system and stores copies of the inbound and outbound files for reprocessing and troubleshooting with data partners.
- **Reporting.** Gainwell Assist provides a robust, enterprise-grade reporting framework that combines standardized regulatory reports with powerful user-configurable reporting tools. Reports support on-demand execution, automated scheduling (multiple cadence options), export, and secure sharing for organizational visibility.

4.2.1.3.1.4. IIS Electronic Exchange Error Resolution

The IIS investigates electronic data exchange errors and anomalies with IIS partners and providers by using the methods described below. These methods collectively confirm that electronic data exchange errors and anomalies are promptly identified, to maintain the integrity and efficiency of data exchanges with IIS partners and providers.

Integration Gateway Monitoring. Gainwell Assist provides a comprehensive File Exchange Dashboard suite combined with an enterprise-grade Integration Gateway. Jurisdictions receive real-time visibility into submission volumes, processing status, HL7 error codes, and data quality metrics. The Integration Gateway monitors inbound and outbound exchanges, applies initial validations, stores transaction copies for reprocessing, and complies with industry

interoperability standards. Together, these capabilities provide transparent, auditable, and standards-compliant data exchange management while enabling rapid troubleshooting and proactive operational oversight.

Issue Identification and Resolution Teams. Gainwell has teams in place to promptly resolve issues. These teams include the Gainwell Support Services Module Support Team, which identifies, investigates, and diagnoses service issues. There is a centralized operations management center that manages routine operation activities and escalates issues to the appropriate subject matter experts (SMEs).

Monitoring Tools. Gainwell uses tools that specifically monitor the flow of data and identify errors.

Continuous Improvement Process/QA Team. This team supports business process automation improvements and manages product release, reporting, and monitoring with software quality proven practices. They handle capacity and performance management and support SLA/KPI performance management.

4.2.1.4 Confirm the Delivery of Immunization Services Reflects Current ACIP Recommendations

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.4.1. The IIS supports pediatric, adolescent, and adult immunization forecasts consistent with Advisory Committee on Immunization Practices (ACIP) recommendations.

4.2.1.4.1.1. The IIS establishes and maintains Clinical Decision Support (CDS) functionality consistent with ACIP recommendations.

4.2.1.4.1.2. The IIS establishes and maintains Clinical Decision Support functionality in alignment with CDSi resources published on the CDC website.

4.2.1.4.1. ACIP-Aligned Immunization Forecasting

Gainwell *Assist* fully supports pediatric, adolescent, and adult immunization forecasting consistent with Advisory Committee on Immunization Practices (ACIP) recommendations and aligns with CDC Clinical Decision Support for Immunization (CDSi) resources.

The IIS supports pediatric, adolescent, and adult immunization forecasts consistent with ACIP recommendations. Gainwell *Assist* delivers comprehensive immunization evaluation and forecasting across the lifespan, including:

- Pediatric schedules (birth through adolescence)
- Adolescent schedules
- Adult schedules, including age-based and risk-based recommendations
- Catch-up schedules
- Four-day grace period logic
- Special risk and contraindication considerations

These capabilities align with the CDC CDSi scope, which includes vaccine groups routinely recommended by ACIP for healthy individuals from birth through age 65+, as well as special-risk indications. The system evaluates immunization histories and generates:

- Evaluation status (valid, invalid, complete)
- Earliest date
- Recommended date
- Overdue indicators
- Series completion guidance

This allows providers to receive accurate, real-time decision support at the point of care.

4.2.1.4.1.1 Clinical Decision Support Based on ACIP Recommendations

The IIS establishes and maintains Clinical Decision Support (CDS) functionality consistent with ACIP recommendations. Gainwell's Clinical Decision Support engine is directly integrated with CDC ACIP schedules through CDSi logic specifications and supporting data. As ACIP recommendations evolve, Gainwell:

- Rapidly incorporates updated vaccine schedules and dosing guidance
- Updates CDS logic in alignment with CDC-published specifications
- Performs full regression testing after each CDSi release
- Validates forecasting outputs using CDC test case methodologies

The CDC CDSi framework translates ACIP clinical recommendations into technical logic using:

- Logic specifications
- Supporting data
- Test cases

Gainwell uses this framework to verify its forecasting engine consistently produces harmonized, standards-based outputs. This approach proved critical during the COVID-19 pandemic, when vaccine guidance and dosing intervals changed frequently. Our structured CDSi integration process enabled rapid and accurate schedule updates without disruption to providers.

4.2.1.4.1.2 Clinical Decision Support Aligned with CDSi Resources

The IIS establishes and maintains Clinical Decision Support functionality in alignment with CDSi resources published on the CDC website.

Gainwell Assist aligns fully with CDC CDSi resources:

- Uses CDC logic specifications
- Applies CDC supporting data (e.g., minimum age, earliest recommended age, dose intervals)
- Executes CDC test cases to validate algorithm outputs
- Conducts Assessment, Alignment, and Reporting Tool (AART) validation

Gainwell runs more than 1,400 CDSi test cases to validate compliance and accuracy. After each new CDSi release:

- A full regression suite is executed
- Forecast outputs are validated against CDC expected outcomes
- AART assessments are performed

- Results are documented to confirm continued compliance

Clinical Decision Support Validation Results

The system has achieved Complete Validation Status for Clinical Decision Support across CDC assessment measures, including:

- Evaluation Status for pediatric, adolescent, and adult groups
- Earliest Date Accuracy for pediatric, adolescent, and adult groups
- Recommended Date Accuracy for pediatric, adolescent, and adult groups
- Use of standard vaccine codes (CVX, MVX, NDC)
- Support for up-to-date (UTD) logic and forecasting workflows

This confirms:

- Full forecast accuracy for pediatric, adolescent, and adult groups
- Accurate earliest date and recommended date calculations
- Complete support for evaluation logic across age groups
- 100% compliance with CDC CDSi validation measures

Ongoing Governance and Maintenance

Gainwell maintains a formal CDS governance process that includes:

- Monitoring ACIP updates
- Reviewing CDC CDSi release notes
- Updating logic specifications
- Executing automated regression testing
- Conducting AIRA AART reassessments
- Documenting validation results

CDSi resources are designed to improve accuracy, consistency, and timeliness of immunization forecasting. Gainwell's structured integration approach supports continued alignment with national standards and consistent forecasting outputs.

Gainwell recognizes that jurisdictions, including West Virginia, may have State-specific vaccination policies, school entry requirements, or programmatic forecasting rules that differ slightly from national CDSi guidance.

Gainwell Assist includes configurable forecasting parameters that allow jurisdiction-specific business rules where permissible. These variations are managed through structured change management processes.

In Lockstep with Emerging Requirements and Standards

Gainwell Assist meets the 12 Clinical Decision Support Validation measures in the AIRA Aggregate Analysis Reporting Tool (AART) Complete Validation 2025 assessment, demonstrating alignment with national expectations for immunization decision support. Our Product Support team regularly enhances the base product to comply with CDC and AIRA updates and even hosts an IIS Advisory Council where customers share practices, learn about upcoming enhancements, and contribute feedback to the product roadmap.

4.2.1.5 Confirm Appropriate User Access to Data

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.5.1. The IIS ensures authorized users have access to patient demographic and vaccination data based on user roles and permissions.

4.2.1.5.1.1. The IIS implements confidentiality policies that protect the privacy of individuals whose data is contained in the system.

4.2.1.5.1.2. The IIS implements comprehensive account management policies consistent with industry security standards.

4.2.1.5.1.3. The IIS supports technical attributes for the set up and access of user roles and permissions.

4.2.1.5.1.4. The IIS provides user access in accordance with policies and procedures.

4.2.1.5.1.5. The IIS supports authorized IIS partners' and providers' appropriate access to data in the IIS for public and population health purposes (e.g. childcare, schools, college, health plans, clinics).

4.2.1.5.1.6. The IIS provides training that covers accessing patient demographic and vaccination data.

4.2.1.5.1.7. The IIS identifies and inactivates user and site accounts when they are no longer active or no longer authorized to access the system.

4.2.1.5.2. The IIS supports authorized public access to official immunization records.

4.2.1.5.2.1. The IIS provides consumers with direct access to immunization records in accordance with policies and procedures.

Gainwell's proposed Gainwell Assist solution enables appropriate user access to data, as described below.

4.2.1.5.1. Authorized User Access to Patient Demographics and Vaccination Data

The IIS verifies that authorized users can access patient demographic and vaccination data based on user roles and permissions through several mechanisms:

- **Role-Based Access Control.** Access to systems and data is granted according to the principle of least privilege. This role-based security model allows authorized users to update data and records change history. Users must authenticate before accessing only the data or functions for which they are authorized.
- **Single Sign-On (SSO).** The system integrates with external portals using an SSO server based on Security Assertion Markup Language (SAML) or OAuth 2.0. This integration supports role- and activity-based access and works with the identity and access management (IAM) solution to provide users the appropriate permissions.
- **Security Policies and Compliance.** Gainwell develops and maintains security policies aligned with industry standards such as ISO/IEC 27001 and NIST guidelines. These policies address control, data protection, and incident response. Compliance with regulations such as HIPAA is supported through scheduled audits and assessments.
- **Data Protection.** Data is encrypted in transit and at rest using Advanced Encryption Standards (AES-256) protections. Data masking and anonymization are applied when needed to support privacy and security.
- **Incident Response and Management.** A documented incident response plan outlines procedures for detecting, reporting, and managing security incidents. Continuous monitoring and logging of network and system activities support rapid identification of potential issues.

These measures verify that only authorized users can access sensitive patient demographic and vaccination data based on their roles and permissions.

4.2.1.5.1.1. Confidentiality Procedures

The IIS implements confidentiality policies to protect individual privacy through several measures:

- **Data Protection and Encryption.** Gainwell applies Advanced Encryption Standards (AES-256) to protect data in transit and at rest, reducing the risk of unauthorized access.
- **Access Control and Identity Management.** Access to systems and data follows the principle of least privilege, giving users only the permissions needed for their roles. Multi-Factor Authentication (MFA) adds a second layer of verification before accessing sensitive systems.
- **Data Masking and Anonymization.** Sensitive data is masked or anonymized, especially for testing and analytics, to support privacy and security across environments.
- **Incident Response and Management.** Gainwell maintains a documented incident response plan outlining procedures for detecting, reporting, and addressing security incidents. Continuous monitoring and logging of network and system activity support early identification of potential security incidents.

4.2.1.5.1.2. Comprehensive Account Management Policies

Gainwell implements account management policies consistent with industry security standards through several components that protect sensitive information and systems:

- **Policy and Governance.** Gainwell establishes and maintains security policies aligned with industry standards such as ISO/IEC 27001 and NIST guidelines. These policies address access control, data protection, and incident response. Compliance with regulations such as HIPAA is supported through regular audits and assessments.
- **Access Control and Identity Management.** Gainwell uses Role-Based Access Control (RBAC) to grant system and data access based on the principle of least privilege. Multi-Factor Authentication (MFA) adds an additional verification step before users access sensitive systems.
- **Continuous Monitoring and Reporting.** Gainwell uses monitoring tools and processes to maintain ongoing compliance. Deviations or findings are tracked and resolved through the Plan of Action and Milestones (POA&M) process, and updates are shared with stakeholders as required.
- **Governance Framework and Compliance Management.** Gainwell's governance framework aligns with industry-recognized standards, including NIST SP 800-53, HIPAA, ISO 27001, and SOC 2 Type 2. This framework guides the design, implementation, and monitoring of security, privacy, and operational controls. A dedicated compliance team oversees adherence to legal, regulatory, and contractual requirements through regular audits, assessments, and training.
- **Continuous Improvement.** Gainwell conducts ongoing risk assessments and audits to identify opportunities for improvement.

Policies and procedures are updated in response to changes in laws, regulations, or industry standards. Automation and advanced monitoring technologies support efficient and accurate compliance activities.

4.2.1.5.1.3. Technical Attributes

The IIS supports technical attributes for configuring and accessing user roles and permissions through several mechanisms, outlined below. These mechanisms provide secure and controlled access that aligns with compliance and security standards.

- **Role-Based Access Control (RBAC).** Access to systems and data is granted according to the principle of least privilege, giving users only the permissions needed for their roles.

This approach restricts access to assets, systems, software, and applications a user supports. Granular authorizations govern viewing, editing, and sharing. Access is granted only when a documented business justification is provided.
- **Single Sign-On (SSO) Integration.** Gainwell Assist integrates with external portals using an SSO server based on Security Assertion Markup Language (SAML) or OAuth 2.0. This integration supports role-and activity-based access and connects with the identify and access management (IAM) solution to assign appropriate rights.
- **Identity Management.** Gainwell Assist uses centralized web services for identity, credential, and access management. The system creates and shares a file of user types and rights available in the application. SSO establishes a security profile for each user, defining which applications and functions they may access. A structured approval process governs the granting of access privileges, which are reviewed regularly to maintain proper confidentiality and access availability.
- **Security and Compliance.** Gainwell maintains security policies aligned with industry standards such as ISO/IEC 27001 and NIST guidelines. These policies address areas including access control, data protection, and incident response. Compliance with HIPAA is supported by scheduled audits and assessments.
- **Technical Controls for Data Security.** The module protects data through identity-management controls, access enforcement mechanisms, threat and vulnerability management, and data security processes. Access is based on role and activity to control exposure to member data, and select users receive least-privileged administrative access to further limit permissions.

4.2.1.5.1.4. User Access

The IIS provides user access in accordance with policies and procedures. The system integrates with external portals using SSO based on Security Assertion Markup Language (SAML) or OAuth 2.0, supporting role-based and activity-based permissions. It also integrates with the identity and access management (IAM) solution to confirm users receive the appropriate level of access. Gainwell maintains security policies aligned with industry standards, such as ISO/IEC 27001 and NIST guidelines, which address access control among other key areas of information security. The IIS further supports data security through role-based access controls and administrative safeguards, including policies and training, that limit use and disclosure of confidential information to what is necessary for job responsibilities.

4.2.1.5.1.5. Authorized IIS Access

The IIS supports authorized partners' and providers' access to data for public-health and population-health purposes.

Gainwell *Assist* accommodates clinical and utilization data for members enrolled in managed-care benefit plans, providing a resource for population-health management across the served population.

Authorized users can access claims-based information, which offers a comprehensive view of a member's history, including encounters and claims stored in the system. Gainwell *Assist* also supports role-based access to data and integrates with SSO-enabled applications to verify that users have the appropriate access.

4.2.1.5.1.6. IIS Training

Gainwell's comprehensive role-based Training Plan covers access to patient demographic and vaccination data. By offering multiple training formats (online, guided seminars, and recorded sessions) and providing clear, plain-language user manuals, we help users feel confident and prepared.

A successful implementation depends on user readiness, and our methodology prepares users, systems, and processes for a smooth go-live.

- **Role-Based Training Program.** We develop and deliver a comprehensive training program tailored to the needs of each user group. Using guided online seminars, recorded sessions, and detailed user manuals, we help users become confident and capable with the new IIS.
- **Operational Readiness Review (ORR).** Before go-live, we conduct a full ORR to validate that technical, operational, and organizational components are ready. This includes reviewing system performance, support-staff readiness, and workflow validation. A final ORR report provides a clear go/no-go recommendation to support a successful launch.

4.2.1.5.1.7 IIS User and Site Account Inactivation

The IIS identifies and inactivates user and site accounts using role-based access control (RBAC) and related security measures. Access to systems and data is granted according to the principle of least privilege, giving users only the permissions required for their roles. This model restricts access to the assets, systems, software, and applications that users directly support and limits access to administrative tools through RBAC.

Gainwell's role-based security framework requires authentication before entities can transmit or request information. Authorized users may update data, and changes are logged to maintain accountability.

Regular risk assessments and security audits support compliance with privacy and security standards. Technical controls for identity management, access enforcement, threat and vulnerability management, and data security processes contribute to identifying and disabling accounts that are inactive or no longer authorized.

4.2.1.5.2. IIS Support of Authorized Public Access to Immunization Records

Gainwell provides comprehensive maintenance, operations, and enhancement services for IIS in the cloud through the Gainwell *Assist* platform, a cloud-based Software as a Services (SaaS) solution that aligns with CDC Functional Standards and AIRA guidance.

The platform is deployed across multiple states and supports large-scale modernization by transitioning extensive immunization-record datasets from legacy IIS environments. For example, in one state, we migrated 72.7 million records without disrupting providers operations during go-live, and in another state, we are migrating 195.3 million records while preserving data integrity and seamless continuity with HIE systems.

4.2.1.5.2.1 Direct Access to Immunization Records

Gainwell Assist is designed for intuitive use. A responsive interface supports rural bandwidth limitations, and dashboards give providers, schools, and public health staff clear, easy-to-use tools for decision-making. The system gives individuals convenient and secure access to their immunization records, strengthening user empowerment and supporting public trust.

4.2.1.6. Support the Generation and Use of IIS Data Through Various Channels and Formats

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.6.1. The IIS supports the reporting needs of federal and jurisdictional immunization programs.

4.2.1.6.1.1. The IIS provides standard and ad-hoc reports to meet federal and jurisdictional reporting requirements.

4.2.1.6.2. The IIS supports ad-hoc queries of patient demographic and vaccination data.

4.2.1.6.2.1. The IIS supports direct access for internal authorized users to IIS databases for data extracts and queries in accordance with policies and procedures.

4.2.1.6.2.2. The IIS supports access to data for data visualization, presentation, and analysis.

4.2.1.6.3. The IIS supports investigation and reporting of vaccine adverse events.

4.2.1.6.3.1. The IIS supports vaccine adverse event investigation.

4.2.1.6.3.2. The IIS refers users to appropriate resources to support adverse event documentation.

4.2.1.6.4. The IIS supports the ability to generate coverage reports that users can access without assistance from IIS staff.

4.2.1.6.4.1. The IIS provides access to data to assess vaccination coverage and identify vulnerable populations.

4.2.1.6.4.2. The IIS manages patient status at provider site and jurisdiction levels.

4.2.1.6.4.3. The IIS provides HS-related training on accessing, generating, and interpreting reports.

4.2.1.6.4.4. The IIS supports compliance with immunization requirements in childcare, school, and college settings.

4.2.1.6.5. The IIS supports reminder/ recall activities.

4.2.1.6.5.1. The IIS supports conducting reminder/recall activities without assistance from IIS staff.

Gainwell's proposed system supports the generation and use of IIS data through various channels and formats. Following are our responses to the Functional Standards listed in the RFP.

4.2.1.6.1. Support Reporting of Federal and Jurisdictional Immunization Programs

Gainwell Assist supports federal and jurisdictional immunization-program reporting through a comprehensive and flexible reporting framework. Reports can be generated on-demand, scheduled for automated delivery, published in a secure role-based reporting portal, or transmitted externally through secure transport mechanisms such as the Immunization (IZ) Gateway or Secure File Transfer Protocol (SFTP), based on the State's preferred workflows and federal reporting needs.

The solution supports recurring operational, compliance, inventory, and surveillance reporting across daily, weekly, monthly, quarterly, and annual schedules. Examples include:

- Monthly CDC reporting (e.g., influenza, COVID-19, and other required submissions)
- Annual Immunization Information System Annual Report (IISAR)
- Quarterly CDC IIS-NIS reporting
- Monthly leadership statistics and performance metrics
- Operational monitoring reports (e.g., organizations with no recent data exchange activity)
- Daily disease-specific counts and demographic summaries (e.g., COVID-19, Mpox)
- Daily job-status and data exchange monitoring reports
- Weekly inventory accountability reports
- Weekly vaccine-administration report files

Reports may be delivered through:

- Secure in-system, permission-based access
- Automated report generation and publication
- Secure file transfer via SFTP
- Transmission through the IZ Gateway, when required for federal workflows

This flexible, multichannel reporting model helps jurisdictions meet federal requirements, program oversight needs, executive reporting expectations, and public-health surveillance objectives in a timely, secure, and auditable manner.

4.2.1.6.1.1. Standard and Ad Hoc Reporting

The IIS provides standard and ad hoc reports to meet federal and jurisdictional reporting requirements. Gainwell's IIS solution includes a comprehensive suite of configurable standard reports designed to support clinical operations, public health oversight, regulatory compliance, inventory management, data quality monitoring, and program performance evaluation. These reports offer structured, statewide visibility into immunization activity, patient status, provider performance, vaccine usage, inventory accountability, adverse-event tracking, and data exchange health.

Standard reports include multi-facility aggregation, statewide roll-up, time-period comparisons, and export functions. Reports are role-based, configurable by date range and organizational scope, and designed to support both operational users and executive stakeholders. Taken together, this framework allows jurisdictions to monitor immunization coverage, maintain compliance with federal and state requirements, manage vaccine inventory and funding programs, evaluate data quality, and support informed public-health decision-making.

4.2.1.6.2 Ad Hoc Queries

The IIS supports ad hoc queries of patient demographic and vaccination data. Gainwell *Assist* includes a **Custom Report Module** that allows authorized users to perform these queries without technical assistance. Users can build custom reports by selecting filters across multiple data domains, including:

- **Patient Demographics.** Status, priority group, birth date range, county, city, ZIP code, area, and other demographic attributes
- **Facility Filters.** Facility name, PIN code, district, and multi-facility selections
- **Immunization Data.** Vaccine group, lot number, trade name, mass-vaccination event, and other vaccination-specific attributes

Reports can be generated in two formats:

- **List View.** Detailed record-level results
- **Count View.** Aggregate counts and summarized data

This flexibility supports both operational and high-level reporting needs. The system allows users to:

- Create and save report templates
- Schedule reports for automated execution (single or recurring cadence: daily, weekly, or monthly)
- Define start and end dates
- Manage report visibility
- Archive or delete templates

Reports can be sorted, filtered, and configured to meet jurisdiction-specific needs. This self-service reporting capability enables users to generate targeted, real-time insights on patient populations, vaccination coverage, compliance monitoring, and program performance.

Together, these features confirm the IIS fully supports ad hoc querying and flexible analysis of demographic and immunization data in alignment with Functional Standards.

4.2.1.6.2.1 Direct Database Access for Authorized Users

Gainwell supports controlled, direct database access for authorized internal users in accordance with jurisdictional policies, security standards, and data governance procedures. Authorized users receive secure, read-only access to the IIS reporting-database environment through an approved database-query interface.

4.2.1.6.2.2. Data Access for Visualization and Analysis

The IIS supports access to data for visualization, presentation, and analysis. Gainwell Assist provides several mechanisms to support these needs for authorized users.

Within the IIS, users have access to interactive dashboards and configurable reports that present immunization, inventory, demographic, and data exchange metrics in visual and structured formats. These dashboards and reports support real-time monitoring, analysis, and operational oversight through sortable tables, aggregated counts, and time-based comparisons.

For expanded analytical needs, the system provides:

- Export of report data in standard formats for use in external visualization tools
- Secure, role-based access to reporting datasets for advanced querying
- Scheduled report generation for recurring analytical reviews
- Aggregation of multi-facility and statewide data

Authorized internal users may also receive controlled, read-only access to the reporting-database environment, supported by a detailed data dictionary and schema documentation. This access allows jurisdictions to integrate IIS data into enterprise analytics platforms, business-intelligence tools, and visualization solutions in alignment with governance and security policies.

Through these combined capabilities, including interactive dashboards, configurable reporting, export functionality, and secure analytical access, the IIS supports comprehensive data visualization, presentation, and analysis. These features help jurisdictions meet federal, jurisdictional, and executive reporting needs with actionable information.

4.2.1.6.3. Support Investigation and Reporting of Vaccine Adverse Effects

Gainwell *Assist* supports comprehensive documentation, investigation, and reporting of vaccine adverse events at the individual-immunization level.

Users record adverse reactions directly within the associated immunization record through a structured **Immunization Reaction module**. Users can:

- Select standardized reaction terms. These may include vaccine-specific adverse-reaction classifications.
- Document reaction dates.
- Flag events for review.
- Record whether the event was reported to the Vaccine Adverse Event Reporting System (VAERS).
- Capture the date reported to VAERS.
- Identify the reporting facility.

This structured documentation supports traceability, clinical review, audit readiness, and public-health investigation activities. To support federal reporting requirements, the system provides a direct link to the **VAERS submission portal** so providers can quickly submit adverse-event details. The IIS also includes standard reports to support monitoring and oversight, including:

- **VAERS Report.** Generates a list of patients with documented adverse events that have been reported to VAERS.
- **Not Reported to VAERS Report.** Identifies documented adverse events that have not yet been reported, supporting follow-up and compliance monitoring.

These reporting capabilities help jurisdictions monitor adverse-event documentation, support timely federal reporting, and enable investigation workflows. Together, these features provide a structured, auditable, standards-aligned approach to adverse-event documentation and reporting that supports CDC guidance, VAERS requirements, and jurisdictional quality assurance processes.

4.2.1.6.3.1 Vaccine Adverse Event Investigation

Gainwell *Assist* supports structured documentation, investigation, and oversight of vaccine adverse events at the individual immunization level. Users record adverse reactions using standardized reaction classifications. Fields capture reaction dates, reporting status to VAERS, reporting dates, and the reporting facility. Users may also flag events for review to support clinical and public-health investigation.

The system provides a direct link to the VAERS submission portal to facilitate federal reporting and includes monitoring reports that track events already reported and those pending submission. This structured, auditable approach supports traceability, timely reporting, and effective investigation workflows in alignment with CDC and VAERS requirements.

4.2.1.6.3.2 Resources for Adverse Event Documentation

Gainwell Assist provides structured tools and configurable resources to support accurate, consistent, and compliant documentation of vaccine adverse events. The system includes standardized reaction terminology within the Immunization Reaction module, allowing events to be recorded using clinically appropriate classifications. Key data elements such as reaction date, VAERS reporting status, reporting date, and reporting facility are captured directly within the immunization record to support completeness, traceability, and audit readiness.

To support federal compliance, the IIS includes a direct link to the VAERS submission portal and provides monitoring reports to track documented events and their reporting status.

Gainwell Assist also includes a configurable **Support and Related Links** area where jurisdictions can publish resources relevant to their adverse-event investigation processes, such as State guidance documents, reporting workflows, or CDC reference materials. The IIS includes a **document-repository capability**, allowing jurisdictions, when required, to upload and store completed VAERS forms or supporting documentation within the system for authorized viewing. This approach keeps documentation centralized, accessible to permitted users, and retained according to jurisdictional policies.

Together, these configurable tools and resources support standardized and transparent adverse-event documentation and reporting, helping jurisdictions meet CDC guidance, VAERS requirements, and local process needs.

4.2.1.6.4. Self-Service Coverage Reporting

The IIS supports the generation of coverage reports that users can access without assistance from IIS staff. Gainwell Assist enables authorized users to independently create immunization coverage reports through both standard coverage reports and a configurable custom-reporting module. Users can define age cohorts, vaccine groups, date ranges, geographic areas, and facility-level filters to calculate and analyze coverage rates.

Users may generate reports in detailed list format or aggregated count format to support both patient-level review and population-level analysis. Coverage reports can be filtered by demographic attributes such as county, ZIP code, age range, provider or facility, funding source, vaccine group, and up-to-date status.

To promote user independence, the system includes integrated on-page guidance and contextual help that explain available filters, report parameters, and expected outputs. This embedded support reduces reliance on technical staff and improves report accuracy and usability.

The IIS enforces robust **role-based access control (RBAC)**. Jurisdictional administrators define which reports are available to each user role and control the scope of accessible data. For example:

- Statewide or multi-facility coverage reports can be restricted to public-health leadership or designated analysts.
- Facility-level users may be limited to generating reports only for their organization or assigned geographic area.

- Access to sensitive demographic or aggregated statewide data can be restricted in accordance with jurisdictional policy.

Reports may be executed on demand or scheduled for recurring automated generation on daily, weekly, or monthly intervals. Saved templates allow users to quickly reproduce commonly used analyses, and outputs can be securely exported for presentation or further analysis.

These capabilities confirm coverage reporting is self-service, secure, policy driven, and appropriately scoped to each user's role, supporting informed public health decision-making while maintaining strict data governance controls.

4.2.1.6.4.1 Data Access for Vaccination Coverage and Population Vulnerability Assessment

Gainwell Assist includes an integrated **Immunization Quality Improvement Program (IQIP) reporting module** that helps jurisdictions assess vaccination coverage, evaluate performance against national standards, and identify vulnerable or under-immunized populations.

The system provides baseline IQIP assessment standards aligned with CDC guidance and allows authorized users to adjust age ranges, vaccine groups, dose counts, and up-to-date criteria to meet jurisdictional reporting needs. This flexibility supports customized coverage analyses within a single reporting workflow and eliminates the need to generate multiple separate outputs.

Users can generate multiple report formats, including:

- Assessment summaries
- Patient listings for targeted outreach
- Provider report cards
- Up-to-date with one visit analysis
- Multi-year trend reports

To support geographic and population-level analysis, the IIS includes **interactive coverage maps** that display vaccination rates by county or statewide region. Color-coded thresholds help users quickly identify areas with lower coverage. By integrating configurable IQIP reporting, demographic filtering, multi-year trend analysis, and geographic coverage mapping, the IIS provides jurisdictions with actionable data to:

- Monitor vaccination coverage rates
- Identify gaps and inequities
- Target outreach and quality improvement efforts
- Support data-driven public health interventions

These capabilities allow jurisdictions to independently evaluate immunization coverage and proactively identify populations or regions at risk.

4.2.1.6.4.2 Managing Patient Status

Gainwell's IIS solution supports comprehensive patient status management at both the provider site and jurisdiction levels. The system enables a **one-to-many status affiliation model**, allowing a patient to have status designations associated with multiple facilities while maintaining a single jurisdiction-level record. Authorized users may assign and manage standardized patient status values, including:

- Active
- Inactive, Unspecified
- Inactive, Lost to follow-up (cannot contact)
- Inactive, Moved or gone elsewhere (transferred)
- Inactive, Permanently inactive (do not re-activate or add new entries to this record)
- Unknown

This flexible framework enables provider sites to manage their active panels while allowing the jurisdiction to maintain broader population oversight and record continuity.

The system also supports **bulk patient status updates**, enabling jurisdictions or authorized provider administrators to efficiently update large patient cohorts based on defined criteria such as absence of recent immunizations, transferred patients, or inactive panels. Bulk-update tools promote operational efficiency and maintain audit logging and role-based controls. Patient status values can also be used in reporting and filtering to:

- Generate lists of inactive or lost-to-follow-up patients
- Identify patients who require outreach
- Exclude permanently inactive records from coverage calculations
- Support panel management and quality improvement activities

Through multi-level status management, a configurable affiliation model, and bulk-update capabilities, the IIS supports accurate patient tracking across facilities while supporting both provider-level operations and jurisdiction-wide public health oversight.

4.2.1.6.4.3 IIS-Related Training

Gainwell provides comprehensive training and user support to help authorized users confidently access, generate, and interpret IIS reports. The system includes a detailed user manual with step-by-step instructions that guide users through the report creation process. These materials explain how to configure filters, select appropriate parameters, and interpret the data elements required for accurate outputs. High-level training sessions demonstrate reporting workflows, outline proven practices, and explain how report selections affect results and coverage calculations.

In addition to formal training materials, the IIS includes integrated on-page help and contextual guidance. These embedded tools offer real-time explanations of report fields, filter options, and output types based on user selections. This guidance supports correct usage and reduces reliance on technical staff.

4.2.1.6.4.4 Compliance with Immunization Requirements

Gainwell Assist includes a fully integrated **School and Childcare Compliance Module** designed to support jurisdiction-specific immunization requirements for K–12 schools, childcare facilities, and higher education institutions. Gainwell collaborates with each jurisdiction to configure the module in accordance with State immunization laws, exemption policies, reporting timelines, and compliance thresholds. The system supports both submission and query, allowing schools and authorized users to securely upload and review student immunization data. Key capabilities include:

- Creation and maintenance of school roster lists
- Grade-level tracking, including K-12 and homeschool
- Total enrollment tracking by grade
- Configurable exemption categories such as medical, religious, provisional
- Automated compliance calculations based on State-defined rules

Standard compliance outputs include:

- **Student List.** Listing of enrolled students
- **Student Immunization History List.** Students with associated immunization records
- **Immunizations Due Report.** Students missing required vaccines
- **Exclusion Letter Generation.** Automated notices for students overdue for vaccine requirements, according to jurisdiction policy

The system supports school and childcare audit reporting that displays:

- Total enrollment counts
- Students with certificates of immunization
- Provisional certificates
- Medical and religious exemptions
- Students without acceptable certificates
- Grade-specific compliance summaries

These reports provide clear visibility into adherence rates and quickly help jurisdictions identify compliance gaps. Through configurable business rules, automated reporting, roster-based tracking, and exclusion workflows, the IIS enables jurisdictions to monitor and enforce school and childcare immunization requirements while supporting streamlined reporting for educational institutions.

4.2.1.6.5. Reminder/Recall Activities

Gainwell *Assist* includes a comprehensive **Reminder/Recall module** that enables jurisdictions and authorized provider sites to proactively identify and notify patients that are due or overdue for immunizations. The system supports both **vaccine-based reminder/recall and vaccine lot recall workflows**. Authorized users can generate targeted reminder reports using configurable criteria, including:

- Immunization due status (due, overdue, upcoming)
- Specific vaccine groups needed
- Vaccine groups to display on the report
- Lot number for recall events
- Vaccination date ranges
- Administering facility or clinician
- Inclusion or exclusion of inactive patients

- Exclusion of patients previously contacted within a defined time frame

Users can apply detailed **facility and patient filters**, such as:

- Facility name or district
- Age ranges and birth date ranges
- County, city, ZIP code, and State
- Race, ethnicity, and gender

Reminder and recall outputs may include:

- Patient letters for outreach
- Patient listings for follow-up activities
- Aggregate reports for authorized designees
- Targeted lot recall reports when applicable

These capabilities help jurisdictions and providers conduct efficient outreach campaigns, support quality improvement initiatives, address coverage gaps, and respond to vaccine recalls. Configurable filters and Role-Based Access Controls (RBAC) confirm reminder and recall activities are scoped to each user's authorized population.

4.2.1.6.5.1 Reminder/Recall Activities without Assistance

Gainwell Assist enables authorized users to conduct reminder and recall activities independently, without assistance from IIS staff. The self-service Reminder and Recall module allows users to define outreach criteria, generate reports, and initiate follow-up workflows directly within the IIS. Output options include patient letters, patient listings, and aggregate reports for designated staff. For vaccine safety events, lot-based recall reporting is also available.

Reminder and recall functions are available through a role-based, permission-controlled interface. Integrated on-page guidance and reporting filters help users understand selection criteria and expected outputs, supporting independent execution of outreach campaigns.

These self-service capabilities confirm that providers and jurisdictional staff can efficiently conduct targeted reminder and recall efforts to improve vaccination coverage and address gaps without relying on technical or administrative IIS support.

4.2.1.7. Support Federal and Jurisdictional Vaccine Program Requirements

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.7.1. The IIS supports management and quality assurance functions for federal and jurisdictional vaccine programs.

4.2.1.7.1.1. The IIS establishes vaccine program procedures in accordance with federal and jurisdictional policies.

4.2.1.7.1.2. The IIS supports the tracking of eligibility at the dose level for publicly purchased vaccines.

4.2.1.7.1.3. The IIS generates a report listing patients that received a non-viable vaccine.

4.2.1.7.1.4. The IIS generates a report listing provider sites that received vaccine lots recalled by the manufacturer.

4.2.1.7.2. The IIS supports vaccine inventory management and reconciliation according to federal and jurisdictional vaccine program requirements.

4.2.1.7.2.1. The IIS supports vaccine inventory management, tracking, and reconciliation at the IIS jurisdiction and provider site levels.

4.2.1.7.2.2. The IIS supports creating vaccine orders and monitoring order status.

4.2.1.7.2.3. The IIS supports reporting vaccine returns and wastage.

4.2.1.7.2.4. The IIS automatically decrements administered doses (not historical doses) from active inventory.

4.2.1.7.3. The IIS supports data exchange with the national Vaccine Tracking System (VTrckS).

4.2.1.7.3.1. The IIS establishes data exchange with VTrckS in accordance with ExIS (External Information System) specifications <https://www.cdc.gov/vtrcks/php/about/exis-functionality.html#cdc-generic-section-1-exis-functionality>.

4.2.1.7.3.2. The IIS completes updates to ExIS functionality following publication of specifications.

4.2.1.7.3.3. The IIS establishes automated data exchange with VTrckS.

Gainwell's proposed system supports federal and jurisdictional vaccine program requirements, as described below in our responses to the Functional Standards.

4.2.1.7.1. Support Management and Quality Assurance Functions

Gainwell *Assist* uses tools such as the Aggregate Analysis Reporting Tool (AART), CDC implementation guides, and staff participation in workgroups including the Measurement for Assessment and Certification Advisory Workgroup (MACAW) and Immunization Gateway (IZ Gateway) program to advance Health Level Seven (HL7) standardization.

These activities position Gainwell as a strong partner to the IZ Gateway, the CDC, and the State. Our team understands the IZ Gateway roadmap and the opportunities it creates for federal reporting and cross-jurisdictional data sharing.

Our solution is designed for high-volume processing. Gainwell *Assist* supports up to 2.5 million HL7 messages per day, including approximately 500,000 Vaccination Update (VXU) messages, and two million Query by Parameter (QBP) messages, without performance degradation. Built-in scalability allows the system to expand quickly to meet increasing demand for larger transaction volumes, more HL7 throughput, and additional users. Gainwell will collaborate with the State to test and transition the anticipated 1,000 HL7 connections to the modernized Gainwell *Assist* Solution.

4.2.1.7.1.1. Vaccine Program Procedures

Gainwell will provide system support for the following:

- **Near- and Real-Time Data Exchange.** The IIS exchanges data with external systems using the preferred transport method and the CDC WSDL.
- **Compliance with CDC HL7 Guidance.** The system follows the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, using SOAP-based transport by using the standard CDC WSDL and IZ Gateway.
- **Robust Reporting and Analytics.** The IIS provides tools to identify, analyze, and export data submission errors.
- **Patient Demographic Capture.** The IIS captures demographic information in alignment with the Core Data Elements for IIS Functional Standards Version 5.0 and the mandatory and optional requirements of the joint CDC and AIRA Reference Test Message (RTM).

- **Audit Logging.** The IIS maintains a log of system data changes, including date, time, and the user or site responsible when individual-level immunization data is created, viewed, or modified.

Gainwell will determine the best approach and protocol as we develop and document interface specifications with each external source system.

4.2.1.7.1.2. Tracking of Eligibility

Gainwell Assist includes the following system components to support eligibility tracking:

- **Vaccine Inventory Management and Accountability.** The system integrates with the CDC Vaccine Tracking System (VTrckS) to order, track, and manage doses for Vaccines for Children (VFC) and non-VFC populations. The module supports dose management, distribution, and required State and federal accountability reporting.
- **Immunization Forecasting.** Gainwell Assist provides clinical decision support to show clinicians upcoming and recommended immunizations based on CDC Advisory Committee on Immunization Practices (ACIP) guidance.

4.2.1.7.1.3. Report Listing Patients

Gainwell confirms the IIS generates a report listing patients who received a non-viable vaccine.

4.2.1.7.1.4. Report Listing Provider Sites

Gainwell Assist provides functionality to deliver reminder and recall notices at the provider, State, county, regional, and territory levels. The system supports clear, efficient communication between jurisdictions, providers, and patients. Gainwell Assist generates patient-specific reminder and recall notifications, helps providers identify age-group cohorts for targeted outreach creates patient lists and schedule calendars for reminder and recall activities, and generates vaccine-recall notices by administering provider.

Jurisdictions can use these capabilities to target populations and improve immunization rates. The system can support reminders for single vaccine or multiple vaccines, and the resulting lists provide leadership with actionable data to guide public-health interventions.

4.2.1.7.2. Support Vaccine Inventory Management and Reconciliation

Gainwell Assist is modular and highly configurable, enabling jurisdictions to customize and scale the system to meet functional and budgetary needs. The solution includes Vaccine Inventory Management and Accountability and integrates with the CDC Vaccine Tracking System (VTrckS) to order and manage doses for the Vaccines for Children (VFC) and other funding streams. The system supports dose management, distribution, and the accountability reporting required at State and federal levels. Reporting capabilities also include inventory auditing to support accountability for the distribution and use of publicly purchased vaccine supplies.

4.2.1.7.2.1. Vaccine Inventory Management, Tracking, and Reconciliation

Gainwell Assist provides data exchange with the national VTrckS through an External Information System (ExIS) interface. Vaccine Inventory Management and Accountability is a core functional area of the solution and is tightly integrated with VTrckS to order and manage doses for the VFC population. Gainwell Assist will also adapt to new VTrckS specifications as they are released.

4.2.1.7.2.2. Creating Orders and Monitoring Status

Gainwell Assist supports a variety of data exchange protocols including data exchange with the national VTrckS via an ExIS interface to retrieve Provider Master Data, inventory data, order date, and vaccine return and wastage data. Vaccine Inventory Management and Accountability is a core functional area of the solution and is tightly integrated with VTrckS to order and manage doses for the VFC population.

4.2.1.7.2.3. Reporting Vaccine Returns and Wastage

Gainwell confirms the IIS supports reporting vaccine returns and wastage. In addition, Gainwell affirms the IIS automatically decrements administered doses (not historical doses) from active inventory.

4.2.1.7.3. Support Data Exchange with National Vaccine Tracking System (VTrckS)

Gainwell follows a structured integration planning approach that includes defining specifications for each solution interface in the form of Interface Control Documents (ICDs). We carefully assess integration needs for each external system and identify the best and most efficient interface protocol. Gainwell Assist supports a variety of data exchange protocols including data exchange with VTrckS through an ExIS interface to retrieve Provider Master Data, inventory data, order date, and vaccine return and wastage data.

Vaccine Inventory Management and Accountability is a core functional area of the solution and is tightly integrated with VTrckS to order and manage doses for the VFC population.

4.2.1.7.3.1. Data Exchange with VTrckS

Gainwell Assist supports a variety of data exchange protocols including data exchange with VTrckS through an ExIS interface to retrieve Provider Master Data, inventory data, order date, and vaccine return and wastage data.

4.2.1.7.3.2. Updates to ExIS

Gainwell confirms the IIS completes updates to ExIS functionality following the publication of specifications.

4.2.1.7.3.3. Automated Data Exchange

Gainwell Assist supports a variety of data exchange protocols including data exchange with VTrckS through an ExIS interface to retrieve Provider Master Data, inventory data, order date, and vaccine return and wastage data.

4.2.1.8. Support the Response Efforts for Vaccine-Preventable Disease Outbreaks and Other Public Health Emergencies

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.8.1. The IIS supports partner and provider onboarding and vaccine management during vaccine-preventable disease response and/or public health emergencies.

4.2.1.8.1.1. The IIS establishes, coordinates, and executes emergency preparedness plans and procedures in accordance with federal and jurisdictional policies.

4.2.1.8.1.2. The IIS supports expedited communication and onboarding with partners to capture patient demographic and vaccination data in an emergency.

4.2.1.8.1.3. The IIS provides training to onboarded partners.

4.2.1.8.1.4. The IIS supports vaccine administration functionality to include offline documentation of vaccine administration.

4.2.1.8.1.5. The IIS supports integration with tools for vaccination appointment scheduling.

4.2.1.8.1.6. The IIS supports public health immunization reporting to federal and jurisdictional authorities.

The IIS supports the response efforts for vaccine-preventable disease outbreaks and other Functional Standards.

4.2.1.8.1. Support Partner and Provider Onboarding and Vaccine Management

Gainwell affirms the IIS supports partner and provider onboarding and vaccine management during vaccine-preventable disease response and/or public health emergencies.

4.2.1.8.1.1. Emergency Preparedness Plans and Procedures

Gainwell establishes, coordinates, and executes emergency preparedness plans and procedures in accordance with federal and jurisdictional policies. Gainwell Assist is cloud-based and uses multiple regions within the Amazon Web Services (AWS) infrastructure. It can mitigate service disruption or degradation proactively by shifting application processing to one region while another is being updated. In this way, the cloud infrastructure minimizes the need for solution downtime.

When production outages are necessary, we will obtain the State's approval beforehand and provide notice at least five working days before the scheduled outage. Issues requiring correction in a shorter period will require mutual agreement between the State and Gainwell. We will report urgent or emergency system outages through the RFP-specified escalation procedures.

4.2.1.8.1.2. Expedited Communication and Onboarding

On the infrastructure side, Gainwell Assist is deployed in a **multiregional AWS cloud environment** with disaster recovery that exceeds standard requirements. This maintains continuity of service even in the rare event of a regional outage. Security and compliance are foundational and we are compliant with **NIST 800-53 Rev. 5, SOC 2 Type 2, and HIPAA standards.**

4.2.1.8.1.3. Training to Onboarded Partners

Gainwell provides training to onboarded partners. Our staff train State personnel on system-configuration management so they can assist with, and if desired eventually take ownership of, configuration activities. Gainwell staff also receive internal training to support effective knowledge transfer and promote long-term self-sufficiency within the State team.

Our methodology emphasizes configuration over customization, accelerating implementation while reducing long-term risk. For the State, this means new business rules and CDC requirements can be implemented through settings, not code changes. Our data migration discipline combines automation and manual stewarding, so IIS data is accurate and trusted on day one. Our integration discipline supports standards-based HL7 and FHIR connectivity with providers and the CDC. Our user adoption discipline emphasizes role-based training, multilingual support, and a user-centered design.

A key differentiator is that our approach delivers more upfront, without relying on costly change orders. Unlike vendors that charge for each CDC or ACIP update, our roadmap is already aligned with federal requirements, and quarterly compliance releases are included at no additional cost. This keeps the State compliant without unexpected expense or rework.

Compliance Continuity with no Surprises

Gainwell Assist delivers configuration-driven updates, eliminating reliance on costly change orders. Quarterly releases already incorporate CDC and ACIP requirements, keeping the State compliant without added expense or operational disruption.

4.2.1.8.1.4. Vaccine Administration Functionality

The IIS supports vaccine administration functionality, including offline documentation capabilities. It provides mass vaccination functionality that enables the creation of both public and private vaccination events, along with reporting capabilities on vaccines administered.

To streamline data entry, the system supports 2D barcode scanning for both vaccines and patient identification, enabling efficient and accurate capture of administration details. In offline scenarios, Gainwell Assist offers a downloadable Excel-based data capture tool that allows users to document vaccine administrations without system connectivity. Once connectivity is restored, the data can be easily uploaded to populate administration records within the IIS.

4.2.1.8.1.5. Tool Integration

The IIS supports integration with tools for vaccination appointment scheduling, including requiring jurisdiction-defined patient demographic information online or offline during a mass vaccination clinic and supporting digital scanning of vaccine information.

4.2.1.8.1.6. Public Health Reporting

Gainwell has direct, hands-on experience implementing and maintaining systems that conform to CDC MMGs for immunizations (HL7 2.5.1, VXU, QBP) and other public health reporting. Data exchanged with the CDC and other partners is structured correctly, facilitating accurate national reporting and surveillance. Gainwell Assist complies fully with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5. It uses SOAP-based transport with the standard CDC and IZ Gateway WSDL and supports flat-file import and vital records file submission.

This compliance continues as part of our product roadmap: We deliver quarterly compliance releases aligned with the CDC's roadmap, keeping the State current without extra cost or change orders, a distinct advantage of Gainwell Assist.

4.2.1.9. Participate in and Prioritize Emerging Technologies and Standards

The vendor should describe how their proposed system achieves the following Functional Standards:

4.2.1.9.1. The HS participates in modernization initiatives and emerging technologies.

4.2.1.9.1.1. The IIS coordinates modernization efforts.

4.2.1.9.1.2. The HS plans and executes efforts that align HS initiatives with modernization priorities.

4.2.1.9.1.3. The IIS participates in initiatives to develop standards and/or capabilities.

Gainwell participates in and prioritizes emerging technologies and standards. We describe below how our proposed system achieves the Functional Standards.

4.2.1.9.1. Participate in Modernization Initiatives and Emerging Technologies

The Health System (HS) participates in modernization initiatives and emerging technologies. Gainwell Assist is aligned with CMS modernization initiatives and supports emerging technologies and industry standards, including Fast Healthcare Interoperability Resources (FHIR) and enhanced security requirements. Gainwell continually evaluates emerging technologies to enhance Gainwell Assist via a dedicated technology council, led by the Chief Technology Officer and subject matter experts (SMEs). This council identifies and recommends advancements and has pursued innovation in Artificial Intelligence (AI)-driven solutions, commercial-off-the-shelf (COTS) tools, process improvements, and infrastructure modernization.

4.2.1.9.1.1. Modernization Efforts

Gainwell coordinates modernization efforts and meets clients at their current stage in the modernization timeline, providing either limited or full-scale support based on each client's initiatives. We integrate technologies across diverse environments and bridge the gap between legacy and modern operations through reengineered business processes. Our team delivers these transformations by managing the detailed work required to move programs forward efficiently and reliably.

4.2.1.9.1.2. Plans and Executes Efforts Aligned to HS Initiatives and Modernization Priorities

Gainwell is a strong proponent of the CDC's Data Modernization Initiative. Our architectural principles promote interoperability through standards-based application programming interfaces (APIs) such as FHIR, strengthening data linkage across systems, and support a resilient, adaptable public health infrastructure. Gainwell Assist helps agencies move from siloed systems to an integrated, response-ready ecosystem designed to modernize data exchange and improve statewide coordination.

Our methodology is proven in practice. It is the same disciplined approach we are using in multiple states to implement the Gainwell Assist Immunization Registry. In each implementation, modernization involves moving jurisdictions from legacy to on-premises IIS platforms to a cloud-based, configurable SaaS solution that supports CDC and AIRA standards, seamless interoperability with HIEs and EHR systems, and greater resilience and scalability.

These projects show the methodology works in both large states with high transaction volumes and rural environments with unique operational needs. With this customized implementation methodology, West Virginia gains the following benefits:

- **Predictability.** Tested tools, templates, and governance structures reduce risk.

- **Adaptability.** Tailored processes support rural connectivity needs and State-specific vaccine distribution workflows.
- **Speed and Compliance.** Quarterly compliance releases maintain alignment with CDC, ACIP, and AIRA requirements without added enhancement costs.

By adopting this methodology, West Virginia selects a path built on partnership, proven technology, and predictable success. Our expert team and disciplined approach deliver an IIS that enhances public health and delivers lasting value West Virginians.

4.2.1.9.1.3. Initiatives to Develop Standards and Capabilities

The IIS participates in initiatives to develop standards and capabilities through several activities:

- **Data Governance and Standards Alignment.** Gainwell collaborates with the State during the Foundation Layer requirements phase to review existing governance processes and align them with the State's Governance Framework. This work includes adopting enterprise-wide standard data definitions and semantics in accordance with State Data Policies and Standards. Gainwell contributes to enterprise data governance initiatives such as data modeling, data dictionaries, Extract-Transform-Load (ETL) mappings, and source-to-target mappings to maintain enterprise data assets. We also establish integration and communication expectations with ISL modernization vendors and partners
- **Data Management and Security.** Gainwell defines role-based access to data and supports Single Sign-On (SSO) integration with the State's security policies, procedures, and standards. Gainwell schedules security and data assessment activities supporting Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0, NIST 800-53, and other security frameworks. We maintain compliance with updated State Data Policies and Standards through regular security reviews.
- **Integration and Communication.** Gainwell works with ISL vendors to establish standards for data sharing, maintenance, interfacing, and reference data usage. We develop Interface Control Documents (ICDs) for data exchanges with appropriate partners and document data validation requirements, content, delivery, and format. Gainwell also defines rules for audit log and auditable-event management and supports data archiving using tools such as SIEM and cloud monitoring solutions that feed into SLA/KPI dashboards.

These activities demonstrate Gainwell's participation in initiatives to develop standards and capabilities, focusing on data governance, security, integration, and communication within the State's environment.

4.2.2. West Virginia Specific Goals and Objectives

The following goals and objectives reflect West Virginia's specific public health priorities, operational workflows, and stakeholder feedback. These capabilities are not required for contract award but are highly desirable. The Vendor should describe their methodology or approach to accomplishing these goals and objectives.

Gainwell's methodology and approach to accomplish West Virginia's specific public health priorities, operational workflows, and stakeholder feedback goals and objectives is set forth below.

4.2.2.1. System Optimization, Innovation, and Interoperability

OEPS seeks to promote continuous improvement and efficiency within the HS. The intent of this section is for Vendors to propose optional features, methods, or enhancements that demonstrate innovation, streamline system performance and improve data quality and interoperability. The following support this goal.

4.2.2.1.1. The Vendor should describe any processes or practices in place for sharing beneficial system improvements or enhancements, developed through work with one jurisdiction, and later offered to their broader customer base at no additional costs. The response should include:

4.2.2.1.1.1. The Vendor should describe how they evaluate and determine whether a customization or optimization may be broadly beneficial.

4.2.2.1.1.2. The process and timeline for releasing such enhancements to all customers.

4.2.2.1.1.3. Any governance, release management, or communication procedures that ensure jurisdictions are informed of available improvements.

4.2.2.1.1.4. Vendors should describe any examples of recent improvements or enhancements provided to customers at no additional cost.

4.2.2.1.2. The Vendor should describe their approach and methodology for achieving an error and hold queue for HL7 messages, or for providing an easy way to identify and sort rejected messages.

4.2.2.1.3. The Vendor should describe their approach or methodology for automating updates and synchronization of code sets with CVX, MVX, and NDC tables.

4.2.2.1.4. The Vendor should describe their approach or methodology to bulk loading, activating, and deactivating providers, facilities, and users.

Gainwell's approach to Immunization Information System (IIS) modernization includes system optimization, innovation, and broad interoperability, as described below:

- **System Optimization.** Gainwell uses a Continuous Improvement Process supported by a Quality Assurance team to manage product releases, provide reporting support, and monitor system performance. This team leads capacity and performance management, SLA/KPI monitoring, and business process automation improvements. Gainwell also conducts quarterly client-facing innovation sessions to review cloud operations, spending, sizing, and performance, promoting ongoing optimization.
- **Innovation.** Gainwell empowers clients with innovative technologies and solutions to improve health and human services outcomes. Our tools help organizations deliver high-quality programs while improving efficiency and operational agility.

For example, Gainwell's Pharmacy Solutions illustrate our ability to lower the total cost of care while supporting improved patient outcomes.

- **Data Extraction and Interoperability.** Gainwell's technical solutions support the State's diverse healthcare ecosystem, including health organizations, remote clinics, pharmacies, and CDC systems. Gainwell Assist provides seamless integration with the CDC IZ Gateway, SMART Health Cards, HL7 v2.5.1 messaging. The Mass Vaccination module is optimized for rural providers operating in low-bandwidth environments. Gainwell's platforms support high-volume data exchange and integrate seamlessly with thousands of external systems, including:
 - Electronic medical record (EMR) and electronic health record (EHR) platforms
 - State-level health information exchanges (HIEs)
 - Vital records systems and managed care organizations (MCOs)

Gainwell completes the mapping of product fields and data extraction logic in the necessary Structured Query Language (SQL) scripts. Gainwell has successfully transitioned from legacy systems using automated ETL tools and rigorous validation protocols. These scripts extract data from the database, then systematically send the extracted data to Gainwell's Data Migration Server for import into Gainwell Assist. This enables secure, cloud-based data management, using Gainwell's position as one of Amazon Web Services (AWS) largest public sector customers of comprehensive cloud computing.

4.2.2.1.1. Process for Sharing Beneficial System Improvements or Enhancements

Following are descriptions of Gainwell's processes or practices for sharing beneficial system improvements or enhancements.

4.2.2.1.1.1. Evaluate and Determine Customization or Optimization

Gainwell evaluates and determines whether a customization or optimization may be broadly beneficial through a comprehensive approach that involves several key strategies:

- **Product Development Model.** Gainwell embraces a true product development model that incorporates user and client feedback directly into the Gainwell Enterprise™ solution and client roadmaps. This approach includes holding quarterly user group sessions with clients to gather insights and recommendations, confirming solutions are innovative and tailored to client needs.
- **Gainwell Assure Reviews.** Gainwell conducts Gainwell Assure reviews for each system development life cycle (SDLC) phase and at least four (4) times a year for current and planned implementation projects. These reviews focus on immediate improvement actions and involve detailed program and project execution level reviews. They include confidential interviews with customer and Gainwell program leads, holistic reviews based on project data, and the development of action-oriented project quality and risk summaries. The resulting Gainwell Assure Summary Report identifies actionable improvement steps to enhance service quality.
- **Advisory Council.** Our national Gainwell IIS Advisory Council features lead personnel from our immunization projects. They meet regularly to discuss upcoming regulatory and industry changes and to share insights to meet these new program requirements effectively. The Advisory Council is a rich resource our Account Delivery Team personnel uses to share new ideas and the latest thinking to improve service to our customers.
- Gainwell also has a dedicated IIS Strategy Executive and other Advisory Support Team members whose responsibilities include keeping our Product Support Team and customers informed about upcoming CDC, AIRA, and IIS Best Practices Community of Practice initiatives. This position also serves as a liaison with the State on Gainwell and IIS Advisory Council activities.
- **Emerging Technologies and Innovations.** Gainwell continually evaluates emerging technologies to enhance the Gainwell Enterprise solution through a dedicated technology council led by the Chief Technology Officer and subject matter experts. This council identifies and recommends advancements in AI-driven solutions, COTS tools, process improvements, and infrastructure modernization.
- **Regular Product Releases.** Gainwell deploys major product releases three times per year, allowing clients to adopt new features and updates at their convenience. These updates are rigorously vetted and tested to enable quality and reliability, with additional testing conducted in dedicated client environments to confirm seamless integration and optimal performance.

4.2.2.1.1.2. Process and Timeline for Releasing Enhancements

Gainwell has a structured process and timeline for releasing enhancements to its customers. We update our products through releases to address federal and industry changes and incorporate enhancements for customers while maintaining solution configurations. The release management process includes rigorous vetting and testing by Gainwell's centralized product development team to provide high standards of quality and reliability. Additional testing is conducted in dedicated client environments to confirm seamless integration and optimal performance tailored to client needs. For immediate requirements, patches are made available on a three-week cycle to address critical updates, and hotfixes are delivered on an ad hoc basis to quickly resolve urgent issues.

Gainwell's release management approach includes managing release preparation and review, building documentation, acquisition, testing and test environments, and closure activities. The company adheres to the State's standards for release and deployment and proven practices for separation of duties between development, testing, and deployment. The continuous integration (CI) and continuous delivery (CD) pipeline supports quick packaging and delivery of new releases to clients in a cloud environment, including updated release documentation and training.

Once installed during non-production hours, except for emergencies, the application of local configuration and data stores takes place in hours, and validation of configuration changes with smoke testing and local testing takes about a week.

4.2.2.1.1.3. Jurisdictions Informed of Available Improvements

Gainwell employs several governance, release management, and communication practices to keep jurisdictions informed of improvements and ongoing system enhancements.

- **Governance and Compliance Management.** Gainwell has a comprehensive governance framework and compliance management processes to verify adherence to applicable laws, regulations, and contractual obligations related to the provision of services to customers. This framework enables Gainwell to meet additional requirements from entities such as the CDC.
- **Release Management and DevOps Methodology.** Gainwell maintains a formal release and deployment management processes and procedures for new or changed services.

The product is usually updated three times a year to address federal and industry changes and incorporate enhancements for customers. This process includes release preparation and review, build documentation, acquisition, testing, and closure activities. Gainwell adheres to the State's IT standards for release and deployment and proven practices for separation of duties between development, testing, and deployment. The CI/CD pipeline supports quick packaging and delivery of new releases to clients in a cloud environment, including updated release documentation and training.

- **Continuous Improvement and Innovation Management.** Gainwell maintains a prioritized log of Continuous Improvement Process (CIP) technical innovation changes and tracks and reports them quarterly.

The Quality Assurance / Continuous Improvement Process (QA/CIP) and Innovation Managers collaborate with the State, other module vendors, and Gainwell staff to support ongoing innovation, maturity, and improvements to technology, processes, and analytical and reporting capabilities.

- **Customer Satisfaction Measurement.** Gainwell measures client satisfaction through frequent and open communication, including formal and informal discussions with clients to gauge satisfaction and seek feedback on performance. Formal mechanisms for feedback include regularly scheduled status meetings, solution release management team meetings, and meetings between clients and senior Gainwell account leadership. Client feedback is a critical input to Gainwell's continuous process improvement activities in the quality management practice.

4.2.2.1.1.4. *Examples of Recent Improvements or Enhancements*

Gainwell Assist brings the advantage of quarterly releases, at no additional cost, to keep current with CDC and AIRA requirements and codes. The Gainwell Immunization Solution Product Team also routinely reviews the product and recommends new functionality, updates to configurations, and updates to supporting business processes to enable efficient and effective use and to continue complying with laws and regulations. Enhancements not included in the quarterly releases can be implemented using enhancement pool hours.

Gainwell will develop and execute a detailed implementation plan for IIS enhancements to maintain compliance and meet or exceed standards and specifications. Our solution supports a variety of options for exchanging data via integration with external source systems, including HL7, SOAP (with CDC and IZ Gateway WSDLs), and flat file. Our solution is COTS-based and relies heavily on standards-based protocols, so we can quickly adopt new integration methods, protocols, and formats, as needed, to provide ongoing support.

Gainwell maintains longstanding, active involvement with AIRA, CDC, ACIP, and other IIS-focused organizations, which allows us to stay informed about current and emerging enhancement needs and upcoming CDC requirements. We understand the urgency associated with these changes and recommend enhancements to the modernized solution that keep it aligned with the State's immunization goals. We also make required updates as promptly as possible.

As part of our ongoing support, Gainwell remains current on national standards and new regulatory requirements that affect immunization systems. Our Solution Product Support personnel engage continuously with the Gainwell Maintenance and Operations (M&O) team to review updates and enhancements through regular releases and the established product roadmap.

Our SaaS delivery model includes centralized development of product enhancements supported by a focused Product Team that works closely with local account delivery teams to support multiple customers. We also maintain a nationwide workgroup of immunization service delivery experts to support customers and define new product capabilities. We provide the following comprehensive range of cloud-based SaaS solutions designed to modernize healthcare and human services:

- **Gainwell Assist™** supports human services and public health programs through person-centered, data-driven capabilities. These include IIS, early intervention systems for children with special needs, and solutions that support Women, Infants, and Children (WIC) programs. **Gainwell Assist is the future-ready SaaS solution we propose for the State's IIS.**
- **Gainwell WholeHealth™** focuses on population health management by using data and analytics to target high-risk groups proactively and improve preventive care.
- **Gainwell Go™ User Experience** expands user access through member and provider portals, management portals, mobile apps, and Gabby, our virtual assistant.
- **FraudCapture®** is a SaaS solution that identifies fraud, waste, and abuse (FWA)

- **Gainwell Provider+**™ enhances provider experiences by optimizing workflows and improving care delivery.
- **Gainwell Connect**™ is a cloud-based systems integration and interoperability solution that helps Medicaid agencies modernize their legacy systems and meet federal standards.
- **Gainwell Enterprise**™ is a core Medicaid platform that modernizes claims, encounters, and financials using intelligent automation and interoperability. It helps agencies streamline operations and improve payment integrity.
- **Gainwell Genius**™ AI- and machine learning (ML)-driven analytics solution that transforms healthcare data into actionable insights.
- **Gainwell Rx**™ optimizes medication management to reduce costs and improve patient outcomes.
- through intuitive, mobile-friendly dashboards with clear visualization and drill-down exploration tools.
- **Special Investigative Unit (SIU) Services** is optional expert support for fraud and abuse investigations.
- **Estate Recovery Services** helps agencies recoup payments efficiently and transparently.
- **Coordination of Benefits (COB), Third-Party Liability (TPL), Payment Integrity (PI), Cost Avoidance, and FWA** optimize financial management and payment processes for the State. These solutions help the State manage its financial resources effectively, reduce unnecessary expenses, verify compliance with regulations, and maintain the integrity of its payment processes.

4.2.2.1.2. Approach and Methodology for Achieving Error and Hold Queue for HL7 Message

The IIS employs a high-performance, scalable approach to HL7 message processing that minimizes reliance on traditional error and hold queues while still providing robust error management and visibility.

Drawing on lessons learned during the COVID-19 pandemic, the system is designed for rapid, high-volume message acceptance and processing, reducing bottlenecks and eliminating unnecessary queuing even at peak load for large populations. Messages are processed near real time, with intelligent validation applied at multiple stages to confirm data quality without impeding throughput.

For error handling and management, Gainwell Assist provides comprehensive monitoring and remediation capabilities, including:

- Advanced search and filtering tools that allow users to quickly identify and isolate messages based on job status, error codes (e.g., HL7 ERR segments), severity, vaccine group, and other attributes.
- Detailed job-level visibility, including message control IDs and error locations, to support efficient troubleshooting and resolution.
- Configurable dashboards that display system performance metrics such as message throughput, response times, and submission trends.
- Real-time status tracking of VXU message processing, enabling users to quickly identify and address failed or rejected messages.

Additionally, the IIS supports flexible reprocessing workflows, allowing corrected messages to be resubmitted without manual re-entry. This approach enables efficient error management while supporting continuous data flow and sustained system performance.

Overall, the methodology emphasizes **high establish, minimal processing delay, proactive monitoring, and user-driven error resolution**, confirming reliable HL7 message ingestion without dependence on large backlog queues.

4.2.2.1.3. Approach or Methodology for Automating Updates and Synchronization of Code Sets

Gainwell Assist integrates directly with the CDC source system allowing for timely downloading and execution of the latest vaccine code sets as they are released. Current Procedural Terminology (CPT), Vaccines Administered (CVX), and National Drug Code (NDC) codes are supported by our Solution using the CDC's Vaccine Code Sets and crosswalks. Integration with the CDC system allows Gainwell to be notified automatically when there is a new code set. With SaaS, we can quickly deploy new code sets to our Staging environment for immediate testing and approval before release to the Production environment. Deploying updated CDC code sets is a mandatory requirement, and our process streamlines this work by removing the need for extensive functional-design documentation or waiting for change control board approvals. This approach accelerates implementation and reduces the burden on the State.

4.2.2.1.4. Approach or Methodology to Bulk Loading, Activating, and Deactivating Providers, Facilities, and Users

The approach or methodology to bulk loading, activating, and deactivating providers, facilities, and users in an IIS involves several key components and processes:

- For activation and deactivation, the system leverages configurable status fields and effective dating, allowing records to be enabled or disabled individually or in bulk without data loss. Administrative users can also manage these updates through role-based access controls within the application interface.
- Where required, automated workflows can be configured to support scheduled or event-driven updates (e.g., onboarding new providers or deactivating inactive users), confirming alignment with external systems such as provider registries or identity management solutions.

This approach provides a flexible, scalable methodology for managing large volumes of provider, facility, and user records while maintaining data quality, auditability, and operational efficiency.

4.2.2.2. Implementation Plan

OEPS seeks to have a seamless transition from existing IIS to new IIS. The intent of this section is for OEPS to evaluate how comprehensive and established the Vendors Implementation Process is. The Vendor should provide a comprehensive description of their approach and methodology for implementing the proposed IIS and migrating existing data. The response should include, but is not limited to, detailed information on the following:

The Vendor's proposed Implementation Plan will be evaluated under Section 4.2.2.2. The finalized Project Plans and Schedule shall adhere to this Implementation Plan in accordance with Section 4.2.3.7, subject to Agency review and approval. Any deviations must be documented, justified and approved by the Agency.

4.2.2.2.1. Overall project management strategy and implementation timeline.

4.2.2.2.2. The environment setup, which consists of the following: Production, Test, and Development servers.

4.2.2.2.3. System configuration and workflow customization.

4.2.2.2.4. Data migration strategy, including:

4.2.2.2.4.1. Existing IIS data migration.

4.2.2.2.4.2. User and roles migration.

4.2.2.2.4.3. Provider, Facility, and Organization migration.

4.2.2.2.4.4. Program enrollment migration.

- 4.2.2.2.4.5. Existing Interface migration and testing.
- 4.2.2.2.5. Change request management process.
- 4.2.2.2.6. Roles and responsibilities of vendor and client teams.
- 4.2.2.2.7. Risk mitigation strategies and contingency planning.
- 4.2.2.2.8. Training, support, and knowledge transfer during implementation.

Gainwell understands the State would like a seamless transition from the existing IIS to a new IIS. We describe our implementation process in our responses to the requirements below.

4.2.2.2.1. Project Management Strategy and Implementation Timeline

Phase 1: Project Initiation Planning. The foundation of a successful project is a meticulously crafted plan. Within 30 days of contract award, we initiate this phase to establish project governance, refine plans, and align with the State.

- **Collaborative Kickoff.** We facilitate a project kickoff meeting to introduce our dedicated project team, establish clear roles and responsibilities, and validate the project scope, goals, and communication plan.
- **Master Project Management Plan (MPMP).** We deliver a comprehensive MPMP that serves as the project's blueprint. This living document includes a detailed work plan/schedule, resource plans, a risk management plan, a change management process, and clearly defined entrance/exit criteria for each project phase.

Phase 2: Agile System Design and Configuration. This phase focuses on translating the State's requirements into a fully configured system. Using an agile approach, we work in sprints to configure, demonstrate, and refine the IIS.

- **Requirements Refinement and Traceability.** We conduct workshops with State stakeholders to validate functional and technical requirements via demonstration-driven requirements validation approach. This process confirms that each requirement is mapped, configured, tested, and delivered.
- **Iterative Configuration and Demonstrations.** Our team configures our base IIS platform to meet West Virginia's specific needs for the Registry, Vaccine Management, Reporting, and Integration modules. A key strength of our platform is its high configurability, which requires minimal custom development. At the end of each sprint, we conduct demonstrations for the State to highlight progress and gather feedback, so the system evolves in lockstep with the State's vision.

Phase 3: Seamless Data Migration and Integration. The integrity of historical and incoming data is paramount. Our proven data migration and interface development methodology mitigates risk and facilitates a seamless transition.

- **Low-Risk Data Migration.** We execute the Data Conversion and Migration Roadmap, using our powerful Extract-Transform-Load (ETL) tools and processes honed over dozens of similar state projects. Our process includes extensive data profiling, validation, and multiple mock conversion cycles to achieve and verify the accuracy and completeness of the more than 1.6 million patient records and 17.6 million vaccination histories.
- **Uninterrupted Interface Transition.** We recognize the critical importance of the active HL7 connections. Our dedicated interface team works directly with provider groups and State staff to transition the existing interfaces to the IIS, preventing disruption in data flow. We also

apply our deep expertise with the IZ Gateway and VTrckS so these national connections are robust and fully compliant.

Phase 4: Comprehensive Testing and Quality Assurance. Our rigorous, multilayered testing strategy delivers a high-quality, reliable, and performant system.

- **Multitiered Testing Cycles.** As outlined in our Test Management Plan, our team conducts comprehensive testing, including unit, system, integration, interface, and regression testing. We resolve the identified defects to the State's satisfaction before User Acceptance Testing (UAT).
- **Collaborative User Acceptance Testing (UAT).** We provide full support to the State during the UAT phase, including providing a dedicated UAT environment, detailed base product test cases/steps, and onsite or remote assistance for users. This collaborative approach results in a system fully vetted and approved by the individuals that use it daily.

Phase 5: User-Centric Training and Go-Live Readiness. A successful implementation hinges on user readiness. Our methodology trains users and prepares systems and processes for a smooth go-live.

- **Role-Based Training Program.** We develop and deliver a comprehensive training program tailored to the specific needs of each user group. Employing a variety of methods, including guided online seminars, recorded sessions, and detailed user manuals, we see that each user is confident and competent in using the new IIS.
- **Operational Readiness Review (ORR).** Before go-live, we conduct a thorough ORR to validate the technical, operational, and organizational components are in place. This includes confirming system performance, as well as supporting staff readiness and workflow validation. We provide a final ORR report with a clear go/no-go recommendation, so the launch can be confident and successful.

Phase 6: Smooth Deployment and Proactive M&O (Go-Live and Beyond). Our responsibility extends far beyond implementation. We are committed to providing exceptional ongoing support, maintenance, and continuous improvement for the life of the contract.

- **Seamless Go-Live.** Following the detailed Implementation and Rollout Plan, we deploy the fully tested and approved IIS into the production environment. Our team provides heightened Hypercare support during the initial post-launch period to address issues rapidly. Hypercare includes a comprehensive support model that is part of Gainwell's Command Center approach. It provides pre-launch and post go-live support for business-as-usual readiness, customer service, quality assurance (QA), and accelerated issue resolution. This support model is designed to enable end users to transition smoothly to the long-term operating model.
- **Proactive Maintenance and Operations (M&O).** We execute the Post-Production Support Plan, delivering on the Service Level Agreements (SLAs) for system availability, performance, and support. Our dedicated M&O team handles routine maintenance, applies patches and upgrades, manages help desk escalations, and keeps the system compliant with evolving CDC standards, including ACIP schedule changes and CDSi logic updates.
- **Driving Value Through Consortium Leadership.** As a leader in the IIS community, Gainwell facilitates a robust consortium of its state partners.

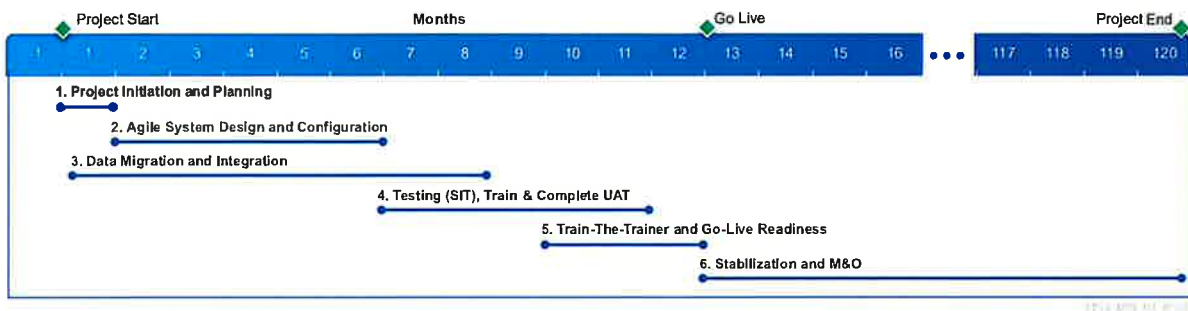
We integrate West Virginia into this group, providing a platform to take advantage of enhancements developed for other states, share proven practices, and collaborate on future

IIS innovations. The State benefits from a consortium model and enables the IIS to remain a leading-edge system.

Timeline to Go-Live

In response to the State's RFP, we propose a 12-month implementation timeline for Gainwell Assist. We believe a 12-month implementation, which is common among IIS projects, is justified to support **high quality and to accommodate a number of critical tasks**. The critical tasks needed for a successful go-live include tailoring configurations to the State's needs; conducting system and user acceptance testing; data migration; training and onboarding users and data providers; risk reduction; and more. The following high-level timeline illustrates our proposed 12-month implementation.

Figure 4. High-Level Project Timeline



4.2.2.2. Environment Setup

Overall, the AWS cloud solution allows for rapid deployment of additional servers, memory, and disk space when needed, confirming that logical environment requirements are continually met. The architecture is elastic to accommodate dynamic workloads, and capacity planning is performed to verify business demands and SLAs are met.

An automated deployment process is used to create each environment, starting with a dataset that does not contain Protected Health Information (PHI). The configuration is customized for the State, allowing for a working system at the earliest stage of implementation.

The environment setup for Production, Test, and Training is designed to meet the needs of the State using Amazon Web Services (AWS) cloud solutions, as described below.

Production Environment

The production environment uses real data and is part of a shared hybrid cloud setup. This environment is architected for reliability and resiliency with no single point of failure, enabling 99.95% uptime. AWS provides redundancy and fault tolerance using Availability Zones, which are discrete data centers with redundant power, networking, and connectivity.

Test Environment

The test environments consist of the following:

- **System Integration Testing (SIT).** This environment uses de-identified or synthetic data and is part of a shared hybrid cloud setup.

- **User Acceptance Testing (UAT).** The UAT environment, also known as the Stage environment, uses both de-identified/synthetic and real data and is part of the shared hybrid cloud setup.
- **Operational Readiness Testing (ORT).** This environment uses de-identified/synthetic and real data and is part of the shared hybrid cloud setup. It is fully turned off once conversion and ORT activities are completed to optimize cloud consumption expenditures.

Training Environment

The Training environment is used for training users using deidentified or synthetic data.

4.2.2.2.3. System Configuration and Workflow Customization

Configuration

We understand each public service agency has unique business processes and operational needs. Our SaaS platform is highly configurable and allows agencies to tailor workflows, user interfaces, business rules, notifications, and reporting modules using built-in configuration tools without requiring custom code. This level of configurability confirms Gainwell Assist remains suitable for a wide range of program requirements while maintaining long-term stability, upgradeability, and supportability.

For needs extending beyond features currently available in the product, such as new or evolving State requirements, Gainwell works collaboratively with clients to assess requirements, prioritize enhancements modules, and incorporate changes through a governed product and configuration process. This approach enables agencies to adapt the system to changing State policies while protecting the integrity of the core product and confirming consistent, predictable performance over time.

Gainwell's SaaS delivery model includes centralized development of product enhancements supported by a dedicated Product Team. This team works closely with local account delivery teams and client stakeholders to understand State specific requirements, validate solutions, and deploy enhancements in a controlled and secure manner.

In addition, Gainwell maintains a nationwide work group of immunization service delivery experts who collaborate across jurisdictions to identify emerging needs, define new product capabilities, and confirm solutions reflect best practices and regulatory expectations.

4.2.2.2.4. Data Migration (including 4.2.2.2.4.1. - 4.2.2.2.4.5.)

The IIS employs a proven, secure, and scalable methodology for data migration, drawing on experience transitioning hundreds of millions of records from legacy IIS systems across multiple states.

Our **Data Conversion and Migration Roadmap** begins with a comprehensive assessment of West Virginia's existing data sources, including IIS records, provider and facility data, user roles, and program enrollment information. We work collaboratively with the State to evaluate data structures, files, data marts, and warehouse environments to define the optimal migration strategy, including data mapping, transformation rules, and validation criteria.

Our migration methodology follows a structured, repeatable lifecycle consisting of:

- Data extraction and profiling from legacy systems and external sources.
- Data mapping and transformation design, aligned to the target IIS data model.

- Automated data validation and cleansing to confirm accuracy and completeness.
- Deduplication and record matching to maintain a single, longitudinal patient and provider record.
- Manual data stewardship and quality review for exception handling and validation.
- Secure data transfer and processing within a scalable, cloud-based environment.

A key component of our approach is **iterative validation and close collaboration with the State**. We conduct multiple rounds of data validation, reconciliation, and user acceptance testing, providing detailed reports and data samples for State review at each stage. This approach promotes transparency and enables the State to confirm that migrated data meets expectations for accuracy, completeness, and usability. We recognize that IIS data represents not just records, but an individual's immunization history, and we prioritize preserving its integrity with the highest level of accuracy and confidence.

To further reduce risk, we perform multiple **mock migrations** (trial conversions) using full and incremental datasets to validate transformation logic, data quality, and system performance. Prior to go-live, we execute a **final production migration and reconciliation**, including detailed comparison reports and formal State review and sign-off to confirm completeness and accuracy.

Our approach also includes a clearly defined **cutover strategy**, confirming continuity of operations and minimal disruption to providers and end users. We maintain **contingency and rollback procedures** throughout the migration process to safeguard data integrity and confirm rapid recovery in the event of issues.

We leverage extensive experience interfacing with external systems, including EHRs (e.g., Epic, Cerner), HIEs, vital records, and MCOs, to efficiently extract and normalize data. Our cloud-based infrastructure, supported by AWS, enables high-performance processing of large data volumes while maintaining strict security and compliance standards.

This structured, collaborative, and risk-mitigated approach supports the delivery of migrated data that meets established expectations for accuracy, completeness, validation, and readiness for use at go-live, while minimizing disruption and supporting continuity of operations.

4.2.2.2.5. Change Request Management Process

Gainwell follows a structured change management process. Change requests are logged, tracked, and monitored until resolution and closure following this structured process. For example, the configurable aspects of Gainwell *Assist* are managed through change control. Approved changes are implemented following our configuration management process in preparation for promotion to Production following release management protocols.

4.2.2.2.6. Roles and Responsibilities of Vendor and Client Teams

To support a smooth and orderly transition of system functions and data, Gainwell will provide a comprehensive Transition Plan outlining the activities required for transferring contracted responsibilities to the new vendor or back to the State. The State and the selected vendor will work collaboratively to verify successful data migration, testing, and overall system readiness. The table below summarizes the key responsibilities for each team.

Table 2. State and Gainwell Responsibilities

Category	State Responsibilities	Gainwell Responsibilities
Data Migration	• Provide complete, current production data for migration and validation • Support database queries, extracts, and clarify data structures and legacy schema	• Lead data-mapping sessions with State stakeholders • Develop and run ETL scripts for conversion, cleansing, and loading • Coordinate end-to-end migration timelines, dependencies, checkpoints, and environment readiness • Perform pre- and post-migration validation, produce reconciliation reports, and resolve discrepancies before UAT and go-live
User Acceptance Testing (UAT)	• Lead planning, coordination, and execution of UAT • Develop and manage UAT test cases and workflow scenarios • Coordinate participation from business users and stakeholders • Execute UAT cycles, document results, validate fixes, and provide timely approval and sign-off	• Provide core product test cases to support the State's UAT design • Support UAT execution through issue triage, defect analysis, environment preparation, data staging, and functional guidance • Assist with UAT status reporting, including defect metrics and test-execution statistics • Resolve UAT defects and support retesting and final validation
Governance and Project Management	• Participates in governance activities, attend status meeting, review deliverables, and make timely decisions	• Maintain the project plan, schedule, migration timeline, and UAT calendar • Provide regular status reports, risk logs, issue logs, and mitigation recommendations • Identify risk early and coordinate mitigation and dependency management with the State

4.2.2.2.7. Risk Mitigation Strategies and Contingency Planning

Gainwell has strategies to mitigate project risk, as described below.

- **Accurate and Secure Data Migration.** Using our migration framework, we successfully transitioned hundreds of millions of records from legacy IIS systems in other states. Our approach combines automated data validation, deduplication, and manual stewardship to deliver clean, accurate, and ready-to-use data from day one.
- **User Adoption.** Resistance to new workflows is a risk. We deliver a customized Train-the-Trainer program for West Virginia's providers and public health staff. Gainwell Assist features role-based user interfaces (UIs), multilingual support, and an integrated help desk.

- This allows providers and public health staff across remote regions to quickly adopt and benefit from the system.
- **Disaster Recovery.** Our Team's deployment across multiple AWS Availability Zones provides a resilient environment that guards against downtime and data loss.
- **Cost Predictability.** Quarterly compliance releases are included, avoiding costly upgrades for CDC or ACIP changes.
- **Key Risk Areas and Mitigation Approaches.** Designing, installing, and maintaining unsupported or free open-source components can result in limited maintainability or challenges in meeting security requirements, and potential for escalating costs. Gainwell mitigates these risks by avoiding unsupported open-source technology for core functionality, protecting stability, performance, and security.
- **Rural Access.** Remote providers with intermittent connectivity may face delays. asynchronous HL7 queueing prevents data loss.

We log, track, and manage general project risks using our project risks, actions, issues, and decisions (RAID) tool. This tool allows staff to document potential risks with mitigation strategies and project issues with resolution plans. We will regularly review these risks and issues with the State during status reporting and meetings, seeking approval before implementing mitigation or resolution plans.

Gainwell will employ a program-wide solution that reduces project risk by using consistent, repeatable processes and documentation specific to IIS projects, establishing clear project management communication, monitoring, and reporting, while maintaining a common understanding of project responsibilities.

Risk Mitigation by Design

Our approach reduces West Virginia's risk with:

- Proven deduplication accelerators for large dataset migrations
- Command Center *Hypercare* support for 90 days post-go-live
- CDC IIS Certification alignment to meet federal requirements

4.2.2.2.8. Training, Support, and Knowledge Transfer During Implementation

Gainwell develops and delivers a comprehensive, role-based Training Plan using a variety of methods to meet diverse user needs.

We conduct a formal Operational Readiness Review (ORR) to confirm the technical, operational, and organizational components are ready for a successful launch. We implement our comprehensive, role-based Training Plan 90 days before go-live. By offering multiple training formats, including online, guided seminar, and recorded sessions, and developing clear, plain-language user manuals, we enable users to be confident and prepared.

Focus on the End User

We understand the system's success depends on its adoption by diverse users. Our comprehensive Training Plan is tailored to the specific needs of each user group, including State staff, healthcare providers, and school nurses. We use a variety of training methods, and provide robust, plain-language user manuals and ongoing Tier 2 help desk support so users can be confident and competent in using the new system.

A successful implementation depends on user readiness. Our methodology trains users and prepares systems and processes for a smooth go-live.

- **Role-Based Training Program.** We develop and deliver a comprehensive training program tailored to the specific needs of each user group. Employing a variety of methods, including guided online seminars, recorded sessions, and detailed user manuals, allows us to confirm each user is confident and competent using the IIS.
- **Operational Readiness Review (ORR).** Before go-live, we conduct a thorough ORR to validate that the technical, operational, and organizational components are in place. This includes confirming system performance, support staff readiness, and workflow validation. We provide a final ORR report with a clear go/no-go recommendation, so the launch can be confident and successful.

Additional Considerations

At the end of the Contract, Gainwell will grant the State, without additional license fees, a perpetual license to Gainwell Assist, subject to Gainwell's current license terms and conditions and exclusive of licenses to third-party embedded components or third-party software required for the operation of Gainwell Assist, solely for the State's internal government business purposes. Continued maintenance and support services, including updates if offered by Gainwell, will be provided pursuant to Gainwell's then-current terms and conditions for such services, including applicable maintenance and support fee(s). The continued use of Gainwell Assist is contingent upon the State obtaining required third-party software licenses and paying associated third-party license fees as necessary for the operation of the module. 4.2.2.3. Vaccine Exemption Functionality

OEPS seeks to enhance its IIS with robust vaccine exemption tracking and reporting capabilities. The intent of this section is for OEPS to evaluate how comprehensive and configurable the Vendor's IIS exemption functionality is, and how well it supports jurisdictional needs for school-entry compliance, public health reporting, and exemption management.

The Vendor should provide a detailed description of their approach, system capabilities, and configuration options related to vaccine exemptions. The response should include, but is not limited to the following:

- 4.2.2.3.1. Ability to record exemptions by vaccine or disease category.
- 4.2.2.3.2. Support for exemption types: permanent, temporary (with expiration date), and provisional (with review date).
- 4.2.2.3.3. Support for exemption reasons: medical, religious, philosophical.
- 4.2.2.3.4. Linkage of exemption records to patient demographics (e.g., age, race/ethnicity, geography).
- 4.2.2.3.5. Reporting capabilities by school, grade, district, exemption type, and compliance status.
- 4.2.2.3.6. Integration with school roster functionality and support for longitudinal tracking.
- 4.2.2.3.7. Configuration options for jurisdiction-specific exemption workflows and review processes.

Following is a description of Gainwell's approach, system capabilities, and configuration options related to vaccine exemptions.

4.2.2.3.1. Record Exemptions by Vaccine or Disease Category

Gainwell Assist supports the recording and management of immunization exemptions at the vaccine or disease category level. The solution provides configurable, role-based permissions that control which user roles may view, enter, edit, or manage exemption records.

The system supports multiple exemption types, including medical, philosophical, and provisional exemptions. Exemption types and associated business rules are configurable to align with jurisdictional requirements. Exemptions may be recorded at both:

- **Individual (Patient) Level.** Allows exemptions to be applied to specific vaccines or disease categories.
- **School Level.** Enables authorized school users to document and manage applicable exemptions in accordance with defined permissions.

Exemption records are maintained with appropriate audit tracking to verify data integrity, accountability, and compliance with program requirements.

4.2.2.3.2. Support for Exemption Types

Gainwell *Assist* supports the documentation and management of jurisdiction-defined exemption types within the patient immunization record, including medical, philosophical, religious (if applicable), provisional, and temporary exemptions with jurisdiction-defined expiration or review dates.

The system enables authorized users to record exemption status and maintain associated documentation. For provisional situations, supporting documentation (such as provisional certificates) may be recorded and maintained within the system to support compliance tracking and verification activities.

Through reporting and data extraction capabilities, jurisdictions may identify individuals with documented exemptions to support operational follow-up and oversight processes, consistent with program policy. Role-based access controls confirm that only authorized users may enter, update, or view exemption information, maintaining appropriate data governance and confidentiality safeguards.

4.2.2.3.3. Support for Exemption Reasons

Gainwell *Assist* provides comprehensive support for configurable exemption types to meet jurisdictional and program-specific requirements. The system supports standard exemption categories, including medical, philosophical, religious (if applicable), provisional, and temporary exemptions with jurisdiction-defined expiration or review dates.

4.2.2.3.4. Link Exemption Records to Patient Demographics

Gainwell *Assist* links exemption records directly to the patient's demographic profile within the system, confirming exemptions are fully integrated with individual-level data for reporting, analysis, and compliance monitoring.

The solution supports robust reporting capabilities that allow exemption data to be analyzed by a wide range of demographic and geographic attributes, including:

- County
- City
- ZIP code
- State
- Vaccine group
- Vaccine trade name

Using configurable custom reporting features, authorized users may generate reports that combine exemption status with demographic data to support public health analysis, school compliance monitoring, and jurisdictional oversight.

Reports may be scheduled with user-defined recurrence rates (e.g., one-time, daily, weekly, or monthly) and can be configured for automated distribution to selected individuals or role-based groups. Report visibility and distribution are controlled through role-based access permissions to provide appropriate data security and confidentiality. Report generation and distribution activities are audit-trailed to support compliance and accountability requirements.

4.2.2.3.5. Reporting Capabilities by School, Grade, District, Exemption Type, and Compliance Status

Gainwell Assist provides role-based access and reporting capabilities to childcare and school staff to assist in disease investigation and control. It provides the necessary reporting and analytics capabilities that accurately outline coverage rates for vaccine-preventable diseases to help the State, schools, and childcare facilities pinpoint individuals lacking immunizations and who are therefore susceptible to outbreaks.

4.2.2.3.6. Integration with School Roster Functionality

Our School Record Management module can be configured for both school and childcare functionality. This module improves compliance rates through immunization requirements. School nurses and staff can use this module to review a child's existing immunization records and enter medically verified historical immunizations that are missing in their IIS.

The State determines the documents to be considered as proof of medically verified historical immunization. Users can generate reports to determine compliance, identify individuals that may be missing immunization requirements, or determine who is susceptible to a vaccine-preventable disease. The benefits providers will realize by promoting this module will be seen with the increased accuracy and completeness of immunization records. Data collected from schools and daycares can be configured to monitor compliance in geographic areas of excellence or areas of further opportunity for outreach and health education.

4.2.2.3.7. Configuration Options for Jurisdiction-Specific Exemption Workflows and Review Processes

The configuration options for jurisdiction-specific exemption workflows and review processes include the following features:

Configurable Workflows. The enhanced configurability of workflows reduces manual processing and increases transparency into tasks at hand, allowing users to create tasks automatically or manually to address specific workflow needs.

Workflows can be configured to meet specific needs, such as error queues, review and approvals, employing a hierarchical, role-based approval process to route electronic work objects through multiple system and user actions.

Task Management and Notifications. This allows alerts and reminders to be configurable to display in the user workspace or sent through email, triggering conditionally or at intervals.

4.2.2.4. Coverage Reporting and Population Definition

OEPS seeks to ensure that the IIS supports accurate, flexible, and jurisdictionally relevant coverage rate reporting. The intent of this section is for OEPS to evaluate how well the Vendor's system defines and applies demographic population parameters for immunization rate calculations, and how configurable the reporting tools are for public health analysis.

The Vendor should provide a comprehensive description of their approach to coverage reporting and how the system supports jurisdiction-specific reporting needs. The response should include, but is not limited to, detailed information on the following:

4.2.2.4.1. Ability to define and document the demographic population used for rate calculations (numerator and denominator).

4.2.2.4.2. Support for jurisdictional filtering by state, county, or other geographic boundaries.

4.2.2.4.3. Ability to generate reports reflecting:

4.2.2.4.3.1. Complete vaccine series.

4.2.2.4.3.2. Initiation of series (1 or more doses).

4.2.2.4.3.3. Final dose needed to complete a series.

4.2.2.4.3.4. Configuration options for customizing report parameters and aligning with CDC and state-defined coverage metrics.

4.2.2.4.4. Configuration options for customizing report parameters and aligning with CDC and state-defined coverage metrics.

Following is an overview of Gainwell's coverage reporting and how the system supports jurisdiction-specific reporting needs.

4.2.2.4.1. Define and Document Demographic Population Used for Rate Calculations

Gainwell's integrated IQIP reporting module helps jurisdictions clearly define how vaccination rates are calculated by walking users through the definition of both the denominator and the numerator. The system allows users to configure who is included in the denominator population by selecting criteria such as:

- Age range (e.g., 24–35 months)
- Birth date range
- Geographic location (county, city, ZIP code, district, statewide)
- Facility or provider
- Patient status (active, inactive, etc.)
- Demographic attributes (race, ethnicity, gender)

Example denominator: Children aged 24–35 months living in a specified county. Once the denominator group is set, the system calculates the numerator using selected vaccine criteria and “up-to-date” (UTD) definitions. Example numerator: The number of children within the denominator group who are UTD for the selected vaccine or vaccine series.

The IQIP module allows users to:

- Define required dose counts per vaccine
- Apply UTD logic consistent with CDS forecasting
- Select individual vaccines or combined series measures
- Generate assessment reports and multi-year trend analyses
- Export documentation that shows how rates were calculated

The IIS documents both the numerator and denominator criteria within each report configuration, providing clear transparency into how vaccination rates are calculated. This allows jurisdictions to explain how coverage rates are derived and supports consistency with program and federal reporting standards.

4.2.2.4.2. Jurisdictional Filtering

Role-based access empowers users to filter data elements directly within the user interface to improve outcomes for underserved populations through dynamic coverage reports and interactive dashboards.

The IIS supports jurisdictional filtering by State, county, ZIP code, or other geographic boundaries, enabling precise geographic analysis and targeted, community-based immunization interventions.

Custom reports offer robust filtering options, including facility name, district or county, patient status, patient demographics, vaccine group, lot number, trade name, and vaccine event. These options give users flexible, user-driven insights to support data-informed decision-making.

Reports can be saved and scheduled with configurable start and end dates, along with recurring delivery options. Users may also control access by selecting specific individuals or roles authorized to view each report, supporting secure and appropriate distribution.

4.2.2.4.3. Ability to Generate Reports (including 4.2.2.4.3.1. - 4.2.2.4.3.3.)

The IQIP report function enables authorized users to generate customized reports for specific age groups and target populations. Users can define parameters such as an “as of” birth date or a specific date range to accurately assess immunization status over time. IQIP functionality also allows users to select individual vaccine antigens or entire vaccine series for more tailored analysis.

Similar to custom reporting, IQIP reports include robust filtering options such as facility, district, city, state, race, ethnicity, gender, and other demographic criteria. Users can choose from multiple report formats such as assessment summaries, patient listings, provider report cards, and “up-to-date with one visit” reports. Once generated, the report status appears on the IQIP page along with the total number of records included. Users can view or download the completed report for further analysis and action.

The IQIP feature supports targeted evaluation of specific populations and helps jurisdictions identify under-immunized groups. These insights guide focused outreach strategies and inform local quality-improvement plans that align with broader statewide immunization goals.

4.2.2.4.4. Configuration Options for Customizing Report Parameters

The configuration options for customizing report parameters and aligning with CDC and State-defined coverage metrics in an IIS are extensive and include several functionalities:

- **Predefined Parameters and Ad Hoc Reporting.** Users can choose from predefined parameters, singly or in combination, to generate user-customized reports. Ad hoc reporting provides visibility into business and operational data, allowing users to configure and run their own reports to analyze various aspects of operations.

Interactive and ad hoc reports can be exported to Microsoft Word, Microsoft Excel, and PDF. Users can view, subscribe to, and manage reports as well as maintain data sources and security settings.

- **Operational Reporting and Dashboards.** The State can quickly access reports and dashboards to set data filters and date ranges, creating targeted subsets of data. Reports can be generated on a regular schedule or ad hoc basis and include appropriate audit trails. Operational reporting through dashboards delivers detailed information for monitoring activities.

- **Role-Based Security and Alerts.** Reporting privileges are role-based and define who may review or update specific materials based on their project role. Dashboards alert users to service level agreement (SLA) threshold issues, processing trends, and program-management concerns. Security measures protect data and systems.

4.2.2.5. Support Scalable Data Exchange and Reporting via Read Replica Integration

The proposed IIS should support integration with the jurisdiction's data warehouse Data Bridge (Attachment H), through the use of a read replica. This architecture is intended to facilitate secure, scalable data exchange between applications, while enabling flexible development of automated reports and analytical workflows. By leveraging a read replica, the jurisdiction aims to minimize vendor-dependent development efforts and ensure timely access to immunization data for cross-system use, public health analysis, and operational reporting.

The Vendor should describe how their proposed HS supports the use of a read-only replica of the production database to facilitate reporting, analytics, and external system access. Responses should address the following:

- 4.2.2.5.1.** Whether the solution includes a read-only replica or equivalent mechanism to support downstream data access.
- 4.2.2.5.2.** The typical update frequency of the replica (e.g., near real-time, hourly, daily)
- 4.2.2.5.3.** How read-only access is managed to avoid performance or integrity impacts on the production environment.
- 4.2.2.5.4.** The Vendor's approach to configuring, deploying, and maintaining the replication process.
- 4.2.2.5.5.** Support services provided for monitoring, troubleshooting, and ensuring data consistency between environments.
- 4.2.2.5.6.** Availability of documentation describing the replication architecture, update cadence, and access protocols.
- 4.2.2.5.7.** Methods for enabling secure, efficient querying by authorized users.
- 4.2.2.5.8.** Methods for quantifying volume of data interfaced inbound and outbound from primary database, whether via established interface traffic, or one time data extracts.

Gainwell understands the above Scalable Data Exchange and Reporting via Read Replica Integration requirements. Following are our responses to these requirements.

4.2.2.5.1. Read-Only Replica Inclusion

Gainwell *Assist* supports downstream data access through the use of read-only repositories. Select events are published in real time to a centralized event management hub, where downstream systems can subscribe to these events. This allows downstream systems to store information in read-only repositories used in business processes that require data from multiple domains.

4.2.2.5.2. Update Frequency of the Replica

The typical update frequency of the replica in an IIS is near real time. This verifies that no data is lost after it has been committed to the disaster recovery (DR) replication databases.

4.2.2.5.3. Management of Read-Only Access to Avoid Performance/Integrity Impacts

The IIS uses several mechanisms to manage read-only access and protect performance and data integrity in the production environment:

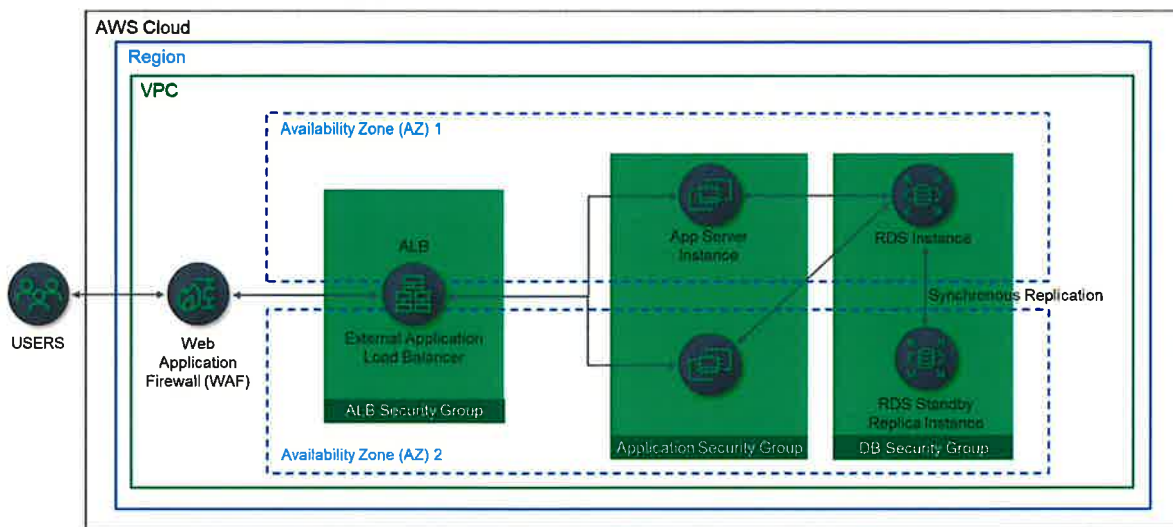
- **RBAC.** Granting access based on the principle of least privilege, verifying users receive only the permissions required for their roles and limiting write access to authorized individuals.

- **Integration Services.** Enabling scalable, service-based business event models that share data across disparate systems in real-time, publishing selected events to a centralized hub where downstream systems subscribe and store data in read-only repositories.
- **Data Governance Controls.** Maintaining normalized transactional databases to minimize redundancy, enforcing foreign key constraints to protect data relationships, and preventing duplicate or orphan records to preserve integrity.
- **Monitoring Tools.** Tracking data flows, detecting errors, and generating alerts for long-running or blocking processes that may affect performance or user experience.

4.2.2.5.4. Approach to Configuring, Deploying, and Maintaining Replication Process

As the following diagram illustrates, our solution's standards-compliant cloud architecture provides a firewall, load balancing, redundancy, and synchronous replication to keep our solution running smoothly. In the rare event of a server or application issue, our architecture leverages multiple AWS Availability Zones, each with independent power and networking, to enable seamless failover. This resilient design protects against data loss and minimizes downtime, delivering continuous availability for West Virginia.

Figure 5. AWS Architecture Diagram



Key elements in each environment include the Application Server instance and the Relational Database Service (RDS) that manages database servers in the cloud, with traffic orchestrated using an External Application Load Balancer. At the database instance level, we have designed Gainwell Assist with the RDS reporting instance separate from the transaction RDS instance, providing more power and resource balancing than within a shared RDS instance.

We use advanced monitoring tools to track throughput and performance and scale the database accordingly. This will help the State gain both operational efficiency and financial predictability.

Security is built into each layer of the architecture. The system uses multi-layered physical, system, and network protections, aligned with NIST 800-53, HIPAA, and IRS Pub 1075 standards, to safeguard protected health information against malicious threats. These protections are continuously monitored, and automated patching and upgrades mean the State benefits from the latest safeguards without the burden of manual intervention.

Gainwell *Assist* provides the State with a future-proof IIS: cloud, secure, and elastic. It will grow and adapt as the State's immunization program evolves, while maintaining uninterrupted service across each community.

4.2.2.5.5. Services Provided for Monitoring, Troubleshooting, and Confirming Data Consistency Between Environments

Gainwell provides several support services for monitoring, troubleshooting, and verifying data consistency between environments in an IIS:

- **Environment Monitoring.** Gainwell uses a selection of tools for environment monitoring.
- **Data Consistency and Governance.** Gainwell coordinates with the State to confirm data integrity across environments. This includes aligning reference data standards in the data lake to verify reporting accuracy, maintain data integrity to validate key identifiers, and protect data accuracy, including referential integrity. Gainwell also establishes standards for data masking and de-identification for testing, defines AWS settings for intrusion detection and prevention, and manages role-based access to data.
- **Incident and Event Management.** Gainwell delivers incident and event management, service management, and technical support through experienced teams. The Centralized Operations Management Center provides 24x7x365 production support for incidents related to the Gainwell environment supporting the State. It manages and categorizes events, detects incidents, manages routine operational activities, and reports on the status or performance of the IIS.
- **Issue Identification and Resolution.** Gainwell has teams in place to promptly resolve issues. The IIS Support Team identifies, investigates, and diagnoses service issues, while the Centralized Operations Management Center manages routine operational activities and coordinates events and incidents. The Technical Team provides advanced user support, and the Cloud Operations Team offers 24x7 technical support.

4.2.2.5.6. Documentation Describing Replication Architecture, Update Cadence, and Access Protocols

Documentation describing the replication architecture, update cadence, and access protocols is as follows:

- **Replication Architecture.** The production environment is architected to provide continuous availability using a multi-Availability Zone architecture, which allows operations to continue if one Availability Zone goes down. Database replication is used to commit transactions across both Availability Zones, providing redundancy and fault tolerance.
- **Update Cadence.** Periodic snapshots of the production environment to support backups and restore capabilities. This is a regular update cadence for maintaining system integrity and disaster recovery.
- **Access Protocols.** The integration with external portals uses an SSO server with Security Assertion Markup Language (SAML) or OAuth 2.0 for role-based access. Additionally, standard data exchange formats such as SOAP and RESTful web services, SFTP, and Transmission Control Protocol/Internet Protocol (TCP/IP) are used for communications and data exchange.

4.2.2.5.7. Methods for Enabling Secure, Efficient Querying by Authorized Users

The methods for enabling secure, efficient querying by authorized users are as follows:

- **Role-Based Access Control (RBAC).** Access to systems and data is granted based on the principle of least privilege, verifying users have only the necessary permissions for their roles.

This approach confines access to assets, systems, software, and the applications they support, providing granular authorizations for access, preview, editing, and sharing. Roles are configurable to specific needs and affiliated with user groups for managing common access needs by business unit or job role/title.

- **Single Sign-on (SSO) Integration.** The modules are integrated with external portals using an SSO server with SAML or OAuth 2.0. This integration provides role- and activity-based access and integrates with the identity and access management (IAM) solution to provide users the appropriate access.
- **Multi-Factor Authentication (MFA).** MFA is implemented to add an extra layer of security, requiring users to provide multiple forms of verification before accessing sensitive systems.
- **Data Protection Measures.** Data is encrypted both in transit and at rest using advanced encryption standards (AES-256) to protect it from unauthorized access. Sensitive data is masked or anonymized where necessary, especially for testing and analytics purposes, to provide privacy and security.
- **Auditability and Monitoring.** Auditability is built into solutions, including platform changes, financial transactions, and history tracking. Cloud auditing tools such as AWS CloudWatch and CloudTrail are used to audit and track changes within the platform. Penetration testing and application vulnerability scans are employed to identify and mitigate vulnerabilities.
- **Governance and Review Processes.** Governance covers data management, data security, data integrity, and data quality control, verifying quality controls are part of the process.

4.2.2.5.8. Quantifying Volume of Data Interfaced Inbound and Outbound

The methods for quantifying the volume of data interfaced inbound and outbound from the primary database include:

- **Integration Gateway Monitoring.** Gainwell's Integration Gateway and service framework monitor data file exchanges and record inbound and outbound metrics. This system supports the receipt and handling of complex interchange transactions, including financial payment processing. It performs initial validations on data inbound into the system and stores copies of the inbound and outbound files for reprocessing and troubleshooting with data partners.
- **Audit Logs.** Audit logs track the inbound and outbound original files as well as applied changes in audit tables to maintain data integrity. These logs help in maintaining the integrity of healthcare data by storing original files for an extended time for potential reprocessing.
- **Automated Monitoring and Validation.** File processing is fully automated and monitored.

The Integration Gateway continually applies data validation to inbound and outbound files with external data partners, retaining full files for a defined time frame for potential reprocessing in the event of errors. CloudWatch is used to monitor the flow of data in and out.

- **Audit Trails.** The IIS produces audit trails related to data and content, stored within a robust table structure. These trails contain specific date and time stamps indicating when information was added or modified, and identifies the individual who made the change. Extract-Transform-Load (ETL) and Electronic Data Interchange (EDI) logs accompany files to identify the number of records inbound and outbound and describe errors found in processing the files.

4.2.2.6. Database Schema and Data Dictionary

To support jurisdictional oversight, data governance, and future system enhancements, the OEPS seeks increased transparency into the structure and logic of the proposed US. Access to a comprehensive database schema and data dictionary enables public health programs to better understand how immunization data is stored, validated, and exchanged.

The Vendor should provide a complete database schema and data dictionary for the proposed IIS solution. These artifacts should include:

4.2.2.6.1. Entity-relationship diagrams or equivalent schema documentation.

4.2.2.6.2. Field-level definitions, including data types, constraints, and allowable values.

4.2.2.6.3. Definitions of key tables, such as patient records, vaccination events, inventory, exemptions, and school roster modules.

4.2.2.6.4. Mapping to CDC HL7 v2.5.1 standards, where applicable.

4.2.2.6.5. Versioning and update protocols for schema changes over time.

For more than 50 years, Gainwell and its predecessor companies have been at the forefront of designing, implementing, and maintaining large-scale government healthcare solutions. A core component of this work has always been the meticulous documentation of complex database schemas. Gainwell will provide a database schema and data dictionary for the proposed IIS solution, as described below. Our team will work closely with the State's subject matter experts (SMEs) to gain an understanding of the current database schemas, data dictionaries, business rules, and hidden data interdependencies.

4.2.2.6.1. Entity-Relationship Diagrams

The Database Administrator updates databases and data dictionaries, resolves issues, and manages schema, performance tuning, and capacity planning.

While aspects of the migration work can be automated, some aspects require manual intervention and adjustments to both database schema objects and database code. Our automated tools for data conversion enable us to migrate data from the existing solution to Gainwell Assist for the State in a manner that retains the integrity of essential data and mitigates the risk of data loss.

4.2.2.6.2. Field-Level Definitions

Field-level definitions will be included. These include data types, constraints, and allowable values. Gainwell provides an automated data dictionary tool that contains codes, code tables, definitions, position definitions, and other descriptors of data collection and display of Gainwell Assist as well as a detailed mapping of legacy fields to the new database fields.

4.2.2.6.3. Definitions of Key Tables

Definitions of key tables, such as patient records, vaccination events, inventory, exemptions, and school roster modules will be included.

4.2.2.6.4. Mapping to CDC HL7 v2.5.1 Standards

Gainwell *Assist* is fully compliant with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, using SOAP-based transport by using the standard CDC WSDL. Gainwell *Assist* also supports flat-file import and vital records file submission.

It is built on the FHIR framework to deploy easily when CDC and AIRA publish an IIS FHIR Implementation Guide. We continually maintain and assess Gainwell *Assist*'s HL7 capability to provide conformity with the latest AART guidelines.

4.2.2.6.5. Versioning and Update Protocols for Schema Changes

Gainwell confirms versioning and update protocols will be performed for schema changes. Sample artifacts are available upon request and will be delivered during implementation in accordance with the approved Project Plan.

4.2.2.7. Oral Health Module

To advance the State's commitment to health equity, the IIS should include an Oral Health module that supports school-based dental screening, documentation, and reporting. This module is intended to reduce disparities in access to preventive oral health services, particularly among underserved student populations.

If provided, the module should include the following capabilities:

4.2.2.7.1. Roster Integration - Students should be linkable to schools via rosters, enabling targeted outreach and reporting by school, grade, and county. This supports identification of geographic and demographic gaps in oral health coverage.

4.2.2.7.2. Dual Workflows:

4.2.2.7.2.1. Dental Professionals should be able to enter administered oral health records directly into the IIS, ensuring timely documentation of care.

4.2.2.7.2.2. School Nurses should be able to enter historical records and manage rosters, supporting continuity of care and retrospective data entry.

4.2.2.7.3. Reporting Capabilities - The modules should support reporting that:

4.2.2.7.3.1. Identify students with or without oral health records.

4.2.2.7.3.2. Filters by urgency of care, school. Grade. And county to prioritize outreach and follow-up for high-need populations.

4.2.2.7.4. User Access and Permissions - The Oral Health module should leverage the system's role-based access control framework as defined in the HS Base Line Requirements RTM. Specifically:

4.2.2.7.4.1. Dental Professionals should be assigned appropriate roles and included in the provider dropdown menu.

4.2.2.7.4.2. School Nurses must be granted access to oral health reports and health service functionality.

4.2.2.7.4.3. The permissions "Enable Oral Health Reports" and "Enable Health Service" should be assignable individually or in bulk, using the system's master role update capability.

4.2.2.7.4.4. Jurisdictional administrators must be able to configure, modify, and inactivate roles and permissions in accordance with jurisdictional policies.

Gainwell fully supports the State's commitment to advancing health equity and reducing disparities in access to preventive oral health services.

Our IIS solution includes an optional Oral Health module designed specifically to strengthen school-based dental screening programs, improve documentation, and expand visibility into oral health needs across student populations, particularly those who have historically experienced

barriers to care. The module integrates seamlessly with the IIS and uses the same secure, role-based framework used across the platform.

4.2.2.7.1 Roster Integration

Gainwell's Oral Health module provides full roster integration, enabling students to be linked to their schools through automated or batch roster uploads. This functionality supports:

- Targeted outreach to students based on school, grade, county, or other demographic attributes
- Identification of geographic and population-specific gaps in oral health coverage
- Streamlined management of school-based screening events
- Improved continuity of care for students who move between schools or districts

This roster-based approach confirms that oral health data can be analyzed in the same equity-driven manner as immunization and other public health indicators.

4.2.2.7.2 Dual Workflows

Workflows are designed to integrate and automate processes across different modules, providing streamlined management and resolution of tasks and cases. They support both manual and automated interactions, enabling efficient and accurate handling of business processes.

Workflow Management. Gainwell *Assist* offers configurable workflows tailored to meet the specific needs of the State. The solution includes features such as error queues, budget reviews, approvals, and capitation adjustment processing tasks. The Workflow Manager employs a hierarchical, role-based approval process, routing electronic work objects through multiple system and user actions.

4.2.2.7.2.1 Dental Professional Workflow

Dental professionals can document administered oral health services directly within the IIS using a streamlined, role-specific workflow. This supports real-time entry of screenings, assessments, and preventive services, providing timely and accurate capture of care delivered during school-based or community events.

4.2.2.7.2.2 School Nurse Workflow

School nurses are provided with a dedicated workflow that enables them to:

- Enter historical oral health records
- Manage and update student rosters
- Support retrospective documentation for students who receive services outside school-based programs

This dual workflow design confirms both clinical and school-based personnel can contribute to a complete and accurate oral health record.

4.2.2.7.3 Reporting Capabilities

The Oral Health module consists of robust reporting tools that allow jurisdictions to monitor oral health outcomes and identify disparities across student populations. Reporting capabilities are outlined in the following sections.

4.2.2.7.3.1 Students With or Without Oral Health Records

Users can generate reports to identify students who have documented oral health screenings or services, as well as those who lack records. This process supports targeted outreach and follow up.

4.2.2.7.3.2 Filters for Urgency, School, Grade, and County

Reports can be filtered by:

- Urgency of care (e.g., immediate need, routine follow-up)
- School
- Grade
- County

These filters help prioritize outreach to high-need populations and support equity-focused program planning.

4.2.2.7.4 User Access and Permissions

Gainwell's Oral Health module uses the IIS' existing role-based access control (RBAC) framework, providing secure and appropriate access aligned with jurisdictional policies.

4.2.2.7.4.1 Dental Professional Roles

Dental professionals can be assigned appropriate roles and will appear in the provider dropdown menu for documentation and reporting purposes.

4.2.2.7.4.2 School Nurse Access

School nurses can be granted access to oral health reports and health service functionality, enabling them to manage rosters and enter historical records.

4.2.2.7.4.3 Assignable Permissions

Permissions such as "Enable Oral Health Reports" and "Enable Health Service" can be assigned individually or in bulk using the system's master role update capability, which simplifies administration across large school districts or provider networks.

4.2.2.7.4.4 Jurisdictional Control

Jurisdictional administrators maintain full authority to configure, modify, or inactivate roles and permissions following local policies and governance requirements.

The IIS will include an Oral Health module that supports school-based dental screening, documentation, and reporting. Role-based access controls allow you to determine who can use specific features, confirming access aligns with local policy and governance standards.

4.2.2.8. Next-Generation Interoperability with FHIR Standards

To support national interoperability initiatives, future system enhancements, and public health modernization, the OEPS seeks vendor commitment to advancing immunization data exchange through adoption of HL7 Fast Healthcare Interoperability Resources. While HL7 v2.5.1 remains the mandatory baseline, FHIR support provides increased flexibility, transparency, and scalability for secure, standards-based exchange of immunization data with IIS partners. Establishing a clear methodology and roadmap for FHIR adoption ensures the proposed solution can evolve alongside emerging federal and jurisdictional priorities.

The Vendor should describe their methodology for supporting the HL7 FHIR standard for immunization data exchange as an optional, innovative feature. The response should detail the following:

4.2.2.8.1. FHIR Standard Support: Which FHIR Release (e.g., R4) the system supports for public health, specifically for the electronic exchange of immunization data.

4.2.2.8.2. Required Resources: The Vendor should demonstrate capabilities for securely generating and receiving data using the HL7 FHIR Immunization resource, which represents vaccine administration events, and the HL7 FHIR Immunization Recommendation resource, which conveys patient-specific immunization forecasting and recommended actions. These resources must be implemented in alignment with the applicable FHIR Release (e.g., R4) to ensure consistency with national interoperability standards.

4.2.2.8.3. Roadmap and Timeline: A detailed plan, including a project roadmap and timeline, for the development and testing of FHIR-based data exchange capabilities. This should confirm FHIR support will be implemented as an addition to, or in parallel with, the existing mandatory HL7 v2.5.1 interfaces.

4.2.2.8.4. API Documentation: Confirmation that comprehensive, public-facing API documentation for all FHIR endpoints will be provided to the Agency and potential IIS partners.

At Gainwell, we develop solutions designed for interoperability, agility, and scalable delivery with a flexible architecture. Gainwell *Assist* provides integration services that are compatible with public, hybrid, and multi-cloud environments. Interoperability has become increasingly critical as the industry shifts to improve patients' access to their medical data. At the heart of our systems integration platform are real-time and near-real-time data exchanges, managed file transfer, SSO, and identity relationship management. Built-in enterprise architecture capabilities equip the State for current and future challenges. Our systems integration and interoperability offerings include:

- Interoperability/FHIR
- Electronic Data Interchange (EDI)
- Systems Integration (SI)

Gainwell *Assist* is fully compliant with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, using SOAP-based transport by using the standard CDC WSDL. Gainwell *Assist* also supports flat-file import and vital records file submission. It is built on the FHIR framework to deploy easily when CDC and AIRA publish an IIS FHIR Implementation Guide. We continually maintain and assess the Gainwell *Assist*'s HL7 capability to provide conformity with the latest AART guidelines.

Gainwell *Assist* leverages tools such as AART, CDC implementation guides, and staff participation in work groups such as Measurement for Assessment and Certification Advisory Workgroup (MACAW) and IZ Gateway to help in achieving HL7 standardization to be a valuable partner to the IZ Gateway project, CDC, and the State. We understand the roadmap for IZ Gateway and the other opportunities it will provide in federal reporting and cross-jurisdictional sharing efforts.

Gainwell *Assist* is built for efficient processing of 2.5 million daily HL7 messages, up to 500,000 daily HL7 VXU messages, and approximately two million HL7 QBP messages per day without performance degradation. Gainwell *Assist*'s built-in scalability makes it possible to scale to high volumes quickly with little to no configuration needed for spinning up additional instances of its various components to meet increasing demand from projected growth of transaction and data volumes, HL7 messages, and number of users.

Gainwell will work with the State to test and then redirect the anticipated 1,000 HL7 connections to the implemented modernized Gainwell *Assist* Solution.

4.2.2.8.1. FHIR Standard Support

FHIR is an evolving standard developed and maintained by HL7. Individual resources, such as immunization, are included in published FHIR specifications; however, many components have not yet reached normative status for the full range of use cases. As a result, finalized FHIR guidance for immunization scenarios continues to mature.

As part of the Gainwell *Assist* roadmap, we are committed to continuing to align with and implement applicable FHIR standards as they mature, verifying our COTS solution remains compliant; interoperable; and aligned with industry practices and support for public health.

4.2.2.8.2. Required Resources

Gainwell *Assist* exchanges data with health information systems in accordance with current interoperability standards endorsed by the CDC and follows AIRA's guidance for acknowledgement (ACK) messages. It fully complies with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging and supports multiple data exchange options, including Simple Object Access Protocol (SOAP)-based transport and flat-file import. Gainwell *Assist* is architected on the Fast Healthcare Interoperability Resources (FHIR) framework, providing compatibility with future deployments once CDC and AIRA publish an IIS FHIR Implementation Guide 2.

Gainwell *Assist* captures the Core Data Elements for IIS Functional Standards v5.0, along with the mandatory and optional requirements defined by the CDC and AIRA joint requirements traceability matrix (RTM). This includes capturing required Facility Identifier Data Elements and Provider Data Elements as part of the primary vaccination event record.

Our Product Team includes leaders with experience in state agencies responsible for immunization registries and who have strong relationships with the CDC and AIRA. Our long-standing working relationship with CMS and CDC highlight our ability to serve as a trusted integrator across public health and federal health initiatives. This experience uniquely positions us to support the State's IIS modernization in a broader health ecosystem.

4.2.2.8.3. Roadmap and Timeline

Gainwell will advance FHIR-based immunization data exchange through a phased roadmap aligned with the State's overall IIS implementation. FHIR will be implemented as an additive interoperability capability in parallel with the mandatory HL7 v2.5.1 interfaces. The mandatory HL7 interfaces will remain on the implementation critical path for initial IIS deployment, partner transition, and Agency Acceptance; availability of FHIR will not delay or disrupt migration of required HL7 interfaces.

The roadmap below is a non-confidential planning baseline. Detailed technical design, partner-specific sequencing, and final production activation dates will be refined with the Agency through the approved Project Plan and interoperability planning process.

Table 3. Gainwell Non-Confidential Planning Roadmap Baseline

Timing	FHIR Roadmap Activity	Development / Testing Outcome	Relationship to Mandatory HL7
Months 1–3 Standards & design baseline	Confirm FHIR release and profiles; validate Immunization and Immunization Recommendation use cases; define API security, authentication, terminology, data mapping, error handling, and documentation requirements.	Approved FHIR scope, use cases, design inputs, resource mappings, and preliminary test strategy.	HL7 inventory, ICDs, connectivity planning, and v2.5.1 migration proceed concurrently. Common patient, vaccination, provider, facility, and terminology mappings are reused.
Months 2–5 Configuration & development	Configure FHIR API services and mappings for supported immunization resources; establish endpoint security, validation rules, auditability, and versioning.	Unit-validated FHIR operations and resource mappings; draft API specifications.	FHIR development stays isolated from the required HL7 transition. HL7 VXU/QBP/RSP/ACK processing remains the mandatory baseline.
Months 4–7 Component & conformance testing	Exercise positive, negative, validation, authentication, terminology, and error scenarios with representative data; validate content against FHIR specifications and adopted guidance.	Conformance results with corrected defects; updated API documentation and test cases.	Where FHIR and HL7 carry equivalent data, results are compared against the common IIS data model to confirm consistent interpretation and quality.
Months 6–9 System & integration testing	Integrate FHIR services into the IIS test environment; run end-to-end functional, security, regression, interface, and performance testing; conduct partner testing when a FHIR-capable partner is available.	SIT results, interface reconciliation, security/performance evidence, defect remediation, and readiness recommendation.	Runs alongside mandatory HL7 interface and integration testing. Required HL7 interfaces must independently meet acceptance criteria.

Timing	FHIR Roadmap Activity	Development / Testing Outcome	Relationship to Mandatory HL7
Months 8–10 Agency validation / pilot	Support Agency UAT and, if agreed, a controlled FHIR pilot with capable IIS partners; validate Immunization and Immunization Recommendation workflows, documentation, and monitoring.	Validation results, partner feedback, resolved priority defects, and production-readiness assessment.	HL7 remains the authoritative exchange for partners outside the pilot. No partner must convert to FHIR for initial go-live.
Months 10–12 Production readiness & phased enablement	Complete operational readiness, API documentation, monitoring and support procedures, and release notes; promote approved FHIR capabilities per Agency approval and readiness criteria.	Versioned public API documentation, production-readiness evidence, and approved phased deployment plan.	Go-live and Acceptance depend on operational HL7 interfaces. FHIR activation may occur with or after base IIS deployment, per standards maturity and partner readiness.
Post go-live Standards evolution & expansion	Maintain FHIR capabilities as standards and CDC/AIRA guidance mature; expand use cases and onboard partners through controlled releases.	Updated endpoints, regression/conformance testing, versioned documentation, release notes, and partner onboarding.	HL7 v2.5.1 continues to support required and existing trading-partner exchanges as FHIR adoption grows with interoperability priorities.

Dependencies and Assumptions. FHIR delivery will be coordinated with the Agency's approved implementation schedule and will depend on: (1) availability and maturity of applicable CDC, AIRA, and HL7 FHIR guidance for IIS use cases; (2) agreement on the applicable FHIR release, profiles, terminology, and supported operations; (3) availability of Agency-approved development and test environments, security and authentication standards, and representative test data; (4) readiness and availability of any external partners selected for FHIR integration or pilot testing; and (5) completion of the underlying IIS data model, patient matching, forecasting, terminology, and interoperability functions used by both HL7 and FHIR exchanges. Changes in emerging national FHIR guidance will be addressed through the established governance and change management processes without reducing Gainwell's obligation to implement and maintain the mandatory HL7 v2.5.1 interfaces.

4.2.2.8.4. API Documentation

Gainwell confirms that comprehensive, public-facing API documentation for HL7 FHIR-based endpoints will be provided to the Agency and to potential IIS partners.

Our Immunization Solution is architected on a FHIR-ready framework and is designed to support future adoption of HL7 FHIR standards for immunization data exchange, consistent with emerging CDC and AIRA guidance.

As part of this commitment, Gainwell will make available full API documentation, including endpoint specifications, payload schemas, authentication requirements, sample request and response patterns, and error-handling guidance, for implemented FHIR Immunization and Immunization Recommendation resources. These materials will be delivered in a format suitable for both technical and non-technical stakeholders and will be accessible to authorized IIS partners to support integration, interoperability, and testing.

In addition, as Gainwell deploys FHIR capabilities in alignment with the project's roadmap, the Agency will receive up-to-date, versioned API documentation and release notes detailing enhancements, updates, and new endpoints. This verifies transparency, consistency, and ease of adoption for trading partners and system integrators throughout the lifecycle of the IIS.

4.2.3. Mandatory Project Requirements

The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. The Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

Gainwell affirms and acknowledges the above RFP requirements. The sections below outline our proposed approach and methodology to meeting the Mandatory Project Requirements.

4.2.3.1. Vendor Compliance Requirements

Vendors must ensure their proposed system meets all essential requirements outlined in Attachment B - HS Baseline Requirements RTM as required by the CDC. Vendors are required to provide a response to each field under the column labeled Vendor Response, including those related to optional functionality.

As part of the technical submission, Vendors must provide printed, bound physical copies of their completed RTM responses. The printed copies must include the following RTM pages:

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

Vendors are responsible for ensuring that the printed version is complete, legible, and organized in a manner that allows evaluators to readily verify compliance with each requirement.

Gainwell has completed the Requirements Traceability Matrix (RTM) and has provided printed copies in accordance with the RFP specifications.

The RTM includes detailed vendor responses describing how Gainwell Assist meets the mandatory requirements and, in several areas, provides additional capabilities aligned with the State's stated objectives. Summaries of these responses for each RTM section are provided below for reference.

4.2.3.1.1. Administer System

Gainwell's IIS provides a highly configurable platform that allows jurisdictions to manage organizational structures, update code sets, tailor enrollment workflows, and enforce data-quality rules. Integrated automation such as geocoding, real-time address validation, VTrckS inventory integration, and continuous CDSi/ACIP updates reduces manual work and improves accuracy. Robust role-based access, configurable alerts, and flexible search and reporting tools strengthen governance and usability.

4.2.3.1.2. Manage Organizations and Facilities

Gainwell's IIS offers a fully configurable enrollment and program-management workflow that streamlines provider onboarding through online enrollment with e-signature, automated form validation, and comprehensive notifications. Secure document-management tools support facility and VFC documentation, while flexible organization features enable activation, hierarchy management, multiple site IDs, contact updates, and address validation. The system also captures VFC coordinator details, training records, and storage plans, with automated controls that adjust ordering based on enrollment status.

4.2.3.1.3. Manage Users

Gainwell's IIS provides a secure, role-based user-management framework that allows authorized administrators to add, modify, inactivate, and reactivate user accounts; assign roles and permissions; switch organizational context; and issue account-status notifications, with actions fully audited. Configurable tools, including the Add/Edit Users interface and Role/Page Access matrix, support precise control of user access. The system incorporates SSO, MFA, temporary passwords, self-service resets, and expiration reminders aligned with jurisdictional security policies.

4.2.3.1.4. Support Interoperability

Gainwell's IIS provides a fully interoperable, standards-aligned framework that supports CDC HL7 2.5.1 messaging, SOAP/WSDL transport, FHIR-ready architecture, and integrations with the IZ Gateway, EHR systems, vital records, and VTrckS. The solution streamlines onboarding with credential issuance, transport validation, formatting checks, and edit/resubmit workflows, and offers dashboards to monitor VXU, QBP, ACK, and error trends. It supports bulk and real-time data exchange, deduplication, automated vital-records updates, and configurable exports for routine or emergency reporting. Strong analytics, error-handling, and flexible workflows provide scalable, CDC- and AIRA-aligned interoperability for day-to-day operations and mass-vaccination response.

4.2.3.1.5. Maintain Data Quality

Gainwell's IIS provides a comprehensive, configurable deduplication framework that uses scoring logic, phonetic matching, and customizable comparison fields to identify potential duplicate patient and vaccination records.

Authorized users can review matches on a centralized Patients Needing Review page, select retained data elements, perform quick-merge or manual merge/unmerge actions, and mark records as non-duplicates. The system preserves full audit history, retains pre-merged records, and issues warnings or HL7 ACK feedback when incoming events appear duplicative. Configurable match thresholds and mirrored logic for vaccination events further strengthen data quality and transparency.

4.2.3.1.6. Evaluate and Forecast

Gainwell's IIS provides fully automated, ACIP-compliant clinical decision support using CDC's CDSi logic, updated in near real time to generate accurate Child/Adolescent, Catch-up, and Adult forecasts. The system identifies due, overdue, future, and completed vaccines; incorporates contraindications, precautions, immunity evidence, and travel-related guidance; and allows jurisdictions to adjust CDS rules. It supports test-case creation and expected-vs-actual comparisons for UAT. Configurable reminder/recall tools and extensive coverage and quality-improvement reporting, aligned with CDC IQIP measures, further strengthen public-health workflows.

4.2.3.1.7. Manage Patient and Immunization Record

Gainwell's IIS delivers comprehensive, configurable functionality for managing patient and immunization records, including advanced search options, full support for CDC Core Data Elements, multi-name/address management, and address verification through Smarty. Users can add audited comments, manage cohort assignments, and apply facility- or jurisdiction-level status controls with bulk-update options. Immunization management supports adding, editing, and deleting events; capturing eligibility, funding, adverse reactions, refusals, and VAERS indicators; and enforcing lot-usage rules. The system also enables secure printing/export, multilingual outputs, and streamlined mass-vaccination workflows, providing a robust, policy-aligned patient-record management solution.

4.2.3.1.8. Manage Vaccine Inventory

Gainwell's IIS provides a fully integrated, automated vaccine inventory management module that supports ordering, tracking, reconciliation, returns, and wastage in alignment with CDC VTrckS and Vaccines for Children (VFC) requirements. The system maintains dose-level tracking, automates dose decrementing and shipment ingestion, and generates reorder recommendations based on usage and safety-stock rules. Jurisdictions can manage ordering permissions, allocations, transfers, and shipment verification, supported by robust alerts and dashboards for wastage, expirations, and accountability. Barcode scanning, offline/online mass-vaccination workflows, temperature-monitoring features, Role-Based Access Control (RBAC), and full audit logging confirm accuracy, security, and compliance across inventory operations.

4.2.3.1.9. Provide Data Access

Gainwell's IIS delivers a mature, scalable reporting and data-access framework that supports extensive standard reports and highly configurable ad hoc queries across major IIS functions,

with export options in CSV, Excel, and PDF. Users can filter, sort, schedule, drill down, and generate geographic or hierarchical reports using Federal Information Processing Standards (FIPS) codes and geocoded data. The system supports batch exports, de-identified Privacy-Preserving Record Linkage (PPRL) sharing, and consumer access to personal records and digital credentials.

Granular RBAC and comprehensive audit logging confirm secure, compliant access to reports and data elements, aligning with CDC, AIRA, HIPAA, and jurisdictional standards.

4.2.3.1.10. Non-functional

Gainwell's IIS provides a modern, cloud-hosted platform that meets non-functional requirements for performance, usability, reliability, security, maintainability, and portability. The system delivers fast response times, supports high-volume throughput, and maintains 99.9% availability through AWS multi-AZ redundancy. It offers Americans with Disabilities Act (ADA) and Web Content Accessibility Guidelines (WCAG) compliant usability, strong reliability with structured backup and recovery, and robust security through Multi-Factor Authentication (MFA), Single Sign-On (SSO), RBAC, encryption, and comprehensive audit logging. Configurable business rules, automated code-set updates, and modular architecture support maintainability, while responsive design and broad browser compatibility confirm portability.

4.2.3.2. System Compatibility Requirements

The IIS must be designed to operate reliably and efficiently within a variety of standard computing environments.

4.2.3.2.1. The IIS must be cloud based software with hosting provided by the vendor.

4.2.3.2.2. The IIS must be fully compatible with major, up-to-date web browsers including but not limited to Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari.

4.2.3.2.3. The IIS must operate efficiently on standard desktop and laptop computers without requiring specialized hardware or software installations.

4.2.3.2.4. The IIS must be accessible without requiring elevated user permission or local software installation. Only a supported web browser and internet access should be required for full functionality.

Gainwell's proposed Solution operates reliably, securely, and efficiently across a wide range of standard computing environments. Our Solution is fully cloud-based, scalable, and engineered to perform consistently without requiring specialized local hardware or elevated permissions.

4.2.3.2.1. Cloud Based Software

The IIS Solution is delivered as vendor-hosted, cloud-based software. The IIS solution is deployed within cloud environments that maintain FedRAMP Moderate or High authorization, consistent with State security requirements and the defined authorization boundary

Documentation confirming FedRAMP authorization for the hosting environment can be provided, including Authorization to Operate (ATO) documentation or the applicable listing on the FedRAMP Marketplace.

Hosting architecture follows Gainwell's enterprise information security policies and aligns with federal cybersecurity frameworks such as NIST SP 800-53 and FIPS-validated encryption requirements for protection of data at rest and in transit. The solution operates within U.S.-based data centers and supports the confidentiality, integrity, availability, and auditability controls required for systems processing protected health information and other sensitive data

4.2.3.2.2. Compatibility with Major, Up-to-Date Web Browsers

The proposed IIS Solution performs effectively across the following supported browsers: Microsoft Edge, Google Chrome, Mozilla Firefox, and Safari.

4.2.3.2.3. Operate Efficiently on Standard Desktop and Laptop Computers

Gainwell will work collaboratively with the State to configure and validate the Solution's integration, confirming compliance with security and access control requirements. Gainwell Assist does not require specialized hardware or software. The only requirement is the use of modern, up-to-date web browsers.

4.2.3.2.4. Accessible Without Elevated User Permission or Local Software Installation

As mentioned above, Gainwell will work collaboratively with the State to configure and validate the Solution's integration. This confirms compliance with security and access control requirements.

4.2.3.3. Service Level Agreement

Service levels, response times, resolution targets, and associated penalties shall be governed by the Service Level Agreement (SLA) provided as a separate attachment to this RFP. (Attachment C)

Gainwell affirms and acknowledges the above RFP requirement.

4.2.3.4. Maintenance and Support

The vendor shall provide annual maintenance and support services for all implemented system components, including software, databases, interfaces, and infrastructure. These services must include:

4.2.3.4.1. Help desk support available during standard business hours (Monday-Friday, 8:00 AM-5:00 PM local time), with documented escalation procedures.

4.2.3.4.2. Bug fixes and security patches delivered within industry-standard timeframes, with critical vulnerabilities addressed promptly.

4.2.3.4.3. System performance monitoring and proactive issue resolution for all hosted or managed environments.

4.2.3.4.4. Version upgrades and compatibility assurance for all vendor-supplied components, ensuring continued compliance with CDC and state interoperability standards.

4.2.3.4.5. Documentation updates reflecting any changes made during the maintenance period.

Gainwell will provide system support for the RFP-required elements, including:

- Near- and real-time data exchange capabilities and interactions with external systems occur in accordance with preferred method using CDC's WSDL.
- Compliance with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, using SOAP-based transport by using the standard CDC WSDL and IZ Gateway.
- Robust reporting and analytics capabilities allow for easy identification and exporting of results of errors for data submission.
- Patient demographic information is captured in accordance with Core Data Elements for IIS Functional Standards v5.0 and the mandatory and optional requirements of the joint CDC and PHII RTM.

- Maintaining a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an Immunization Solution record are created, viewed, or modified.

We will determine the best approach and interface protocol as we develop and document interface specifications with each external source system. Please refer to the RTM for more details on our proposed System Support.

4.2.3.4.1. Help Desk Support During Standard Business Hours

Gainwell's Level 2 help desk support is available Monday - Friday from 8:00 a.m. to 5:00 p.m. local time, with after hours from 5:00 p.m. to 10:00 p.m. local time for critical issues only. Our help desk support approach uses the capabilities of our cloud services, data services, computer networks, storage systems, telecom, software applications, and reporting systems to provide fast and accurate resolution to user technical questions and resolve problems in accordance with the State's performance standards.

4.2.3.4.2. Bug Fixes and Security Patches Delivered Within Industry-Standard Timeframes

We follow a formal change management process defined in our internal ISPS-010 – Change Management Standard, which requires system upgrades, including feature releases, patches, and security updates, be planned, documented, reviewed, and approved in partnership with the State. This verifies compatibility with operational requirements and minimizes service disruptions.

4.2.3.4.3. System Performance Monitoring and Proactive Issue Resolution

Gainwell uses the AWS Cloud environment, which is architected to deliver the uptime availability under its SLA. AWS achieves this through a highly resilient design that includes:

- Continuous monitoring and proactive incident response, which allow for early detection and rapid resolution of potential issues before they impact service delivery.
- Multiple AZs within each AWS region, each operating as an independent, physically separate data center with its own power, networking, and cooling. This confirms system continuity even in the event of localized disruptions.
- Redundant compute, storage, and networking resources, designed to eliminate downtime caused by component failure.
- Load balancing and automated failover mechanisms that seamlessly redirect workloads in case of disruption, delivering uninterrupted operations.
- Self-healing infrastructure that automatically adapts to fluctuations in demand and recovers from faults without human intervention.

Building on this foundation, we will apply our healthcare technology expertise and proven operational practices to extend AWS' reliability. The Gainwell team will configure, monitor, and manage these environments to meet or exceed the availability requirements of the State. Our approach combines AWS' resilient infrastructure with our robust governance, proactive performance monitoring, and healthcare-specific security and compliance framework.

4.2.3.4.4. Version Upgrades and Compatibility Assurance for Vendor-Supplied Components

The Gainwell team will work collaboratively with the State to determine the content, timing, and scheduling of system upgrades, including coordination of changes across development, test,

and production environments. As mentioned above, system upgrades, including feature releases, patches, and security updates, will be planned, documented, reviewed, and approved in partnership with the State.

4.2.3.4.5. Documentation Updates Reflecting Changes Made During the Maintenance Period

As mentioned above, we follow a formal change management process defined in our internal ISPS-010 – Change Management Standard, which requires system upgrades be documented.

4.2.3.5. Data Storage

The Vendor must store all IIS data - including backups, logs, and metadata - exclusively within data centers physically located in the continental United States of America (U.S.). No data may be transmitted, processed, or stored outside U.S. borders, including U.S. Territories, at any time, including but not limited to during disaster recovery, failover, or support operations. The Vendor must provide documentation verifying U.S.-based data residency and maintain compliance with applicable federal and state data protection laws and regulations.

4.2.3.5.1. Business Continuity and Disaster Recovery (BCP/DR): The Vendor must maintain a documented Business Continuity Plan and Disaster Recovery plan for the IIS environment. Requirements include:

4.2.3.5.1.1. Plan Documentation: Vendor shall provide copies of its BCP and DR plans to the Agency within 60 calendar days of contract execution and upon request thereafter.

4.2.3.5.1.2. NIST Alignment: Plans must be aligned with the most current version of NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems) or successor publications, throughout the contract term.

4.2.3.5.1.3. Annual Testing: Vendor must conduct annual BCP/DR testing (tabletop or live failover exercises) and provide a summary report of results, corrective actions, and remediation timelines to the Agency within 30 calendar days of test completion.

4.2.3.5.1.4. U.S. Data Residency: All BCP/DR activities, including backups, failover, and recovery operations, must comply with Section 4.2.3.5 data residency requirements (U.S.-based only).

4.2.3.5.1.5. Continuous Improvement: Vendor must update its BCP/DR plans within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment.

4.2.3.5.1.6. Certification: Vendor must annually certify to the Agency that its BCP/DR plans remain current, tested, and compliant with federal and state requirements.

The State's data and systems information, and the components and services associated with Gainwell's IIS delivered to the State, remain in the continental United States.

Gainwell Assist is deployed in **the East Region of AWS' cloud environment**. Security and compliance are foundational; we are compliant with **NIST 800-53 Rev. 5, SOC 2 Type 2, and HIPAA standards**. Our team's deployment across multiple AWS Availability Zones provides a resilient environment that guards against downtime and data loss.

Our solution is hosted in the AWS US East 1 (Virginia) primary data center, with our secondary data center in AWS US West 2 (Oregon).

4.2.3.5.1. Business Continuity and Disaster Recovery (BCP/DR)

In the following sections, Gainwell affirms that it meets the requirements of the RFP.

4.2.3.5.1.1. Plan Documentation

Gainwell affirms and acknowledges the above RFP requirement and agrees to provide copies of its Business Continuity Plan (BCP) and Disaster Recovery (DR) within 60 calendar days of contract execution.

4.2.3.5.1.2. NIST Alignment

Gainwell's continuity program follows HIPAA, NIST, CMS, Disaster Recovery Institute International (DRII), and other state and federal standards.

4.2.3.5.1.3. Annual Testing

Gainwell provides one annual DR exercise and one annual BC exercise. The assigned Gainwell DR Manager, along with the Gainwell account team, collaborate with the State to schedule the first exercises. Based on that initial date, they set the annual cadence for the subsequent exercises.

The systems and applications in scope for DR protection are in scope for the exercise. The State can, for exercises, set the scope to focus on specific applications or a subset of the whole IIS environment. The servers, databases, and applications in scope for recovery are recovered, validated, and then thoroughly tested with approved application test scripts. Testing evidence is gathered and provided along with the post-exercise summary report. The State is welcome to participate in the exercise and application testing if desired.

Aside from the one annual live exercise, the State may also request a tabletop exercise. Additional live and tabletop exercises may be requested at an additional cost.

The live DR exercise is conducted in a manner that isolates the DR environment so production will remain up and active and not be affected by the DR exercise. Gainwell provides an Exercise Scope and Objectives document to the State for approval before the exercise. Post-exercise activities include lessons-learned sessions, resolution of issues, Disaster Recovery Plan (DRP) updates as required, and providing the State with an Exercise Summary Report.

The DR and BC plans are also reviewed before exercises and updated if and as needed for currency and accuracy. They are reviewed again after the exercise and updated if and as needed based on the results of the exercise.

4.2.3.5.1.4. U.S. Data Residency

As mentioned above, the State's data and systems information, and the components and services associated with Gainwell's IIS delivered to the State, remain in the continental United States.

4.2.3.5.1.5. Continuous Improvement

Gainwell affirms and acknowledges the above RFP requirement.

4.2.3.5.1.6. Certification

Gainwell affirms and acknowledges the above RFP requirement.

The IIS establishes and tests recovery plans to mitigate system downtime through a comprehensive Business Continuity/Disaster Recovery (BC/DR) framework. This framework complies with NIST SP 800-34 Contingency Planning Guide for Federal Information Systems standards. Key elements of this framework include:

- **Disaster Recovery Environment.** The system provides a DR environment in the AWS East region with Availability Zones for resiliency. This confirms system resiliency and the recovery strategy used to achieve the 24-hour recovery time objective (RTO) and one-hour recovery point objective (RPO).
- **BC/DR Plan.** A BC/DR Plan is provided, identifying core business processes included in the Gainwell Assist Solution in accordance with the State's requirements. This plan supports recovery of critical services and includes a notification process in case of a disaster. The plan is updated at least annually to incorporate new functionality.
- **BC/DR Testing.** Testing of the BC/DR Plan is supported as part of operational readiness and conducted annually to demonstrate compliance with SLAs. Coordination with the State is done to identify DR test dates. During testing, collaboration occurs with State partners to validate connectivity and interoperability for integrated applications. Lessons learned are tracked and contribute to the Continuous Improvement Plan.
- **Backup and Restore Procedures.** Gainwell's procedures for backing up and restoring data in the AWS Cloud support the State's backup and retention requirements in accordance with SLAs.

4.2.3.6. Data Ownership

4.2.3.6.1. The vendor must agree that the Agency retains full ownership of all data.

4.2.3.6.2. The Vendor must agree that all data related to the execution of the contract is collected on behalf of, and remains the sole property of, the Agency.

4.2.3.6.3. The Vendor must agree to provide privacy and security safeguards to protect all data from any use or disclosure for any purpose other than the described within this solicitation.

4.2.3.6.4. The Vendor must return the entire dataset in a specified format upon request or contract termination at no additional cost and in a format specified by the Agency to ensure usability and accessibility.

4.2.3.6.5. The Vendor must cooperate with the Agency and any subsequent Vendor should the contract, which is the subject of this RFP, be terminated, and to deliver any and 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.

4.2.3.6.6. The Vendor must destroy all data in the System at the end of the contract and/or upon the request of the Agency in accordance with the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-88. Destruction of data shall not begin prior to receipt of written authorization from the Agency Project Manager and must be completed within 30 days of receipt of that authorization.

4.2.3.6.1. The Agency Retains Full Ownership of Data

State data is owned by the State and will remain the property of the State. Gainwell is permitted to use such State data solely for the purposes set forth in the contract and for no other purpose. At no time will Gainwell access, use, or disclose State data for a purpose except as expressly and specifically agreed to in writing by the State.

4.2.3.6.2. Data Related to the Execution of the Contract is Collected on Behalf of, and Remains the Sole Property of, the Agency

Gainwell agrees that data related to the execution of this contract is collected solely on behalf of the Agency and remains the exclusive property of the Agency. Gainwell acknowledges that it does not obtain, retain, or assert ownership or proprietary interest in such data.

4.2.3.6.3. Provide Privacy and Security Safeguards to Protect Data

Gainwell agrees to provide comprehensive privacy and security safeguards to protect Agency data from use or disclosure for a purpose other than those expressly described in this solicitation and the resulting contract. Our commitments include the following controls and practices:

- **Security Governance and Compliance.** We maintain an enterprise security program aligned to HIPAA, NIST 800-53, and SOC 2 Type 2, and operate our SaaS solution within an AWS environment designed and managed against these standards. This framework governs access control, data protection, incident response, auditability, and continuous monitoring.
- **Least-Privilege, Role-Based Access, and Strong Authentication.** Access to systems and data is restricted by RBAC and the principle of least privilege, enforced with Single Sign-On (SAML/OAuth 2.0) and MFA. User permissions are reviewed regularly; inactive or unauthorized accounts are promptly inactivated.
- **Encryption of Data in Transit and at Rest.** Confidential data is encrypted using industry-standard cryptography (e.g., AES-256) at rest and Transport Layer Security (TLS) in transit to prevent unauthorized disclosure or alteration.
- **Monitoring, Logging, and Auditability.** We employ continuous monitoring and centralized logging (e.g., CloudWatch/CloudTrail/SIEM) to detect anomalous activity, provide traceability, and support investigations. Audit logs record access and changes to data and are retained per policy.

4.2.3.6.4. Return Dataset in a Specified Format Upon Request or Contract Termination

Gainwell will return the Agency's full dataset upon request or at contract termination at no additional cost. Data will be delivered in the format specified by the Agency to allow continued usability, accessibility, and seamless transition.

4.2.3.6.5. Cooperation with the Agency and Subsequent Vendor

Gainwell will fully cooperate with the Agency and subsequent vendor in the event of contract termination. We will deliver required data, documentation, and work products to the Agency or its designated recipient within thirty working days of receiving notice of termination, providing a smooth and timely transition at no additional cost.

4.2.3.6.6. Destruction of Data in the System at the End of the Contract

The Gainwell team follows the State's internal Media Sanitization Standard (ISPS-004), which aligns with NIST SP 800-88 Revision 1. Electronic media containing Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry (PCI), Criminal Justice Information (CJI), or other sensitive data is subject to secure sanitization or destruction before disposal. Sanitization methods may include cryptographic erasure, degaussing, or physical destruction, depending on the media type and data classification.

We will work with the State to define acceptable forms of disposal documentation. This may include a Certificate of Media Disposal, third-party attestation, or chain-of-custody documentation, depending on the media type and disposal method. Records of media sanitization events will be retained according to our internal retention policy and the State's contractual requirements.

4.2.3.7. General Project Requirement

Vendor must host an initial planning session(s) with the Agency within 30 days after project start date, with the goal to finalize the project plan and schedule.

4.2.3.7.1. The Vendor's finalized Project Plan and Schedule must adhere to the Implementation Plan proposed in Section 4.2.2.2, subject to Agency review and approval.

4.2.3.7.2. Any deviation from the proposed Implementation Plan must be documented, justified, and approved by the Agency.

4.2.3.7.3. The Vendor shall not assess, invoice, or otherwise charge the Agency for any fees, including but not limited to annual licensing, subscription, hosting, maintenance, or support fees, during the Implementation Period. Payment for implementation services shall be tied to the successful completion of mutually agreed-upon implementation milestones established during the initial planning sessions and incorporated into the approved Project Plan. No milestone payment shall be due until the Agency has verified and approved completion of the corresponding milestone. Final implementation payment shall be made only upon the Agency's formal written Acceptance of the fully implemented IIS solution, as defined in Section "Acceptance Criteria." No recurring or annual fees shall begin or accrue until the system has been fully implemented, operational, and accepted by the Agency.

4.2.3.7.3.1. Milestone Definition and Approval: All implementation milestones must be jointly developed during the initial planning sessions and incorporated into the Vendor's Project Plan. Each milestone must include:

4.2.3.7.3.1.1. A clear description of required deliverables

4.2.3.7.3.1.2. Objective acceptance criteria

4.2.3.7.3.1.3. Documentation requirements

4.2.3.7.3.1.4. A proposed payment amount tied to that milestone.

4.2.3.7.3.2. No Unilateral Changes: The Vendor may not add, remove, modify, subdivide, or consolidate milestones without the Agency's prior written approval. Any attempt to alter milestone definitions or payment amounts without approval is void and unenforceable.

4.2.3.7.3.3. Verification Before Payments: No milestone payment shall be due until the Agency verifies that all deliverables and acceptance criteria associated with that milestone have been fully met. Verification shall be documented in writing by the Agency.

4.2.3.7.3.4. No Partial or Conditional Payments: The Agency will not issue partial payments for partially completed milestones. Milestone payments are all-or-nothing and contingent upon full completion and Agency approval.

4.2.3.7.3.5. No Recurring Fees Before Final Acceptance: Regardless of milestone progress, annual, recurring, subscription, hosting, maintenance, or support fees will not begin or accrue until the Agency issues formal written Acceptance of the fully implemented IIS solution.

4.2.3.7.3.6. Milestone Failure and Remediation: If the Vendor fails to meet a milestone, the Agency may issue a Notice of Deficiency. The Vendor must remediate all deficiencies at no additional cost and resubmit the milestone for Agency verification. The Agency may repeat any testing or review necessary to confirm remediation.

4.2.3.7.4. Liquidated Damages for Implementation Delays: The Agency reserves the right to assess liquidated damages if the Vendor fails to meet any mutually agreed-upon implementation milestone by the approved milestone due date. In such cases, the Agency may assess liquidated damages in the amount of \$500.00 per calendar day until the milestone is completed and verified by the Agency. For delays in achieving final system Acceptance, the Agency may assess liquidated damages at a rate of \$1,000.00 per calendar day. Total liquidated damages shall not exceed ten percent (10%) of the total implementation costs.

Milestones are not valid until formally approved in writing by the Agency.

Gainwell affirms and acknowledges the RFP requirement. During the planning phase, the Gainwell Team refines and publishes an updated Project Management Plan (PMP) and Project Work Plan in collaboration with the State. Gainwell will host the initial planning session(s) with the Agency within 30 days after the project start date.

We also collaborate with the State to develop and finalize other planning deliverables, such as a comprehensive RTM containing solution requirements confirmed by the State.

4.2.3.7.1. Project Plan and Schedule to Adhere to the Implementation Plan

Gainwell affirms and acknowledges the RFP requirement. The PMP and Schedule will adhere to the proposed Implementation Plan and will be developed in collaboration with the State.

4.2.3.7.2. Deviation from Proposed Implementation Plan

As mentioned above, the PMP and Schedule will adhere to the proposed Implementation Plan and will be developed in collaboration with the State.

4.2.3.7.3. No Assessment, Invoice, or Other Charge the Agency for Fees

Gainwell agrees to this requirement. We will not charge fees during the Implementation Period, and payments will be tied solely to Agency-approved milestone completion. No recurring or annual fees will begin until the system is fully implemented, operational, and formally accepted by the Agency.

4.2.3.7.3.1. Milestone Definition and Approval including 4.2.3.7.3.1.2 – 4.2.3.7.3.1.4

Milestone Governance and Approval. The foregoing milestone schedule represents Gainwell's proposed implementation baseline and will be jointly reviewed and finalized with the Agency during the initial planning session(s), which will occur within 30 calendar days after the Project Start Date. The finalized Project Plan and Schedule will adhere to the Implementation Plan proposed in Section 4.2.2.2 and will be subject to Agency review and written approval. Any subsequent modification to a milestone, deliverable, acceptance criterion, documentation requirement, schedule date, or payment amount will require the Agency's prior written approval.

Milestone Acceptance and Payment. Each implementation milestone will include a clear description of required deliverables, objective acceptance criteria, supporting documentation requirements, and a milestone-specific proposed payment amount. Milestones are not valid until formally approved in writing by the Agency. No milestone payment will become due until all associated deliverables and acceptance criteria have been fully satisfied and completion has been verified and approved in writing by the Agency. No partial or conditional milestone payments will be requested. Final implementation payment will be contingent upon the Agency's formal written Acceptance of the fully implemented IIS solution.

Table 1. Gainwell's Milestone Schedule

Milestone	Target Schedule	Required Deliverables	Objective Acceptance Criteria	Required Documentation / Evidence	Proposed Payment Amount
M1 – Project Initiation, Planning & Baseline Approval	Project Start – Day 30 / Month 1	Kickoff and initial planning sessions; finalized Project Management Plan (PMP); integrated Project Work Plan and Schedule; governance structure; staffing plan; communications plan; RAID management approach; initial RTM; milestone/payment baseline	Initial planning session(s) completed within 30 days of project start; PMP and schedule align to the proposed Implementation Plan; roles, dependencies, governance, milestones and acceptance process agreed; Agency comments resolved; Agency provides written approval	Approved PMP; baseline schedule; meeting minutes; governance plan; staffing plan; communications plan; RAID log; RTM baseline; Agency approval record	TBD – milestone-specific amount established in Cost Proposal / approved Project Plan
M2 – Requirements Validation, Solution Design & Environment Readiness	Months 1–3	Validated requirements/RTM; solution design; configuration specifications; workflow designs; interface inventory; security architecture; Production/Test/Development environment setup; environment readiness confirmation	Requirements traceable to RFP/RTM; designs address approved State workflows; required environments provisioned and accessible; security and configuration reviews completed; no unresolved critical design issues preventing configuration	Updated RTM; requirements documentation; design specifications; architecture diagrams; workflow documentation; environment configuration records; security review evidence; design-review minutes/signoff	TBD – Agency-approved milestone amount

Milestone	Target Schedule	Required Deliverables	Objective Acceptance Criteria	Required Documentation / Evidence	Proposed Payment Amount
M3 – Core System Configuration & Initial Demonstration	Months 2–5	Configured Gainwell Assist solution; State-specific workflows/business rules; user roles and permissions; core reporting configuration; configured functional modules; sprint demonstrations	Approved requirements assigned to the milestone are configured; configuration passes Gainwell QA/unit validation; demonstrations completed with State; material findings resolved or entered into approved issue/change process	Configuration workbook/log; demonstration records; sprint results; test evidence; updated RTM; configuration documentation; issue/change log; Agency approval	TBD – Agency-approved milestone amount
M4 – Data Migration & Conversion Readiness	Months 3–7	Data conversion/migration plan; source-to-target mappings; ETL processes; mock conversion(s); data-cleansing results; reconciliation reports; migration defect resolution; production migration/runbook	Required source data successfully converted in test environment; reconciliation thresholds agreed with Agency and achieved; critical/high migration defects resolved; migrated data demonstrated as complete, accurate and usable for downstream testing	Data Migration Plan; mapping documents; ETL specifications; mock conversion reports; reconciliation reports; defect logs; data quality results; migration runbook; Agency validation/signoff	TBD – Agency-approved milestone amount
M5 – Interface Development, Integration &	Months 3–8	Required HL7/interfaces; interface specifications/ICDs; connectivity configuration; interface test cases; external	Required interfaces successfully exchange data in applicable test	ICDs/interface specifications; connectivity records; interface test results;	TBD – Agency-approved milestone amount

Milestone	Target Schedule	Required Deliverables	Objective Acceptance Criteria	Required Documentation / Evidence	Proposed Payment Amount
Interoperability Readiness		system integration; data exchange monitoring; interface reconciliation	environments; messages meet approved specifications; error/ACK processing validated; critical/high interoperability defects resolved; Agency-designated interface testing completed	message validation results; defect/retest evidence; monitoring evidence; updated RTM; Agency approval	
M6 – System & Integration Testing Complete	Months 6–9	Test Management Plan execution; functional testing; system testing; integration/interface testing; regression testing; accessibility testing; security testing; performance/load testing as applicable; resolved defects	Approved test cases executed; agreed pass-rate achieved; all Critical/High defects within milestone scope resolved; remaining lower-severity defects do not materially prevent UAT; traceability demonstrates requirements have been tested	Test Management Plan; test scripts/cases; execution results; requirements traceability; defect reports; retest evidence; performance/security results; test-completion report; Agency acceptance	TBD – Agency-approved milestone amount
M7 – UAT Readiness & User Acceptance Testing	Months 8–10	UAT environment; UAT plan; test scenarios/cases; migrated test data; State UAT support; defect triage; corrected/retested items; UAT completion package	Agency-designated users complete UAT; required workflows validated; Critical/High UAT defects resolved; corrections successfully retested; Agency	UAT Plan; test cases; participant records; test results; defect and resolution log; retest evidence; UAT status reporting; written UAT approval	TBD – Agency-approved milestone amount

Milestone	Target Schedule	Required Deliverables	Objective Acceptance Criteria	Required Documentation / Evidence	Proposed Payment Amount
			confirms UAT completion/signoff		
M8 – Training, Knowledge Transfer & Operational Readiness	Begin no later than 90 days before Go-Live; Months 9–11	Role-based Training Plan; administrator training; provider/end-user training; school nurse/public-health partner training; train-the-trainer activities; digital user guides/manuals; on-demand materials; knowledge-transfer activities; Operational Readiness Review (ORR)	Training begins 90 days before planned Go-Live; required training audiences addressed; materials delivered; operational support functions demonstrate readiness; ORR completed; material readiness issues resolved; go/no-go recommendation issued	Training Plan; curricula; user guides; training materials; attendance/completion records; knowledge-transfer documentation; ORR checklist/report; readiness issue log; go-live recommendation	TBD – Agency-approved milestone amount
M9 – Production Cutover & Go-Live	Target: Month 11	Approved cutover plan; final production migration; production interfaces; production configuration; user access; support/help-desk activation; go-live communications; production deployment; hypercare initiation	Cutover activities completed successfully; production solution available; required interfaces operational; migrated data validated; security/access controls operational; no unresolved issue prevents safe production use; Agency authorizes Go-Live	Approved cutover plan; deployment logs; production migration report; production validation results; interface validation; security/access checklist; go-live issue log; Agency Go-Live authorization	TBD – Agency-approved milestone amount
M10 – Stabilization &	Months 11–12; Final Acceptance by end of Month	Stabilization/hypercare; production defect remediation; performance monitoring;	Solution operates in production for the mutually agreed	Stabilization reports; defect/retest records; SLA/performance results;	Final implementation payment – TBD;

Milestone	Target Schedule	Required Deliverables	Objective Acceptance Criteria	Required Documentation / Evidence	Proposed Payment Amount
Final Acceptance	12, subject to Agency verification	operational transition; final documentation; architecture/configuration guides; training materials; administrative procedures; final RTM; contractual reporting; final implementation acceptance package	stabilization period without material errors; Critical/High defects resolved; interfaces operate accurately; security controls validated; required documentation delivered; all contractual implementation deliverables completed; Agency issues written Notice of Acceptance	final RTM; final configuration and architecture documentation; user/admin manuals; contractual reports; implementation completion report; Agency Notice of Acceptance	payable only after formal written Acceptance

Milestones developed through this process are not considered valid or actionable until formally approved in writing by the Agency, and no work or billing against a milestone will proceed without the Agency's explicit written approval.

4.2.3.7.3.2. No Unilateral Changes

Gainwell affirms and fully accepts this requirement. We agree that implementation milestones may only be changed with the Agency's prior written approval. Gainwell will not add, remove, modify, subdivide, or consolidate milestone without such approval, and we acknowledge that attempt to alter milestones or payment terms without written authorization from the Agency is void and unenforceable.

We will maintain strict change-control discipline and confirm that milestone-related updates are documented, jointly reviewed, and formally approved by the Agency before implementation.

4.2.3.7.3.3. Verification Before Payments

Gainwell affirms and fully accepts this requirement.

4.2.3.7.3.4. No Partial or Conditional Payments

Gainwell affirms and fully accepts this requirement.

4.2.3.7.3.5. No Recurring Fees Before Final Acceptance

Gainwell affirms and fully accepts this requirement.

4.2.3.7.3.6. Milestone Failure and Remediation

Gainwell affirms and fully accepts this requirement.

4.2.3.7.4. Liquidated Damages for Implementation Delays

Gainwell affirms and acknowledges the RFP requirement regarding Liquidated Damages for Implementation Delays.

4.2.3.8. Vendor Staffing

The awarded Vendor will provide staffing resources to successfully complete the implementation tasks, including system configuration, customization, testing, training, and go-live support tasks to meet Agency requirements. The Vendor's internal policies and procedures for hiring must comply with:

4.2.3.8.1. WV Office of Technology Policies (<https://technology.wv.gov/policy-governance/ot-policies>)

4.2.3.8.2. Agency Office of Shared Administration the Office of Management Information Services (OMIS) Policy #0529 (Attachment D): Vendor/Contractor Employee Background Check Policy)

4.2.3.8.3. OMIS Procedure #OP-35 (Attachment E): Vendor/Contractor Employee Background Check Procedure), and Appendix A (Attachment F)

Gainwell's PMP will contain a Project Staffing Plan detailing staff responsibilities including time commitments, qualifications, and specific relevant experience required. The State requires an expert staffing strategy to complete the requirements of the RFP. It is crucial that a vendor's team offers:

- Deep technical knowledge in COTS-based solution implementation
- Proven experience in delivering an IIS solution on time
- A work ethic that produces efficiencies through day-to-day collaboration

Gainwell team members bring valuable qualities and skills to the project. We have worked diligently so our staffing solution recognizes the value and specific needs of each person. Our solution incorporates communication activities, knowledge transfer, organizational change, retention, learning, and development. Our staffing strategy is outlined in the following pages. We offer:

- Technical expertise in developing and operating healthcare solutions.
- A team of IIS professionals who deliver solutions on time. The team we bring to the State comprises healthcare professionals with expertise in each aspect of the requirements detailed in the RFP.
- A workplace culture that strengthens the State's commitment to collaboration and transparency. Our team will work side by side with the State to fully understand both the benefits and challenges of the system in place today, which best facilitates the Gainwell team to deliver exactly what the State needs. This understanding brings continuity to the proposed Solution and minimizes disruptions.

Descriptions of our proposed staff roles are given in the following table.

Table 4. Proposed Staff Roles

Role	Skills and Responsibilities
Account General Manager	• Develops and cultivates strong customer relationships at the State executive level • Accountable for overall customer delivery to the State • Acts as the primary point of contact (POC) with the State for activities related to contract administration, including being able to legally bind Gainwell with State agreements • Provides oversight and management for account leadership for this contract • Identifies digital transformation ideas and methods of providing services to respond to changing strategies and regulations
Project Manager	• Verifies that maintenance and operations groups provide support as contractually required • Serves as primary daily contact to interact with the State's IIS Manager and project team; facilitates and prepares materials for weekly status meetings • Keeps the State's IIS Manager informed of interactions with State staff and escalates issues to the Gainwell Account General Manager and executive team • Delivers contract performance measures, reporting and tracking documents, and other documents to State-authorized personnel, as required • Verifies that deliverables are developed and submitted as required and obtains State approval for contractual deliverables • Manages the project scope to confirm deliverables meet the definition as approved by the State • Manages the project using the approved project management methodology and system lifecycle • Maintains the project repository including project work plan, issues list, and project deliverables • Manages the delivery of Tier 2, Tier 3, and Emergency level Help Desk support beginning with go-live and continuing throughout the duration of the contract

Role	Skills and Responsibilities
	• Provides transition support during the Design, Development, and Implementation (DDI) phase of the modernized Immunization Solution • Manages and tracks activities during the development, testing, and implementation phases for the new Immunization Solution • Delivers contract performance measures, reporting and tracking documents, and other documents to State-authorized personnel, as required • Verifies that deliverables are developed and submitted as required and obtains State approval for contractual deliverables • Manages the project scope to confirm deliverables meet the definition as approved by the State • Maintains the project repository including project work plan, issues list, and project deliverables
Technical Lead/ Developer	• Reviews coding and design changes to verify adherence to project standards • Leads the technical design for changes and configurations • Verifies that design, construction, and unit testing of developers meets Gainwell standards • Updates technical support documentation required for changes and configurations assigned • Participates in application walkthroughs as requested • Reviews requirement documents and test plans for understanding and accuracy, including working with the lead business analyst to answer questions or make modifications when needed • Provides Tier 2 and Tier 3 support for known technical problems and issues as reported by Help Desk technicians • Conducts peer review design walkthroughs and peer code review walkthroughs for work assigned • Provides transition support during the Maintenance and Operations (M&O) phase of the modernized Immunization Solution
Account Delivery Lead	• Responsible for customer delivery to the State • Oversees issue resolution and project scope changes • Provides oversight and management for delivery of services for this contract
Chief Security Engineer	• Provides security and compliance expertise, direction, and leadership • Works with Gainwell leadership to identify and establish applicable compliance requirements • Provides recommendations on security staffing and resources • Oversees completion of relevant work products and documentation • Establishes and designs the necessary end-to-end security controls for the account • Makes sure compliance with policies and security standards is followed, as spelled out in the contract • Works with the Gainwell Security Practice to identify gaps in the operating model and available controls and capabilities when compared to the established compliance requirements • Provides specific technical expertise, direction, and leadership to implementation team for specific tasks

Role	Skills and Responsibilities
	• Provides information, strategies, and guidance on security and privacy-related technologies, methods, and tools for the project team • Coordinates with other project security resources and account-level security resources, such as Security Team and project managers, to confirm execution plans are progressed • Tracks progress of execution activities and milestones related to security compliance across in-scope accounts and provides guidance when appropriate • Provides specific technical expertise, direction, and leadership to other project team members as it relates to a compliance requirement or deliverables for the project • Evaluates the proposed capabilities and deliverables by verifying them against existing standards and procedures
Account Infrastructure Lead	• Defines and enables the tools and services to be implemented in Gainwell's cloud infrastructure • Performs scans and audits of cloud infrastructure to verify compliance with standards and performance requirements • Remediates findings of scanning and auditing processes
Director of Product	• Monitors and evaluates product progress at each stage of the process • Consults with the Product team and Delivery team • Defines the vision for the team's product • Creates a product roadmap based on this vision
Product Advisor / Project Manager	• Transforms data management processes to enhance data integrity • Implements Lean methodologies to streamline workflows and eliminate process waste • Works closely with marketing, sales, and engineering to confirm business case and customer satisfaction goals are met
Principal Application Architect	• Reviews coding and design changes to verify adherence to project standards • Performs technical design for changes and configurations • Confirms that design, construction, and unit testing meet Gainwell standards • Participates in application walkthroughs as requested • Reviews requirement documents and test plans for understanding and accuracy, including working with business analysts to answer questions or make modifications when needed • Provides support for known technical problems and issues • Participates in peer review design walkthroughs and peer code review walkthroughs for work assigned
Developers	• Reviews coding and design changes to verify adherence to project standards • Performs technical design for changes and configurations • Confirms that design, construction, and unit testing meet Gainwell standards • Participates in application walkthroughs as requested • Reviews requirement documents and test plans for understanding and accuracy, including working with business analysts to answer questions or make modifications when needed • Provides support for known technical problems and issues

Role	Skills and Responsibilities
	• Participates in peer review design walkthroughs and peer code review walkthroughs for work assigned
Business Analysts	• Develops and submits deliverables as contract requires and Gainwell Project Manager directs • Consults with customers to elicit and document requirements and design screen mockups • Meets the project schedule and milestones as defined in the work plan and the contract • Confirms that design and system testing meet Gainwell standards • Successfully completes testing as assigned and verify that testing meets Gainwell standards • Appropriately reports and records environment or application issues found • Executes testing and walkthroughs for work assigned • Conducts application walkthroughs with the State, as required • Completes and updates design documents, test plans, and other documentation, as prioritized
Database Administrator	• Verifies that databases and data dictionaries are updated according to specified schedules • Works with team members to resolve database questions or problems • Creates and maintains database schema definitions, performance tuning procedures, and capacity planning • Collaborates with other systems and operations units to maximize the value of the data and determine the impact of changes on the project • Coordinates systems resource availability with database analysts, system and application developers, and other users • Maintains industry-recognized policies, procedures, and standards relating to database management
Business Analyst / Trainer	• Assists with development of the Gainwell Training Plan under the guidance of the Project Manager • Assists with training needs assessment and other training planning activities • Develops training materials in coordination with Gainwell Product Team and Account Team • Conducts in-person and remote instructor-led training, including providing Train-the-Trainer training to designated State personnel
Help Desk Support Specialist	• Coordinates with the State's Division Help Desk and Vaccine Systems Unit for the hand-off of service requests from the State to Gainwell • Provides support for timely resolution of Immunization Solution related service requests escalated from the State • Logs, tracks, and monitors Help Desk service requests within the designated tracking tool

4.2.3.8.1. West Virginia Office of Technology Policies

Gainwell affirms that its hiring policies and procedures comply with the West Virginia Office of Technology Policies.

4.2.3.8.2. Agency Office of Shared Administration the Office of Management Information Services (OMIS) Policy #0529

Gainwell affirms it will comply with OMIS Policy #0529.

4.2.3.8.3. OMIS Procedure #OP-35

Gainwell will partner with West Virginia and follow the process outlined in OMIS Procedure OP-35, OMIS Vendor and Contractor Employee Background Check Process while adhering to applicable laws, regulations, and client policies.

4.2.3.9. Project Manager

The awarded Vendor will provide a project manager, and the Agency will engage a project manager during the system implementation phase.

Gainwell affirms it will provide a dedicated Project Manager to lead and coordinate implementation activities, and acknowledges that the Agency will also engage the Project Manager during the system implementation phase. As mentioned above, the skills and responsibilities of our proposed Project Manager will be as follows:

- Verifies that maintenance and operations groups provide support as contractually required
- Serves as primary daily contact to interact with the State's IIS Manager and project team; facilitates and prepares materials for weekly status meetings
- Keeps the State's IIS Manager informed of interactions with State staff and escalates issues to the Gainwell Account General Manager and executive team
- Delivers contract performance measures, reporting and tracking documents, and other documents to State-authorized personnel, as required
- Verifies that deliverables are developed and submitted as required and obtains State approval for contractual deliverables
- Manages the project scope to confirm deliverables meet the definition as approved by the State
- Manages the project using the approved project management methodology and system life cycle
- Maintains the project repository including project work plan, issues list, and project deliverables
- Manages the delivery of Tier 2, Tier 3, and Emergency level Help Desk support beginning with go-live and continuing throughout the duration of the contract
- Provides transition support during the DDI phase of the modernized Immunization Solution
- Manages and tracks activities during the development, testing, and implementation phases for the new Immunization Solution
- Delivers contract performance measures, reporting and tracking documents, and other documents to State-authorized personnel, as required
- Verifies that deliverables are developed and submitted as required and obtains State approval for contractual deliverables

- Manages the project scope to confirm deliverables meet the definition as approved by the State
- Maintains the project repository including project work plan, issues list, and project deliverables

4.2.3.10. Comprehensive and Role-Specific Training Plan

The awarded Vendor must not only provide training materials but also submit a comprehensive, documented training plan. The goal is to ensure all user groups achieve full proficiency and maintain it throughout the contract term.

The Vendor's response must include and detail the following mandatory requirements:

4.2.3.10.1. Role-Specific Training Strategy: The Vendor shall propose a detailed training plan tailored to the distinct needs and responsibilities of the following primary user roles (at minimum):

4.2.3.10.1.1. OEPS I Agency Administrator: Focus on system configuration, data quality monitoring, advanced reporting, and system maintenance tasks.

4.2.3.10.1.2. Provider Office Staff/ End-Users: Focus on day-to-day data entry, search/query functions, clinical decision support usage, and basic troubleshooting.

4.2.3.10.1.3. School Nurses/ Public Health Partners: Focus on roster management, exemption tracking, and public health follow-up workflows.

4.2.3.10.2. Training Deliverables: The Vendor must provide current, digital, and user-specific training resources, including but not limited to:

4.2.3.10.2.1. Training Deliverables: The Vendor must provide current, digital, and user-specific training resources, including but not limited to:

4.2.3.10.2.1.1. On-demand video instructions or demonstrations for each user role.

4.2.3.10.2.1.2. Digital user guides or manuals for both functional and technical reference.

Gainwell will deliver a comprehensive, fully documented, and role-specific Training Plan designed to confirm each IIS user group achieves and sustains system proficiency throughout the life of the contract. Our approach integrates structured training development, multi-format delivery, user readiness validation, and ongoing support mechanisms. Gainwell's Training Plan exceeds the requirement by providing a structured, repeatable, and long-term training framework that:

- Helps each user group become fully proficient
- Supports ongoing retention and refreshing of system knowledge
- Evolves in alignment with changing requirements, system enhancements, and CDC/AIRA updates
- Keeps documentation and support resources accessible and current
- Gives the State continuous visibility into user readiness and competency

This approach enables users to achieve proficiency before go-live and maintain it throughout the duration of the contract.

4.2.3.10.1 Role-Specific Training Strategy

Gainwell has developed a comprehensive training program tailored to the specific needs of each user group. Employing a variety of methods, including guided online seminars, recorded sessions, and detailed user manuals, we see that each user is confident and competent in using

the Solution. Gainwell has included a detailed Training Plan as part of the Implementation Plan deliverables that we will supply after contract award.

4.2.3.10.1.1.OEPS / Agency Administrator

Gainwell will deliver a targeted training program specifically designed to equip OEPS Agency Administrators with the knowledge and skills required to configure the IIS, oversee data quality, produce advanced reports, and support ongoing system maintenance. This training aligns fully with our role-based methodology, which includes instructor-led sessions, recorded modules, and clear, plain-language user documentation.

Training Focus Areas

- **System Configuration and Role Management.** Administrators will receive focused instruction on configuring jurisdiction-specific settings, workflows, and RBAC. This includes managing user permissions and applying least-privilege and RBAC controls to provide secure, compliant access across the IIS.
- **Data Quality Monitoring.** Training will cover the tools and processes used to monitor and maintain IIS data quality, including deduplication practices, address standardization, and the use of audit logs and dashboards to identify and resolve data integrity issues.
- **Advanced Reporting and Analytics.** Administrators will learn to create, schedule, and distribute advanced reports using the system's reporting tools, including operational, ad hoc, and dashboard-based reporting capabilities. Training will also include managing report security and providing data for internal and external stakeholders.
- **System Maintenance and Operational Readiness.** Gainwell will train administrators on their responsibilities in system monitoring, issue escalation, and operational readiness activities. This includes an overview of SLAs, alerts, operational dashboards, and their role in the change and release management processes.

4.2.3.10.1.2. Provider Office Staff/ End-Users

Gainwell will deliver a role-based training program tailored to Provider Office Staff / End-Users who perform day-to-day data entry, patient search/query, use clinical decision support (CDS) for vaccine forecasting, and conduct basic troubleshooting. Training will be provided through instructor-led sessions, recorded micro-modules, and plain-language user manuals to promote consistent adoption and self-sufficiency. Training focus areas include:

- **Day-to-Day Data Entry and Record Management.** End-users will be trained to accurately enter patient demographic and vaccination information using the IIS interface and configured workflows. Instruction emphasizes completeness, accuracy, and prevention of duplicate or fragmented records.
- **Search and Query Functions.** Participants learn efficient methods to locate patient records, review immunization history, and access relevant clinical information. Hands-on practice is conducted in training or UAT environments that mirror production and use de-identified/synthetic data.
- **Clinical Decision Support (CDS) Usage.** End-users will be instructed on interpreting ACIP-aligned CDS forecasting, which includes identifying due or overdue vaccinations and understanding recommended next steps to support clinical decision-making during patient encounters.

- **Basic Troubleshooting and Support Pathways.** Training includes guidance on resolving common user issues, identifying when to escalate, and preparing effective help-desk submissions. Users are shown how to leverage Hypercare office hours and standard support channels following go-live.

4.2.3.10.1.3. School Nurses/ Public Health Partners

Gainwell will deliver a role-specific training program tailored to School Nurses and Public Health Partners, with a focus on roster management, exemption tracking, and public health follow-up workflows. Training will follow our established role-based methodology, using instructor-led sessions, recorded modules, and clear, plain-language user documentation to build confidence and consistency across diverse public health settings. Training focus areas include:

- **Roster Management.** Training will prepare School Nurses and Public Health Partners to manage student rosters using the School Record Management module. Users will learn to review immunization records, add medically verified historical doses, identify students who are non-compliant, and generate roster-based reports for school and district-level analysis. These capabilities support accurate tracking of child and adolescent immunization status.
- **Exemption Tracking.** Learners will receive instruction on navigating exemption records, including how to identify students with exemptions, interpret exemption status within school workflows, and use exemption-related reports. This includes role-appropriate access to exemption data and reporting to support compliance monitoring.
- **Public Health Follow-up Workflows.** Training will cover the use of IIS tools to identify individuals who lack required vaccinations, are susceptible to vaccine-preventable disease, or are overdue for routine immunizations. Users will learn how to generate follow-up lists, apply geographic or demographic filters, and support targeted outreach based on immunization gaps. These workflows assist with disease control and community-level public health intervention.

4.2.3.10.2. Training Deliverables including 4.2.3.10.2.1 – 4.2.3.10.2.2.

Gainwell will provide current, digital, and role-specific training resources that confirm each IIS user. Users include administrators, clinical providers, school and childcare staff, public health personnel, and technical teams. They will have access to clear, intuitive, and on-demand guidance. Our approach emphasizes accessibility, self-service learning, and continuous updates aligned with product enhancements and CDC/AIRA changes.

Gainwell will deliver a full library of role-based, on-demand video modules designed to support each user's job functions within the IIS. These modules will be accessible through the user portal and will include:

- Task-based demonstrations including entering vaccinations, running coverage reports, onboarding partners, and managing exemptions.
- Role-specific walkthroughs for providers, school nurses, administrators, help desk staff, inventory managers, and public health analysts.
- Scenario-based demonstrations showing real-world public health use cases.
- Closed-captioned and accessible content.

Video content is updated as part of our quarterly release cycle to confirm alignment with new features, regulatory updates, and usability enhancements. Gainwell will provide comprehensive

digital user guides and technical reference manuals, each tailored to a specific audience and delivered in searchable, downloadable formats including PDF/HTML.

4.2.3.10.3. Post-Implementation Support and Refreshers

The Vendor must outline the type and duration of support and training to be provided after the system's Go-Live date. This must include:

4.2.3.10.3.1. Post-Implementation Support: A defined period of enhanced dedicated support to resolve user-adoption issues and ensure smooth transition.

4.2.3.10.3.2 Annual Training Refreshers: A plan for providing annual or on-demand refresher training modules and updated documentation to cover new system features, version upgrades, and changes to federal or jurisdictional standards.

Following go-live, Gainwell provides a comprehensive, multi-layer post-implementation support and training program designed to allow system stability, user confidence, and continued proficiency across stakeholder groups.

4.2.3.10.3.1. Post-Implementation Support

Immediately following go-live, Gainwell initiates a 90-day Hypercare period staffed by dedicated technical, functional, and training resources. During this time, we provide:

- Real-time issue triage and resolution with accelerated response times
- Hands-on support for providers, schools, and public health users as they begin live operations
- Daily or weekly status checkpoints with OEPS, depending on State preference
- Prioritized defect remediation and rapid deployment of fixes
- Dedicated trainers available for refresher demonstrations or workflow clarification

This enhanced support phase confirms system users have the assistance they need as they transition into production use and that issues are promptly addressed to maintain confidence and continuity.

4.2.3.10.3.2. Annual Training Refreshers

Gainwell will provide annual and on-demand refresher training modules to confirm users remain proficient as the system evolves. Training materials including on-demand videos, updated user guides, and workflow-specific job aids are maintained in the Learning Management System (LMS) and updated whenever new features, version upgrades, or changes to CDC, AIRA, ACIP, or jurisdictional standards are introduced. Refresher content is delivered through recorded sessions, digital documentation updates, and role-based micro-training modules to confirm users have timely access to current information.

4.2.3.11. Privacy

Privacy:

4.2.3.11.1 The Vendor must comply with all relevant State and Federal Data Privacy Laws, Regulations, and Policies.

4.2.3.11.2. The IIS must maintain an internal audit log of all user access and activity, including logins, data additions, edits, deletions, and exports. The Agency is required to keep the data for 6 years and Vendor must provide this to the agency at

designated timeframes or upon request. Access to audit logs shall be limited to authorized Agency staff and may be used for compliance monitoring or investigation of suspected breaches.

4.2.3.11.3 If a data breach is discovered or suspected Vendor shall immediately follow the process outlined in the most recent version of the Office of Management Information Services Incident Reporting and Response Procedures, (Attachment G) ([https://www.wvdhhr.org/mis/policies/Incident Reporting and Response.pdf](https://www.wvdhhr.org/mis/policies/Incident%20Reporting%20and%20Response.pdf))

4.2.3.11.4 The Vendor shall ensure that data maintained on behalf of the IIS is not used, released, or sold without specific authorization of the Agency, regardless of whether the data has been de-identified or included with a limited data set.

4.2.3.11.5. The Vendor must certify that it is not currently under investigation by any state or federal authority for a breach of data security.

4.2.3.11.6. The Vendor must disclose whether it has been involved in any breach of data security and provide details relating to the causes of the breach and the mitigating actions taken in response to the breach.

4.2.3.11.7 The vendor must disclose details of any previous or current investigation by any state or federal authority, including investigations that did not result in formal sanctions, related to privacy or security of patient information. The details must include the resulting corrective action plan or details of the final resolution, including the assessment of any fines or other sanctions against the Vendor.

4.2.3.11.7.1. The State reserves the right to request supporting documentation or conduct independent verification. Failure to disclose relevant investigations may result in disqualification, contract termination, or other remedies.

4.2.3.11.8. The Vendor must certify that it has never been convicted of, charged with, or is under investigation for, violation of any criminal law, or violation of any civil law governing health care fraud, abuse, or waste.

4.2.3.11.9. The Vendor must certify that it does not employ any individuals who have been excluded or debarred by the federal or any state government from participating in any federal or state programs or contracts.

4.2.3.11.10. The Vendor shall not use the IIS data for analytics, AI/ML training, model development, or any secondary purpose without explicit written approval from the State.

Gainwell is committed to protecting the confidentiality and integrity of IIS data. Our approach follows strict federal and state privacy requirements, confirming the Agency retains full ownership of information and that no data is accessed, shared, or repurposed without explicit authorization. IIS data remains securely stored within U.S.-based AWS data centers, supported by robust safeguards including encryption, role-based access, audit logging, and continuous monitoring. Through disciplined governance, rapid incident response, and NIST-aligned privacy practices, we provide a secure and compliant environment for managing the State's immunization data.

4.2.3.11.1 Compliance with State and Federal Data Privacy Laws, Regulations, and Policies

Gainwell confirms its compliance with relevant State and Federal Data Privacy Laws, Regulations, and Policies.

4.2.3.11.2. Internal Audit Log

The Gainwell team confirms the proposed solution will support audit logging, retention, and reporting capabilities as outlined by the State, including detailed event capture, secure log storage, and integration with the State's Security Information and Event Management (SIEM) solution when applicable.

Our Audit Logging and Monitoring Standard (ISPS-009) requires the collection of detailed audit logs for relevant systems, including user and system activity such as record creation, modification, deletion, viewing, printing, and search actions, as well as login and logout events. Each log entry includes the user ID, timestamp, network location, the data accessed, and when applicable, the record's state before and after changes.

Audit logs are retained online for at least 90 days and archived for a minimum of six years in accordance with internal compliance policies. These logs are for internal use only and are maintained to support compliance monitoring, incident response, and regulatory investigations as required by our policies and applicable contract terms.

4.2.3.11.3. Data Breach

Gainwell acknowledges the requirement and shall follow the process outlined in Attachment G of this RFP.

4.2.3.11.4. Data Maintenance

Gainwell acknowledges and affirms that data maintained on behalf of the Solution is not used, released, or sold without specific authorization from the State.

4.2.3.11.5. Investigation

Gainwell certifies that it is not currently under investigation by a state or federal authority for a breach of data security.

4.2.3.11.6. Data Security Breach

In September 2022, Gainwell detected and responded to a ransomware incident affecting an isolated and limited part of its Information Technology systems. The company promptly took the impacted environment offline, launched an investigation with cybersecurity experts, eliminated the threat, and notified law enforcement. Affected services were promptly restored, and there was no evidence that data was extracted. Following the incident, Gainwell further enhanced our security measures.

4.2.3.11.7. Investigation Disclosure

Gainwell received and responded to formal Requests for Information (RFIs) from the Department of Health and Human Service Office of Civil Rights (OCR) in response to the following:

- Unauthorized access to vendor's system due to social engineering (November 2020)
- A mis-mailing event involving one of Gainwell's third-party contractors (December 2020).
- Two related instances of unauthorized access to a vendor's system due to social engineering (March 2022).
- Reportable breach incident caused by a system configuration issue (February 2022).
- Unauthorized access to vendor's system due to social engineering (May 2022).
- Unauthorized access to vendor's system due to social engineering (May 2023).

After responding to OCR and cooperating with their investigations, these incidents were closed without findings or penalties. No corrective action plans were imposed.

4.2.3.11.7.1. Supporting Documentation

Gainwell acknowledges the State's right to request supporting documentation or conduct its own independent verification.

4.2.3.11.8. Vendor Certification of Legal and Regulatory Compliance

Gainwell certifies that it has never been convicted of, charged with, nor is under investigation for violation of a criminal law, or violation of a civil law governing health care fraud, waste or abuse.

4.2.3.11.9. Certification Regarding Excluded or Debarred Personnel

Gainwell certifies that it does not employ individuals who have been excluded or debarred by the federal or any state government from participating in any federal or state programs or contracts.

4.2.3.11.10. Written Approval Consent

Gainwell uses client data strictly for purposes defined within the contract and in accordance with applicable federal, state, and contractual data protection requirements. IIS data is processed solely to deliver contracted services and support authorized public health functions. Gainwell does not use IIS data for analytics outside the contracted scope, artificial intelligence or machine learning training, model development, or secondary purposes without explicit written approval from the State.

Data governance controls, access restrictions, and documented use limitations are enforced through the Gainwell Information Security Policy, Data Protection Policy, and role-based access controls. Contractual data use restrictions are embedded within operational procedures and technical safeguards to promote adherence to State-approved purposes and protect the confidentiality and integrity of IIS data.

4.2.3.12. Security and Audit Compliance

Security and Audit Compliance

Gainwell maintains a comprehensive security and audit compliance program aligned with the Gainwell Information Security Policy, Logging and Monitoring Standard, Threat and Vulnerability Management standards, Secure Development Standard (ISPS-013), and System Acquisition, Development, and Maintenance Security Standard (ISPS-15). The IIS solution supports formal security governance, centralized monitoring, documented control implementation, and periodic internal and independent assessments. Audit logging captures security-relevant events including authentication activity, administrative actions, data access, and configuration changes, and logs are retained in accordance with jurisdictional policy and contractual requirements.

Gainwell supports audit readiness through maintained compliance artifacts such as System and Organization Controls (SOC) 2 Type II reports, independent penetration testing reports, documented vulnerability remediation tracking, and formal incident response documentation. Security controls are subject to periodic review, centralized monitoring, and defined escalation procedures. Audit evidence can be provided under appropriate confidentiality controls to demonstrate adherence to applicable federal, state, and contractual cybersecurity and compliance requirements.

4.2.3.12.1. Federal Security Compliance Requirements

Federal Security Compliance Requirements: The Vendor must ensure the IIS solution complies with applicable federal cybersecurity standards, including:

Gainwell aligns the IIS Solution with applicable federal cybersecurity standards in accordance with the Gainwell Information Security Policy, Secure Development Standard (ISPS-013), Threat and Vulnerability Management standards, and System Acquisition, Development, and Maintenance Security Standard (ISPS-15). Gainwell's enterprise security program is structured around the NIST 800-53 control framework and incorporates supporting guidance from NIST 800-61 (Incident Response) and NIST 800-218 (Secure Software Development Framework). Security controls are documented, formally governed, periodically reviewed, and subject to internal oversight processes including vulnerability management, access control enforcement, logging and monitoring, encryption management, and secure change control.

Where contractually required, Gainwell supports environments aligned to FedRAMP Moderate-equivalent control baselines and implements Federal Information Processing Standards (FIPS)-validated cryptographic mechanisms for protection of data at rest and in transit. Compliance artifacts such as SOC 2 Type II reports, independent penetration testing reports, and documented security policies are maintained and can be provided under appropriate confidentiality controls. Gainwell's security governance structure promotes ongoing adherence to applicable federal cybersecurity standards through documented procedures, centralized monitoring, and defined incident response processes.

4.2.3.12.1.1. FedRAMP Authorization

FedRAMP Authorization: The solution must be FedRAMP Moderate or High authorized at the time of contract award. Vendors must provide proof of FedRAMP authorization (ATO letter or listing on the FedRAMP Marketplace). Cloud providers must also maintain FedRAMP Moderate or High authorization; SOC 2 Type II may be submitted only as supplemental evidence.

Gainwell's enterprise security program aligns to the NIST 800-53 control framework and supports deployment within cloud environments that maintain FedRAMP Moderate or High authorization. Where the IIS solution is hosted within a FedRAMP-authorized cloud service provider (CSP), Gainwell leverages that provider's FedRAMP Moderate or High Authorization to Operate (ATO) as documented on the FedRAMP Marketplace. Documentation such as the CSP's FedRAMP authorization status and supporting security artifacts can be provided under appropriate confidentiality controls. SOC 2 Type II reports and related assessments are maintained as supplemental assurance evidence consistent with the RFP requirement.

Gainwell as an application vendor does not independently hold a FedRAMP Authority to Operate (ATO) unless the specific IIS deployment is sponsored and authorized under a federal agency FedRAMP authorization boundary. If the RFP requires the application itself to hold a FedRAMP Moderate or High ATO at time of award, that status depends on the selected hosting architecture and authorization scope. Gainwell can deploy within a FedRAMP-authorized environment and support required federal security controls; confirmation of full FedRAMP authorization at award is contingent upon the hosting and authorization boundary defined for the contract.

4.2.3.12.1.2. FIPS 140-2/3 Validated Cryptography

FIPS 140-2/3 Validated Cryptography: All cryptographic modules used for data at rest and in transit must be validated under NIST's Cryptographic Module Validation Program (CMVP).

Gainwell implements encryption controls in alignment with the Gainwell Information Security Policy and the Gainwell Encryption Standard. Cryptographic mechanisms used to protect data at rest and in transit leverage modules validated under NIST's Cryptographic Module Validation Program (CMVP), consistent with FIPS 140-2 or FIPS 140-3 requirements, depending on the hosting environment and applicable federal guidance. Encryption in transit is enforced through secure protocols such as TLS 1.2 or higher using FIPS-validated libraries, and encryption at rest is applied at the storage, database, or disk layer using validated cryptographic modules.

Cryptographic configurations are governed through documented key management procedures, controlled access to encryption keys, and centralized security oversight. Validation status of underlying cryptographic modules can be confirmed through CMVP listings for the applicable cloud service provider or platform components, and documentation can be provided under appropriate confidentiality controls in support of contract requirements.

4.2.3.12.1.3. Transport Layer Security (TLS)

Transport Layer Security (TLS): All IIS data exchanges, including connections to CDC's IZ Gateway, must use TLS in accordance with the most current version of NIST SP 800-52 (Guidelines for the Selection, Configuration, and Use of TLS Implementations). At minimum, the IIS must support TLS 1.2 and TLS

1.3 at contract award. Vendors must demonstrate the ability to implement newer TLS versions or configurations within 12 months of publication by NIST or CDC. All TLS implementations must use cryptographic modules validated to FIPS 140-2 or FIPS 140-3 under NIST's Cryptographic Module Validation Program (CMVP) and must employ only approved cipher suites.

Gainwell supports Transport Layer Security (TLS) for IIS data exchanges in alignment with the Gainwell Information Security Policy, the Gainwell Encryption Standard, and applicable federal guidance including NIST SP 800-52. External and system-to-system communications, including connections to CDC's IZ Gateway, are configured to support TLS 1.2 and TLS 1.3 at contract award. TLS configurations use FIPS 140-2 or FIPS 140-3 validated cryptographic modules under NIST's Cryptographic Module Validation Program (CMVP), and only approved cipher suites are enabled in accordance with federal security guidance and platform capabilities.

TLS configurations are governed through documented configuration management and security review processes. Gainwell maintains the capability to adopt updated TLS versions, protocol configurations, or approved cipher suite changes following publication of revised guidance from NIST or CDC, subject to platform support and formal change management. Security configurations are reviewed periodically to promote alignment with current federal standards and evolving cryptographic requirements.

4.2.3.12.4. Ongoing Compliance

Ongoing Compliance: Vendors must maintain compliance with evolving federal cybersecurity standards throughout the contract term and report any changes to FedRAMP authorization, FIPS validation, or TLS support within 30 days.

Gainwell maintains ongoing compliance with evolving federal cybersecurity standards through several key processes and strategies, including:

- **Gap Analysis and Policy Updates.** Conduct thorough gap analyses to identify additional requirements and controls necessary to meet specifications from the State or CMS. This includes developing or updating policies and procedures to address new requirements.
- **Process Implementation and Stakeholder Collaboration.** Establish operational processes and controls to achieve compliance, including staff training and integration into existing workflows. Work closely with stakeholders to verify the implementation aligns with expectations and priorities.
- **Security Risk Management.** Employ a comprehensive security risk management process that includes ongoing risk assessments and audits to identify areas for improvement. This area regularly updates policies and procedures based on changes in laws, regulations, or industry standards.
- **Monitoring and Reporting.** Perform static and dynamic code, application, and compliance scans monthly, along with on-call scans as needed. This minimizes the potential effect of threats by addressing technical, environmental, and personnel aspects holistically.
- **Security Audit Reports and Mitigation Plans.** Provide annual security audit reports using SSAE 18 SOC 2 Type II, including a Plan of Action and Milestones (POA&M) to remediate deficiencies found during audits. Address major deficiencies with mitigation plans to correct noncompliance issues.

Through these measures, Gainwell maintains ongoing compliance with evolving federal cybersecurity standards through its enterprise security governance and compliance management programs. Gainwell's security framework aligns with recognized federal standards including NIST SP 800-53, FedRAMP security baselines, FIPS-validated cryptographic requirements, and NIST guidance for TLS implementations. Security policies, control mappings, and operational procedures are periodically reviewed and updated through formal governance processes to maintain alignment with updated federal and state cybersecurity requirements throughout the contract term.

Gainwell's compliance program includes continuous monitoring of regulatory and framework updates affecting FedRAMP authorization status, FIPS cryptographic validation, and TLS protocol requirements. When material changes occur to the hosting environment, authorization status, or supported cryptographic or transport security configurations, Gainwell provides notification to the State within thirty calendar days and supplies supporting documentation describing the change and its impact on the system's security posture. This governance model promotes sustained alignment with evolving cybersecurity standards while maintaining transparency with the State regarding compliance status.

4.2.3.12.2. SOC 2 Type II Audit Report

SOC 2 Type II Audit Report

4.2.3.12.2.1. The awarded Vendor shall provide a current SOC 2 Type II audit report within 60 calendar days of the contract execution. The report must cover a review period ending no more than 12 months prior to submission and demonstrate compliance with the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy.

4.2.3.12.2.2. The vendor shall provide an updated SOC 2 Type II audit report annually within 30 calendar days of the contract anniversary date for the duration of the contract term. The State reserves the right to review and approve the sufficiency of the report and may request additional documentation or clarification in the event of material changes to the Vendor's hosting environment or security posture.

4.2.3.12.2.3. ISO/IEC 27001 certification may be submitted as supplemental evidence of organizational security maturity but does not substitute for the SOC 2 Type II requirement or the State's U.S. data residency policy.

In the following sections, Gainwell confirms its ability and willingness to provide current System and Organization Control (SOC) 2 Type II audit reporting at the frequency required by the State.

4.2.3.12.2.1. SOC 2 Audit Compliance

Gainwell acknowledges the SOC 2 Type II requirement and will provide the report when audit conditions are met, with interim assurance artifacts (e.g., SOC 2 Type I, bridge letter, or attestation) available as appropriate.

SOC 2 Type II Audit Report

Gainwell maintains a mature information security and compliance program aligned with the SOC 2 Trust Services Criteria for **Security, Availability, Confidentiality, and Privacy**. Gainwell has completed a **SOC 2 Type I audit**, which can be made available upon request. A SOC 2 Type II audit is dependent upon the existence of live production environments over a sufficient review period, as certain required audit evidence is not available until the State environments are operational.

Following contract execution, Gainwell will work to provide the required SOC 2 Type II audit once the necessary operational conditions are met. If a finalized SOC 2 Type II report covering a review period ending no more than twelve months prior is not available within 60 calendar days of contract execution, Gainwell will provide appropriate alternative assurance documentation, which may include:

- The completed SOC 2 Type I report
- Confirmation of SOC 2 Type II audit scope and status; and/or
- A bridge letter or written attestation describing Gainwell's control environment and ongoing compliance efforts.

Upon completion of the SOC 2 Type II audit and subject to standard confidentiality and distribution restrictions, Gainwell will provide the finalized report to the State.

4.2.3.12.2.2. SOC 2 Audit Report

Gainwell acknowledges the RFP requirements regarding SOC 2 Type II Audit Reports and will provide an updated audit report on an annual basis within 30 calendar days of the contract anniversary date for the duration of the contract term.

4.2.3.12.2.3. ISO/IEC 27001 Certification

Gainwell acknowledges the RFP requirement and will provide ISO/IEC 27001 certification as supplementary evidence of organizational security maturity.

4.2.3.12.3. Penetration Testing and Vulnerability Management

Penetration Testing and Vulnerability Management: The Vendor must perform third-party penetration testing of the hosted IIS environment on an annual basis, in compliance with NIST 800-53 standards. A detailed report of findings and remediation actions shall be submitted to the State within 30 calendar days of test completion. The Vendor shall maintain a documented vulnerability management program and address all critical or high-risk findings within 30 calendar days, unless otherwise approved by the State.

Gainwell performs independent third-party penetration testing of hosted environments on an annual basis in alignment with NIST Special Publication (SP) 800-53 security control expectations and applicable federal security guidance.

The annual assessment includes testing of network infrastructure, application layers, authentication and access controls, and encryption mechanisms. Testing is conducted by qualified independent security firms, and a detailed report documenting findings, risk ratings, and remediation actions is produced upon completion. Consistent with the RFP requirement, Gainwell will provide the State with a detailed penetration testing report and documented remediation status within thirty calendar days of test completion.

In addition, Gainwell maintains a documented vulnerability management program aligned with the Gainwell Information Security Policy, Threat and Vulnerability Management standards, Secure Software Development standards, and the NIST 800-53 control framework. The program includes continuous vulnerability scanning of infrastructure and applications, risk-based classification of findings, formal tracking and remediation workflows, and defined escalation procedures for critical issues. Critical and high-risk vulnerabilities are remediated within thirty calendar days unless an alternative remediation plan is formally documented and approved by the State. Where remediation cannot be completed within the required timeframe, Gainwell documents compensating controls, performs formal risk review, provides written justification and a defined remediation timeline, and seeks State approval prior to closure.

4.2.3.12.4. Secure Software Development Lifecycle (SSDLC) Practices

Secure Software Development Lifecycle (SSDLC) Practices: The Vendor must adhere to secure software development lifecycle (SSDLC) practices to ensure the IIS is developed, maintained, and operated in accordance with federal cybersecurity standards. Requirements include:

Our secure application development processes are governed by ISPS-013 – Software Security and Secure Development Standard, which integrates leading industry frameworks and federal guidance into our Secure Software Development Lifecycle (SSDLC). This includes conformance with the OWASP

Top 10 for web application vulnerabilities, the NIST SP 800-218 Secure Software Development Framework (SSDF), and ISO/IEC 27034 for application security structure and validation.

4.2.3.12.4.1. Documented SSDLC Process

Documented SSDLC Process: The Vendor shall maintain and provide documentation of secure development lifecycle practices, aligned with NIST SP 800-218 (Secure Software Development Framework) or equivalent.

Gainwell acknowledges the requirement. As mentioned above, Gainwell's SSDLC includes conformance with the NIST SP 800-218 SSDF.

4.2.3.12.4.2. Static and Dynamic Application Security Testing (SAST/DAST)

Static and Dynamic Application Security Testing (SAST/DAST): The Vendor must perform SAST scans integrated into the development pipeline for every code commit or build and DAST scans at least quarterly, and following any major release or production update. The Vendor must provide remediation plans for all identified vulnerabilities, with critical and high-risk findings resolved within 30 calendar days, unless otherwise approved by the Agency.

Gainwell complies with the requirement to perform comprehensive Static and Dynamic Application Security Testing (SAST/DAST) as part of our secure software development lifecycle.

SAST Integration into the Development Pipeline

We integrate automated SAST scans directly into our CI/CD pipeline, confirming codes commit and build, undergoing security review before it can progress to later stages of development or deployment. This continuous scanning approach enables early detection of vulnerabilities and prevents insecure code from entering the production path.

DAST Execution Cadence

In alignment with the requirement, Gainwell performs Dynamic Application Security Testing at least quarterly and additionally after major releases or production updates. These scans evaluate the running application for real-world, exploitable vulnerabilities, confirming continuous protection of the production environment.

4.2.3.12.4.3. Vulnerability Management Integration

Vulnerability Management Integration: Findings from SAST/DAST must be incorporated into the Vendor's vulnerability management program, with remediation timelines consistent with Section 4.2.3.12.2.

Identified vulnerabilities are logged, triaged, and addressed through a formal remediation process. Gainwell prepares and provides detailed remediation plans for findings, including root cause, mitigation strategy, and expected resolution timelines. Critical and high-risk vulnerabilities are remediated within 30 calendar days, unless an alternative timeline is formally approved by the Agency.

4.2.3.12.4.4. Third-Party Component Security

Third-Party Component Security: The Vendor must track and document all third-party libraries and modules, ensuring they are updated and free of known critical vulnerabilities.

Gainwell maintains a rigorous third-party component security program as part of our Secure Software Development Lifecycle (SSDLC).

In compliance with the requirement, we track, document, and continuously monitor third-party libraries, frameworks, and modules used within the IIS solution. This includes both open-source and commercial components. Gainwell maintains a complete, continuously updated inventory of third-party components integrated into the solution. This documentation includes component versions, dependencies, licensing details, and security status, confirming accountability and full transparency.

4.2.3.12.4.5. Continuous Monitoring

Continuous Monitoring: The Vendor must implement continuous monitoring practices consistent with FedRAMP and NIST guidance, including automated code scanning and penetration testing at least annually.

We maintain full transparency with the Agency through routine reporting on scan results, remediation activities, and risk posture. This includes providing evidence of completed SAST/DAST scans, remediation verification, and continuous improvement actions within our secure development lifecycle.

4.2.3.12.5. Cloud Provider Attestations

Cloud Provider Attestations: If the Vendor utilizes a third-party cloud service provider, the Vendor shall provide:

4.2.3.12.5.1. Documentation confirming that the cloud provider maintains FedRAMP Moderate or High authorization; SOC 2 Type II may be submitted only as supplemental evidence.

4.2.3.12.5.2. Evidence that all IIS data is stored and processed exclusively within U.S.-based data centers, in compliance with federal government and West Virginia's cybersecurity and data residency requirements.

4.2.3.12.5.3. Supports compliance with applicable Executive Branch and Office of Management Information Services (OMIS) Security Policies.

When a third-party cloud service provider (CSP) is used, Gainwell leverages cloud environments that maintain documented security attestations consistent with federal and industry requirements. Gainwell obtains and maintains current compliance artifacts from the CSP, including FedRAMP authorization status (Moderate or High where applicable), SOC 2 Type II reports, FIPS 140-2/3 cryptographic validation documentation, and relevant NIST control alignment evidence. These attestations are reviewed as part of Gainwell's third-party risk management and supplier security governance processes.

Cloud provider compliance documentation can be provided under appropriate confidentiality protections, including ATO letters, FedRAMP Marketplace listings, SOC reports, and security responsibility matrices that define shared control responsibilities. Gainwell's governance program includes periodic review of CSP compliance status, monitoring of authorization updates, and formal risk evaluation processes to maintain alignment with contractual, federal, and jurisdictional cybersecurity requirements.

4.2.3.12.5.1. FedRAMP Confirmation

Gainwell provides documentation confirming that the CSP maintains FedRAMP Moderate or High authorization status. This documentation includes the cloud provider's current Authorization to Operate (ATO) letter or official listing on the FedRAMP Marketplace that verifies the authorization level and status. Where required, Gainwell provides the relevant FedRAMP authorization package documentation under appropriate confidentiality controls.

SOC 2 Type II reports may also be provided as supplemental assurance documentation; however, FedRAMP Moderate or High authorization documentation serves as the primary evidence of federal security compliance, consistent with the RFP requirement.

4.2.3.12.5.2. U.S.-based Data Centers

Gainwell deploys the IIS solution within U.S.-based data centers consistent with federal cybersecurity requirements and West Virginia data residency requirements. Hosting architecture is configured to restrict data storage, processing, backups, logging, and disaster recovery environments to U.S. geographic regions only. Gainwell can provide documentation from the CSP confirming U.S. region deployment, data residency configuration, and geographic restrictions as part of the hosting architecture.

Data residency controls are governed through documented cloud configuration standards, contractual requirements with the cloud provider, and third-party risk management oversight. Region restrictions are enforced through infrastructure configuration settings and monitored through change management and security review processes to promote ongoing compliance with federal government and State of West Virginia cybersecurity and data residency obligations.

4.2.3.12.5.3. OMIS Compliance

Gainwell supports compliance with applicable Executive Branch and Office of Management Information Services (OMIS) Security Policies.

4.2.3.12.6. Vendor Attestation Form

Vendor Attestation Form:

The State reserves the right to request updated attestations annually or upon material changes to the Vendor's operations or hosting environment. All vendor attestations are subject to verifications under Section 4.2.3.12.8. Audit and Attestation Requirements.

4.2.3.12.6.1. The awarded Vendor shall complete and submit a Vendor Attestation Form within 30 calendar days of contract execution, certifying compliance with the following:

The State reserves the right to request updated attestations annually or upon material changes to the Vendor's operations or hosting environment. All vendor attestations are subject to verifications under Section 4.2.3.12.8. Audit and Attestation Requirements.

4.2.3.12.6.1.1. U.S.-based data residency and transmission restrictions.

4.2.3.12.6.1.2. SOC Type II audit submission timelines.

4.2.3.12.6.1.3. Penetration testing and vulnerability remediation protocols.

4.2.3.12.6.1.4. Cloud provider compliance.

4.2.3.12.6.1.5. All applicable state and federal cybersecurity policies and standards.

4.2.3.12.6.1.6. All applicable state and federal information security and privacy requirements.

Gainwell acknowledges and affirms that the State reserves the right to request updated attestations annually or upon material changes to Gainwell's operations or hosting environment. We understand attestations are subject to verifications under Section 4.2.3.12.8. Audit and Attestation Requirements.

4.2.3.12.6.1. Vendor Attestation Form

If awarded the contract, Gainwell will complete and submit a Vendor Attestation Form within 30 calendar days of contract execution.

4.2.3.12.6.1.1. U.S.-based Residency and Transmission Restrictions

Gainwell's Vendor Attestation Form will certify compliance with U.S.-based data residency and transmission restrictions.

4.2.3.12.6.1.2. SOC Audit Submission Timelines

Gainwell's Vendor Attestation Form will certify compliance with SOC Type II audit submission timelines, as the IIS must be running in the production environment for at least six (6) months.

4.2.3.12.6.1.3. Penetration Testing and Vulnerability Remediation Protocols

Gainwell's Vendor Attestation Form will certify compliance with penetration testing and vulnerability remediation protocols.

4.2.3.12.6.1.4. Cloud Provider Compliance

Gainwell's Vendor Attestation Form will certify compliance with Cloud provider compliance.

4.2.3.12.6.1.5. State and Federal Cybersecurity Policies and Standards

Gainwell's Vendor Attestation Form will certify compliance with applicable state and federal cybersecurity policies and standards.

4.2.3.12.6.1.6. State and Federal Information Security and Privacy Requirements

Gainwell's Vendor Attestation Form will certify compliance with applicable state and federal information security and privacy requirements.

4.2.3.12.7. Incident Response (IR) Policy and Plan Requirements

Incident Response (IR) Policy and Plan Requirements: The Vendor must maintain and provide documentation of its own incident response (IR) policy and plan, in addition to following the Agency's incident response procedures in 4.2.3.11.3.. Requirements include

Gainwell creates a Solution-specific Security Plan, which provides Gainwell's overall security management strategy, and details Gainwell's approach and techniques for protecting the Solution. As part of our Security Plan, Gainwell details an Incident Response strategy, addressing security incidents and findings, including the following.

Interruption of Service, Including Denial-of-Service Attacks. Typically, interruption of service is treated as noncompliance with a performance metric and would be covered under SLA performance management rather than security; however, if an interruption occurred as a result of a security incident such as a distributed denial-of-service (DDoS) attack, Gainwell treats the instance as a Security Incident and handles it according to our Incident Response Plan. Gainwell's security protocols defined in our Security Plan includes solutions to prevent or mitigate DDoS attacks from occurring. Gainwell's Incident Response Plan is as follows:

- Incident determination
- Initial response and investigation
- Interim reporting
- Incident remediation
- Final reporting
- Incident remediation follow-up and lessons learned

4.2.3.12.7.1. NIST Alignment

NIST Alignment: The Vendor's IR policy and plan must be aligned with the most current version of NIST SP 800-61 (Computer Security Incident Handling Guide) or successor publications.

Gainwell confirms that the proposed solution is aligned with the most current version of NIST SP 800-61.

4.2.3.12.7.2. Ongoing Updates

Ongoing Updates: The Vendor must update its IR policy and plan within 6 months of any NIST revision or federal mandate affecting incident response practices.

Gainwell affirms that it will update its Incident Response (IR) policy and plan within six months of a revision to applicable NIST publications or a new federal mandate impacting incident response practices.

This commitment aligns with the requirement outlined in the RFP, which specifies timely updates to confirm continued compliance with evolving federal cybersecurity guidance, including NIST SP 800-61 and successor publications. To meet this requirement, Gainwell will:

- Monitor NIST, federal, and sector-specific cybersecurity updates through our enterprise compliance program and dedicated cybersecurity governance team.
- Assess regulatory or standard updates for impact to our IR procedures, incident handling workflows, escalation models, and communication plans.
- Revise IR policies and procedures within the required six-month window, incorporating mandated updates into our documented processes, technical playbooks, and staff training materials.
- Integrate updates into coordinated incident response operations shared with the Agency, confirming aligned detection, reporting, containment, eradication, and recovery activities.
- Document revisions and make the updated IR plan available to the Agency upon request, along with required annual certifications.

This disciplined update cycle is supported by Gainwell's broader continuous improvement and security governance practices, which include regular audits, vulnerability assessments, tabletop exercises, and lessons-learned integrations. These mechanisms confirm our IR posture remains current, actionable, and fully aligned with federal expectations.

4.2.3.12.7.3. Integration with Agency Plan

Integration with Agency Plan: The Vendor must demonstrate how its IR plan complements and integrates with the Agency's incident response procedures, ensuring coordinated detection, reporting, containment, eradication, and recovery.

Gainwell's Incident Response (IR) plan is designed to fully complement and integrate with the Agency's procedures by aligning detection, reporting, containment, eradication, and recovery activities with the coordinated processes required in the RFP. Our IR framework synchronizes with the Agency's response steps through shared monitoring and alerting, required incident reporting workflows, and collaborative containment and recovery actions.

4.2.3.12.7.4. Testing and Exercises

Testing and Exercises: The Vendor must conduct annual incident response exercises (e.g., tabletop or simulated breach scenarios) and provide summary reports of findings and corrective actions to the Agency within 30 calendar days.

Gainwell will conduct annual incident response exercises, including tabletop and simulated breach scenarios, and will provide the Agency with summary reports of findings and corrective actions within 30 calendar days, as required.

4.2.3.12.7.5. Availability

Availability: The Vendor must make its IR policy and plan available to the Agency upon request and certify compliance annually.

Gainwell will make its IR policy and plan available to the Agency upon request and will certify compliance annually, as required.

4.2.3.12.7.6. Continuous Improvement

Continuous Improvement: The Vendor must incorporate lessons learned from incidents and exercises into its IR plan within 60 calendar days of identification.

Gainwell will incorporate lessons learned from incidents and incident-response exercises into its IR plan within 60 calendar days of identification, as required, to support continuous improvement.

4.2.3.12.8. Audit and Attestation Requirements

Audit and Attestation Requirements: The State reserves the right to audit or request attestation regarding any security controls required under this contract. The Vendor shall:

Gainwell maintains a structured security governance and audit readiness program aligned with the Gainwell Information Security Policy, Secure Development Standard (ISPS-013), Threat and Vulnerability Management standards, and Logging and Monitoring Standard. Gainwell supports the State's right to audit and to request formal attestation regarding security controls required under the contract. Upon receipt of a written request, Gainwell provides documented policies, control descriptions, configuration standards, testing summaries, vulnerability remediation status, encryption documentation, and formal attestation statements that reflect the current security control environment.

Audit coordination is managed through established governance processes to promote accurate, secure, and timely delivery of requested materials. Gainwell collaborates with the State to facilitate structured evidence review sessions, compliance walkthroughs, and controlled documentation exchanges under appropriate confidentiality protections. This approach promotes transparency into implemented security controls while preserving system integrity, operational security safeguards, and regulatory compliance obligations.

4.2.3.12.8.1. Provide Evidence at No Cost

Provide Evidence at No Cost: Supply system documentation, policies, configurations, testing results, audit reports, or other evidence necessary to verify compliance at the State's request, without additional cost.

Gainwell maintains comprehensive security documentation and compliance artifacts as part of its established governance and audit readiness program. Upon written request from the State, Gainwell provides relevant system documentation, security policies, configuration standards, penetration testing summaries, vulnerability management status reports, and formal attestation materials necessary to validate compliance with contractual security requirements.

Documentation is supplied under appropriate confidentiality protections and in alignment with defined contractual obligations.

Direct access to internal system logs or unrestricted internal security reports is not provided; however, Gainwell collaborates with the State to furnish structured reports, executive summaries, and controlled evidence packages that address the requested control areas. Requested compliance evidence is delivered at no additional cost to the State, consistent with contractual commitments and established security governance practices.

4.2.3.12.8.2. Timely Response

Timely Response: Provide requested evidence within 30 calendar days of the State's request, unless otherwise approved in writing by the Agency.

Gainwell supports timely audit and compliance reporting in accordance with contractual obligations. Upon receipt of a formal written request from the State, Gainwell provides requested documentation, structured compliance reports, attestations, and audit overviews within thirty calendar days, unless an alternative timeframe is approved in writing by the Agency.

Requests are tracked through established governance and coordination processes to promote accurate, complete, and secure delivery of evidence. Where requested materials require compilation or redaction to protect sensitive internal security information, Gainwell coordinates with the State to provide appropriate documentation within the required timeframe while maintaining system integrity and confidentiality controls.

4.2.3.12.8.3. Independent Verification

Independent Verification: Permit the State or its designated third-party auditor to conduct independent verification of security controls, including site visits or technical assessments, with reasonable notice.

Gainwell supports independent verification of security controls consistent with contractual audit rights and established security governance practices. Upon reasonable written notice, Gainwell cooperates with State-led reviews and third-party auditor assessments by providing structured documentation, control attestations, security program overviews, and compliance artifacts necessary to demonstrate adherence to contractual and regulatory requirements. Gainwell facilitates remote technical validation sessions, evidence reviews, and detailed walkthroughs of implemented security controls under appropriate confidentiality protections.

Where site visits or technical assessments are requested, coordination is conducted in advance to align with operational security safeguards and hosting environment requirements. For cloud-hosted environments, physical data center access follows the applicable provider's security and authorization policies. Gainwell works collaboratively with the State to arrange appropriate verification mechanisms that provide meaningful transparency into security controls while maintaining system integrity, data protection obligations, and regulatory compliance.

4.2.3.12.8.4. Ongoing Attestation

Ongoing Attestation: Complete and submit updated attestation forms annually, or upon material changes to the Vendor's hosting environment, security posture, or compliance status.

Gainwell maintains a formal security governance and compliance management program that includes documented attestation processes aligned with contractual and regulatory requirements. Updated security attestation forms can be completed and submitted on an annual basis and upon material changes to the hosting environment, security controls, compliance posture, or authorization status. Changes that may affect contractual security commitments are evaluated through established change management and risk review processes, and updated attestations are prepared to reflect the current control environment.

Material changes to infrastructure, hosting configuration, authorization boundary, or security certifications are documented and reviewed through centralized governance oversight.

Where such changes occur, Gainwell coordinates with the State to provide updated attestations and supporting documentation in accordance with contract requirements and defined reporting timelines.

4.2.3.12.8.5. Future Standards Alignment

Future Standards Alignment: Ensure that audits and attestations remain aligned with the most current versions of applicable federal and state cybersecurity standards (e.g., NIST, FedRAMP, FIPS, OMIS policies).

Gainwell maintains a structured security governance program that tracks updates to federal and state cybersecurity standards and incorporates revisions into its control framework through formal policy review and change management processes. Security policies, control mappings, audit procedures, and attestation documentation are periodically reviewed and updated to align with the most current versions of applicable standards, including NIST publications, FedRAMP baselines, FIPS cryptographic requirements, and relevant state-specific security policies such as OMIS guidance where applicable.

When federal or state standards are revised, Gainwell evaluates the impact to the hosting environment, security posture, and contractual obligations through documented risk assessment and governance review. Audit methodologies and attestation materials are updated accordingly to reflect the current control environment and regulatory expectations, and updated documentation can be provided to the State under appropriate confidentiality protections.

4.2.3.12.8.6. Remediation Obligation

Remediation Obligation: Address any deficiencies identified during audits or attestations within 60 calendar days, or as otherwise approved by the Agency, and provide written confirmation of remediation.

Gainwell maintains a formal corrective action and remediation management process aligned with the Gainwell Information Security Policy, Threat and Vulnerability Management standards, and Secure Development Standard (ISPS-013). When deficiencies are identified through audits, attestations, or security assessments, findings are documented, risk-rated, and tracked through established remediation workflows. Remediation activities are prioritized based on risk impact and contractual obligations, and corrective actions are implemented within sixty calendar days unless an alternative timeline is approved in writing by the Agency.

Following remediation, Gainwell provides written confirmation detailing the corrective actions taken, validation steps performed, and current control status.

Where remediation requires phased implementation or architectural modification, Gainwell documents interim compensating controls and coordinates with the Agency regarding approved timelines. This structured approach promotes accountability, transparency, and alignment with contractual and regulatory security requirements.

4.2.3.13. Acceptance Criteria

4.2.3.13.1. General Acceptance Requirement: The Agency will issue written Acceptance of the IIS solution only after verifying that all functional, technical, security, interoperability, and performance requirements defined in this Solicitation have been fully met. No portion of the system shall be considered Accepted until all Acceptance activities are completed and approved in writing by the Agency.

Gainwell affirms and fully accepts this requirement.

4.2.3.13.2. Acceptance Testing

Acceptance Testing: The Vendor must support and participate in Agency-led Acceptance Testing, which includes but is not limited to:

All defects identified during Acceptance Testing must be remediated by the Vendor at no additional cost to the Agency.

4.2.3.13.2.1. Functional testing of all modules and workflows

4.2.3.13.2.2. Data migration validation

4.2.3.13.2.3. Interface and interoperability testing (e.g., HL7, FHIR, IIS-to-IIS, HIE, EHR connections)

4.2.3.13.2.4. Performance and load testing

4.2.3.13.2.5. Security and access control verification

4.2.3.13.2.6. User acceptance testing (UAT) with Agency-designated staff

Gainwell fully supports and will actively participate in Agency-led Acceptance Testing activities. We recognize Acceptance Testing as a critical step to confirming solution quality, stability, and readiness. Gainwell agrees that defects identified during Agency-led Acceptance Testing will be remediated at no additional cost, and we will work collaboratively with Agency staff to validate successful correction. Our approach includes full participation in each required testing area, as described below.

4.2.3.13.2.1. Functional Testing

Gainwell conducts comprehensive, multilayered testing, including unit, system, integration, interface, regression, accessibility, security, performance, load, data conversion, and User Acceptance Testing (UAT), to verify that application modules and workflows meet approved requirements. We use a structured Test Management Plan to guide test activities and provide traceability and documentation throughout the process.

4.2.3.13.2.2. Data Migration Validation

Data migration is performed using a proven, low-risk methodology that includes data profiling, cleansing, multiple mock conversions, and rigorous validation reporting. During Acceptance Testing, Gainwell will validate data integrity with the Agency and correct discrepancies at no additional cost.

4.2.3.13.2.3. Interface and Interoperability Testing

Gainwell will participate in Agency-led interface and interoperability validation for required connections, including HL7 v2.5.1, FHIR (as applicable), IIS-to-IIS exchange, HIEs, EHR vendors, and the CDC's IZ Gateway. Our interface testing covers message transport, content validation, acknowledgments, error-handling workflows, and real-time or batch processing requirements. We confirm discrepancies are remediated to meet CDC and AIRA interoperability standards.

4.2.3.13.2.4. Performance and Load Testing

Gainwell performs performance and load testing using dedicated environments and industry-standard tools to validate responsiveness, throughput, scalability, and SLA compliance under production-like conditions. Our architecture is designed to scale quickly and handle high-volume transactions, including millions of HL7 messages per day, without degradation.

4.2.3.13.2.5. Security and Access Control Verification

Gainwell will participate in security and access control verification activities required by the Agency. Our Solution uses role-based access control, Single Sign-On (SAML/OAuth 2.0), MFA, and detailed audit logging to confirm that only properly authorized users can access data. Our security testing includes:

- Validation of user roles and permissions
- Authentication and session control testing
- Penetration testing support
- Verification of encryption, audit logging, and incident response workflows

4.2.3.13.2.6. UAT

Selected State staff will be responsible for executing test plans on solution enhancements. State staff will also be needed to perform UAT. Additionally, time may be required before the UAT if the State wishes to develop independent UAT plans. Timing and effort needed for UAT depends on the items included in a release. State staff and the Gainwell Project Manager will have an agreed-on time frame to complete each UAT cycle.

4.2.3.13.3. Acceptance Criteria

Acceptance Criteria: The IIS solution will be deemed acceptable only when all of the following conditions have been met:

4.2.3.13.3.1 All system functionality is fully implemented as described in the Vendor's approved Implementation Plan and the requirements of this Solicitation.

4.2.3.13.3.2. All required interfaces are operational, exchanging data accurately and consistently with Agency-designated systems.

4.2.3.13.3.3. All defects classified as Critical or High severity are resolved, and no Medium or Low defects materially impact system operation or Agency workflows.

4.2.3.13.3.4. All documentation is delivered, including system architecture, configuration guides, user manuals, training materials, and administrative procedures.

4.2.3.13.3.5. All security controls are implemented and validated, including authentication, authorization, audit logging, and compliance with Agency security standards.

4.2.3.13.3.6. The system operates in the Agency's production environment without material errors for a mutually agreed-upon stabilization period (e.g., 30 days).

4.2.3.13.3.7. The Vendor has met all contractual deliverables, including reporting, project management, and communication requirements.

Gainwell acknowledges and affirms the Acceptance Criteria as detailed in this RFP.

4.2.3.13.3.1. Implementation

System functionalities must be fully implemented as described in the Vendor's approved Implementation Plan and the requirements of this Solicitation. This includes delivery of modules, features, workflows, and configurations identified as in-scope.

4.2.3.13.3.2. Operational Interfaces

Required interfaces must be fully operational, exchanging data accurately and consistently. Completion of interface testing, demonstrated ability to send, receive, and process data in the correct formats, frequencies, and protocols.

4.2.3.13.3.3. System Classifications

Defects classified as Critical or High severity must be fully resolved. Additionally:

- No Medium or Low severity defects may materially impact system operation, data integrity, reporting, or Agency workflows.
- The Agency must validate and approve defect closure through regression testing or user acceptance testing.

4.2.3.13.3.4. Documentation Delivery

Required documentation must be delivered in final, examples include:

- System architecture diagrams, data models, data dictionary documents, and user manuals.
- Training materials such as slide decks, job aids, videos, and quick-reference guides.
- Documentation must be complete, accurate, and updated to reflect the final production configuration.

4.2.3.13.3.5. Implementation of Security Controls

Required security controls must be implemented and validated, and comply with Agency standards and applicable regulations. This stage also includes the completion of security testing, including vulnerability scanning, penetration testing, and remediation of findings.

4.2.3.13.3.6. Stabilization Period

Continuous system availability meeting agreed-upon uptime requirements, this includes:

- No recurring or systemic issues that disrupt user workflows or data processing.
- Vendor responsiveness to issues identified during stabilization, including timely remediation and communication.

4.2.3.13.3.7. Contractual Deliverables

Completion of reporting obligations, such as status reports, risk logs, and performance metrics and adherence to project-management requirements, including confirmation that contractual commitments including technical, administrative, and operational, have been satisfied.

4.2.3.13.4. Formal Acceptance

Formal Acceptance: Upon successful completion of all Acceptance activities, the Agency will issue a written Notice of Acceptance. Only upon issuance of this Notice may the Vendor invoice for implementation-related fees. No annual, recurring, subscription, hosting, or maintenance fees may begin prior to Acceptance.

Gainwell acknowledges and accepts the Formal Acceptance requirements as detailed in the RFP.

4.2.3.13.5. Rejection and Retesting

Rejection and Retesting: If the system fails to meet any Acceptance Criteria, the Agency will issue a Notice of Rejection identifying deficiencies. The Vendor must correct all deficiencies at no additional cost and resubmit the system for Acceptance Testing. The Agency reserves the right to repeat any portion of testing necessary to validate corrections.

Gainwell acknowledges and accepts the Rejection and Retesting process as detailed in the RFP.

4.2.3.13.6. Prorated Annual Fees Post-Implementation

Prorated Annual Fees Post-Implementation: Upon the Agency's formal written Acceptance of the fully implemented IIS solution, the Vendor may invoice only for the prorated portion of the annual licensing, subscription, hosting, maintenance, or support fees corresponding to the remainder of the current contract year. Under no circumstances may the Vendor invoice for a full annual fee for a partial contract year. Proration shall be calculated based on the number of days remaining in the contract year following the date of Acceptance.

Gainwell acknowledges and accepts the Prorated Annual Fees Post-Implementation requirement as detailed in the RFP.

4.2.3.13.7. Annual Fee Billing Limits and Advance Billing Requirements

Annual Fee Billing Limits and Advance Billing Requirements: Following completion of the prorated billing period described in Section 4.2.3.13.6, the Vendor may invoice the Agency for no more than twelve (12) months of annual licensing, subscription, hosting, maintenance, or support fees for any given billing period. Under no circumstances shall the Vendor invoice the Agency for multiple years of annual fees in a single lump-sum invoice. Annual fees shall be billed only in advance for the upcoming twelve (12) month period, or, at the Vendor's option and subject to Agency approval, in quarterly installments billed in advance for the upcoming quarter. The Vendor shall not invoice for any period beyond the next twelve (12) months, nor for any period that has not yet commenced.

Gainwell acknowledges and accepts the Annual Fee Billing Limits and Advance Billing Requirements as detailed in the RFP.

4.3. Qualifications and Experience

Qualifications and Experience: Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as mandatory below.

Gainwell brings a broad portfolio of public healthcare technology, services, and clinical expertise, with deep experience in each area. Thirteen current IIS clients nationwide experience the benefit from having not just an immunization registry vendor, but a true partner that collaborates with states on public health, often providing technology enhancement, operations, and cloud transformation under ongoing contracts. We have worked alongside several state programs for decades, learning their needs, advising on strategies, and recommending solutions to better serve their populations, improve their return on investments, and rooting out fraud, waste, and abuse. We get to know the State's organization, goals, concerns, processes, and people, enabling us to be a trusted partner.

4.3.1. Qualifications and Experience Information

Qualifications and Experience Information: Vendor should describe in its proposal how it meets the desirable qualifications and experience requirements listed below.

In the following sections, Gainwell describes how it meets the desired qualifications and experience requirements.

4.3.1.1. Business

Business: The Vendor should briefly describe the company's core business, background, and experience in providing IT solutions to government health and human services agencies.

Gainwell's Established Presence and Proven Partnership in West Virginia

Gainwell brings a long history of successful collaboration with the State of West Virginia, delivering mission-critical health and human services solutions that support the State's Medicaid program, its providers, and its members. Our operational footprint in West Virginia is extensive, and our teams have deep familiarity with the State's policies, priorities, and program needs. This experience positions Gainwell as a trusted partner capable of supporting the State's evolving vision for integrated, equitable, and high-performing health systems.

Comprehensive Medicaid Enterprise Support

Gainwell currently operates and supports multiple core components of West Virginia's Medicaid enterprise, including:

- **Medicaid Management Information System (MMIS) Claims, Encounters, and Financials (CEF).** Gainwell provides the foundational MMIS capabilities that support claims processing, financial management, and program integrity functions across the Medicaid program.

- **Fiscal Agent Services.** We serve as the State's fiscal agent, confirming accurate, timely, and compliant financial operations.
- **Pharmacy Point-of-Sale (RX POS).** Gainwell processes pharmacy claims for Medicaid, Children's Health Insurance Program (CHIP), and foster care members, confirming real-time adjudication and uninterrupted access to medications.
- **Prescription Drug Rebate Administration.** Our team manages the full drug rebate lifecycle, supporting accurate invoicing, collections, and financial reconciliation.

Provider and Member Support Services

Gainwell delivers a full suite of provider and member support functions to confirm smooth program operations and high-quality service delivery:

- **Provider Enrollment and Screening.** We manage provider onboarding, screening, and ongoing compliance activities.
- **Provider Services.** Our teams support providers with training, issue resolution, and program guidance.
- **Provider and Member Portals.** Gainwell maintains secure, user-friendly portals that streamline access to program information and self-service tools.
- **Member Services.** We support members through responsive customer service, program education, and issue resolution.
- **Call Center Operations.** Gainwell operates call center services that meet or exceed service-level expectations for both providers and members.
- **Mailroom Operations.** Our mailroom services confirm timely processing of inbound and outbound correspondence, supporting program integrity and operational efficiency.

Multi-Tenant Support for West Virginia and the U.S. Virgin Islands

Gainwell supports West Virginia's partnership with the U.S. Virgin Islands through multi-tenant applications that serve both jurisdictions. This shared-services model demonstrates our ability to deliver scalable, secure, and cost-effective solutions that meet the needs of diverse populations while maintaining jurisdictional autonomy.

Additional Program Support Capabilities

Beyond core MMIS and operational services, Gainwell provides specialized program support that strengthens the State's oversight and service delivery, including:

- Early intervention program support
- Third-Party Liability (TPL) services
- Recovery Audit Contractor (RAC) services
- Residency verification services

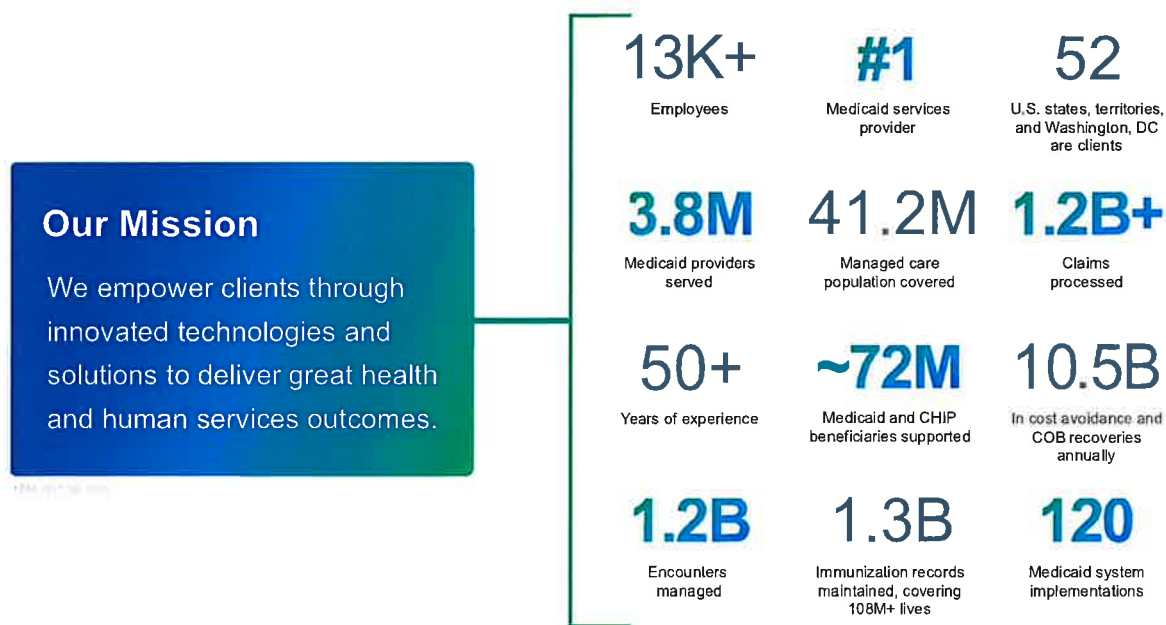
These capabilities reinforce Gainwell's role as a comprehensive partner supporting the full Medicaid lifecycle from eligibility and enrollment to claims processing, program integrity, and member services.

National Leader in Public-Sector Health Technology

Gainwell is the nation's premier provider of Immunization Information Systems (IIS), bringing over 30 years of unparalleled experience and a sterling reputation to the State of West Virginia. Our singular focus on health and human services in the public sector gives us a deep understanding of the unique challenges and objectives of our government partners.

- **Unmatched Scale and Experience.** We support solutions for 52 U.S. states, territories, and Washington D.C. With a workforce of over 13,000 professionals and 50 + years of experience, Gainwell is firmly committed to long-term public health.
- **Proven Success in Complex Environments.** We have a proven track record of successfully implementing and modernizing large-scale complex public health registries.
- **Technical and Interoperability Leadership.** Our solutions align with modern standards including SMART Health Cards and FHIR, and we support seamless data exchange with the Centers for Disease Control and Prevention's (CDC's) IZ Gateway. We have successfully integrated hundreds of EHR systems using bidirectional messaging, enabling providers to both query and update registries with accurate, near-real-time data.
- **Dedicated Expertise.** Gainwell's IIS Center of Excellence includes over 120 full-time specialists with an average of 10 years of IIS experience, including certified HL7 interface developers and interoperability subject matter experts (SMEs). This specialization is unmatched in the industry, meaning we have the knowledge the State seeks in an IIS provider. The following figure provides an overview of our capabilities and experience.

Figure 6. Gainwell Experience Overview



Our team includes certified HL7 interface developers and interoperability SMEs who specialize in onboarding, routing logic, and standards-based data exchange. We are confident in our ability to collaborate effectively with the State, ramp up quickly, and provide a reliable, scalable, and modular solution that supports the State's public health objectives now and into the future.

Gainwell's Experience: A Decade of Proven Leadership in Public Sector Cloud Solutions

For more than 10 years, Gainwell has been at the forefront of providing secure, cloud-based hosting for public sector health and human services solutions. Our experience, which includes hosting over 90 Health and Human Services solutions in Amazon Web Services (AWS) and Microsoft Azure, has enabled us to develop a best-in-class methodology that streamlines implementation, release management, and testing for our clients.

Pioneering Immunization System Cloud Migration

We are leaders in modernizing critical public health infrastructure. Since beginning our focused cloud migration for IIS in 2020, we have successfully transitioned seven state immunization registries to a secure and scalable cloud environment. With this specialized experience, the State can be confident that Gainwell provides a seamless and efficient transition for its most critical systems.

A key advantage of our AWS cloud architecture is the ability to scale on demand. Its intelligent design enables the system to automatically adjust to traffic fluctuations, such as during a public health emergency or a back-to-school rush, providing high performance and cost-efficiency that traditional on-premise solutions cannot match.

Unparalleled Scale and Exclusive Health and Human Services Focus

Gainwell is dedicated to serving government agencies across 52 states and U.S. territories. We are the trusted advisor supporting 52 states for solutions impacting millions of lives daily, which demonstrates our domain expertise. Gainwell supports:

- 3.8 million Medicaid providers served annually
- 1.7 billion immunization records maintained, covering 163 million + lives
- 120 Medicaid system implementations

From Medicaid Management and Systems Interoperability to Analytics and Public Health, our focus is on health and human services. This exclusive dedication allows us to deliver innovative, next-generation cloud technologies that simultaneously reduce costs, improve patient outcomes, and enhance the provider experience.

4.3.1.2. Corporate Identity

Corporate Identity: The Vendor should provide the identity of any parent corporation, including address, phone and fax numbers, federal employer identification number (FEIN) or tax ID number, company website, and contact email. Provide the identity of any subsidiaries, as applicable.

Legal Entity / Vendor Name

Gainwell Technologies LLC

Parent Corporation

Gainwell Acquisition Corporation

Parent Corporation Address

225 East John Carpenter Freeway, Suite 500

Irving, Texas 75062

Phone Number

214 453 3000

Fax Number

469 320 5153

Federal Employer Identification Number (FEIN)

27 1510177 (Gainwell Technologies LLC)

85 1850812 (Gainwell Acquisition Corporation)

Company Website

<https://www.gainwelltechnologies.com>

Primary Contact Email

amoyer@gainwelltechnologies.com

Subsidiaries

Gainwell Technologies LLC operates as a wholly owned subsidiary of Gainwell Acquisition Corporation. No additional subsidiaries are proposed for this engagement.

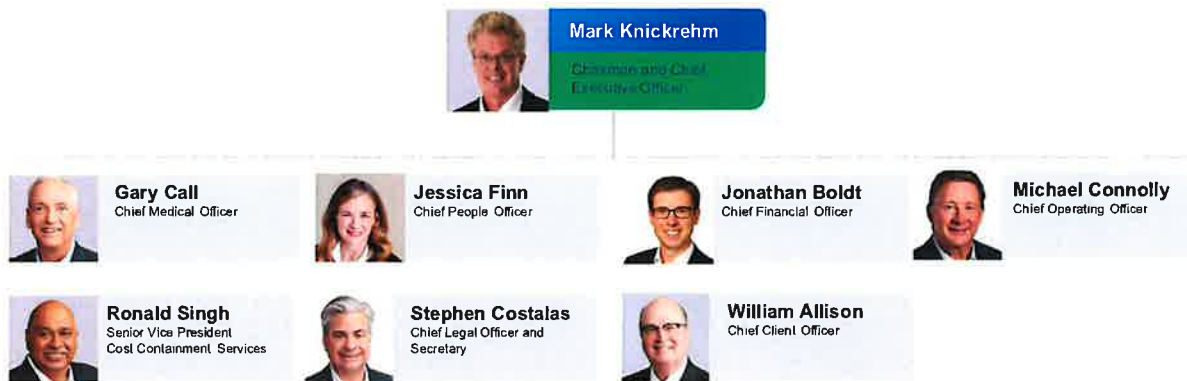
4.3.1.3. Organization and Structure

Organization and Structure: The Vendor should provide an overview of its organizational operating structure and describe the operational and functional relationships of the business units of its organization as they relate to the Vendor's proposal and the Agency's stated needs and requirements. Organizational charts are helpful supplements to the descriptions.

Gainwell's leadership and teams work closely with customers and each other to enable the underserved to get top-quality healthcare. Our management philosophy reflects a commitment to enabling our people to deliver on our mission to empower customers through innovative technologies and solutions to deliver great health and human services outcomes. Achieving this objective requires clear lines of accountability and an ongoing commitment to service excellence and continuous improvement.

Our organization chart shows the Gainwell operating structure. We are committed to maintaining the highest standards of corporate governance, essential for sustained success and long-term stakeholder value. The organization chart for the Gainwell Technologies LLC subsidiary that serves the State appears below.

Figure 7. Gainwell Technologies Corporate Leadership



Organizational and Operational Structure

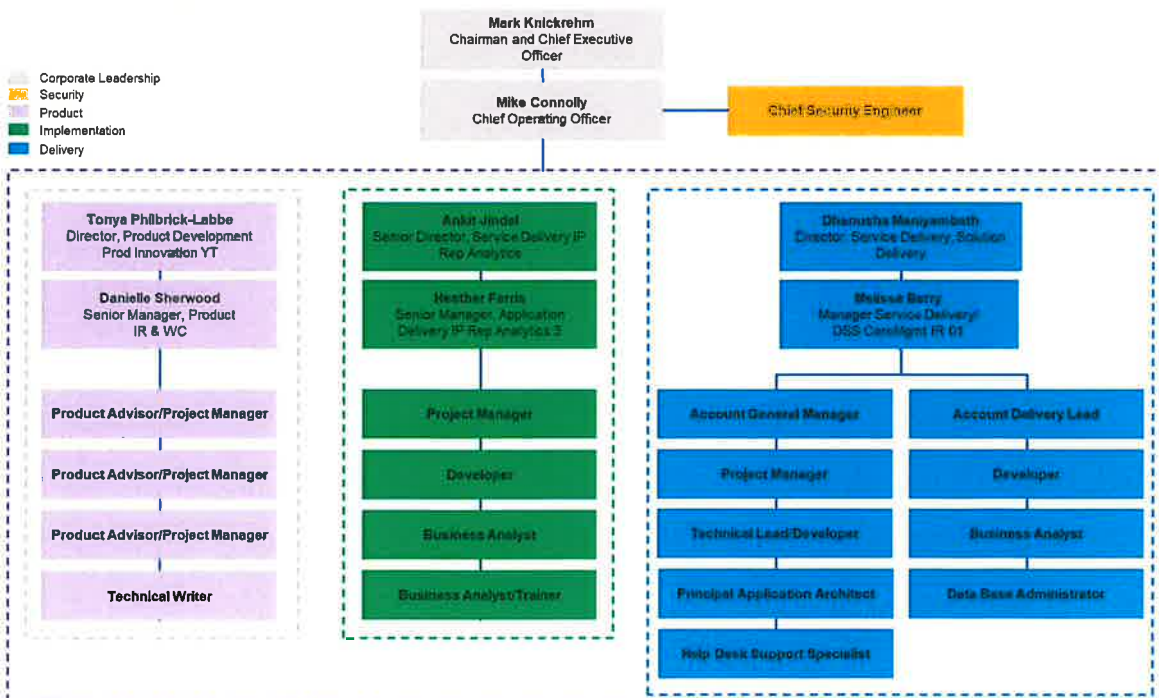
Success is not simply a factor of adopting the right technology; it is also about enlisting a capable and skilled project team with a drive for success and incorporating the tools and methods to help promote that success. This subsection describes our operational/delivery team structure and responsibilities as well as lines of authority and escalation paths.

Gainwell Operational/Delivery Team Structure

Our delivery team brings the needed experience and qualifications to the project, is available to start on contract day one, and remains appropriately allocated until the contract period ends.

The following figure presents our proposed project organization and the staff who provide the services requested in the RFP. The chart illustrates the lines of authority within the project team.

Figure 8. Project Organization Chart



4.3.1.4. Locations

Locations: The Vendor should describe the geographical locations of their firm at the national, regional, and local levels, as applicable. Identify all locations that will be used to support a resultant contract and the operations managed from these locations. Clearly identify any overseas locations which may be used to support the resultant contract. No State or Federal data may be stored on servers or systems outside of the United States of America (U.S.), including U.S. Territories.

Gainwell has nearly 13,000 employees and offices dispersed throughout the United States, including an office in West Virginia at 1201b Greenbrier St. Charleston, WV 25311.

Gainwell has a long-standing and trusted partnership with the State of West Virginia, delivering mission-critical Medicaid and health and human services solutions that support the State, its providers, and its members. With an extensive operational footprint and teams deeply familiar with West Virginia's policies, priorities, and program requirements, Gainwell is well positioned to support the State's vision for an integrated, high-performing, and equitable Medicaid enterprise.

This work is supported by Gainwell's established in-State presence, including its West Virginia office located in Charleston, reinforcing Gainwell's commitment to local engagement, responsiveness, and long-term partnership with the State.

Gainwell currently operates and supports multiple core components of West Virginia's Medicaid ecosystem, including the Medicaid Management Information System (MMIS) Claims, Encounters, and Financials (CEF), Fiscal Agent services, Pharmacy Point of Sale processing for Medicaid, CHIP, and foster care populations, and full Prescription Drug Rebate Administration. In addition, Gainwell provides comprehensive provider and member support services such as provider enrollment and screening, provider services, secure provider and member portals, call center operations, member services, and mailroom operations. These support services confirm continuity, compliance, and high-quality service delivery across the program.

Beyond these core functions, Gainwell delivers specialized program support including Early Intervention services, Third-Party Liability (TPL), Recovery Audit Contractor (RAC) services, and residency verification. Gainwell also supports a shared, multi-tenant service model serving both West Virginia and the U.S. Virgin Islands, demonstrating the scalability, security, and cost-effectiveness of its solutions while maintaining jurisdictional independence.

Gainwell has 45 offices and five data centers in the continental United States and two offices in U.S. territories. Our immunization team works remotely from locations throughout the continental United States. The data and system information components and services for our solution are located within the continental United States.

Gainwell's Account Manager and Project Manager are available to travel onsite as needed. Also, numerous project activities are scheduled to occur onsite. These include a kickoff meeting, several weeks of face-to-face requirements and design sessions, and training activities.

After implementation, Maintenance and Operations activities are coordinated remotely. In addition to regular weekly calls, we propose to conduct quarterly onsite planning and review meetings with the State. These onsite visits help promote the health of the relationship. This commitment involves having key staff visit the State's offices for two to three days each quarter. The onsite time is used to review recent activities and developments, facilitate planning, and conduct a quarterly review of relevant legislation and regulatory changes.

The solution fully complies with data center and architecture requirements, standards, and federal and State guidelines, rules, and regulations.

US East and US West Regions are discrete data centers with redundant power, networking, and connectivity, allowing for seamless failover should an incident occur. As a result, Gainwell provides more highly available, fault tolerant, and scalable production applications and databases than a single data center could accommodate.

Gainwell U.S. Office Sites

- Albany, NY
- Anchorage, AK
- Atlanta, GA
- Augusta, ME
- Austin, TX
- Baton Rouge, LA
- Bengaluru, India
- Boise, ID
- Camp Hill, PA
- Charleston, WV
- Chennai, India
- Conway, AR
- Denver, CO
- Dublin, OH
- East Hartford, CT
- El Paso, TX
- Frankfort, KY
- Hamilton, NJ
- Indianapolis, IN
- Irving, TX
- Janesville, WI
- Lenexa, KS
- Little Rock, AR
- Madison, WI
- Montgomery, AL
- Newark, DE
- Oklahoma City, OK
- Phoenix, AZ
- Raleigh, NC
- Rancho Cordova, CA
- Rancho Cucamonga, CA
- Reno, NV
- Reston, VA
- Richmond, VA
- Ridgeland, MS
- Rochester Hills, MI
- Roseville, CA
- St. Thomas, VI
- San Juan, PR
- Tallahassee, FL
- Topeka, KS
- Warwick, RI
- Washington, DC
- West Sacramento, CA
- Williston, VT

Data Centers

- Las Vegas, NV
- Orlando, FL
- Richardson, TX
- Salt Lake City, UT
- Scottsdale, AZ

4.3.1.5. References

References: The Vendor should provide three (3) references from system implementation projects or systems in operations within the last five (5) years that demonstrate the Vendor's ability to achieve the goals and objectives in Section 4.2 and meet the requirements in the RFP.

Vendors may provide only one (1) reference per project performed and should include details about the Project such as project goals and objectives, general functionality, implementation timeline, and length of time the system has been in operation if applicable.

Gainwell has successfully delivered numerous implementations across the country to fulfill a wide range of client needs. The following representative projects have been in operation within

the last five years and illustrate our ability to achieve the goals and objectives in RFP Section 4.2 and the RFP requirements.

Table 5. Reference 1 – Maryland

Organization Name	Maryland Department of Health - Prevention and Health Promotion Administration - Center for Immunization
Project Goals and Objectives	Gainwell maintains, supports, and enhances Maryland's immunization registry, ImmuNet. Since its adoption, ImmuNet has been customized to align with evolving federal and State program requirements. The system is hosted in the AWS Cloud through a third-party supplier. Gainwell provides end-to-end support for the ImmuNet application and its associated services, including installation, upgrades, enhancements, and monitoring.
General Functionality	• Delivers a fully functional IIS that meets the needs of diverse user groups and complies with critical CDC IIS Functional Standards. • Expands provider access to immunization records, supporting timely care delivery and public health decision-making. • Provides an intuitive and user-friendly IT tool that enhances end-user productivity and supports the State's long-term goals for scalability and adaptability. Strengthens data quality and enhances the State's ability to access, analyze, and leverage vaccination data stored within the IIS. • Maintains clearly delineated development, testing, and production environments, with physical network separation where necessary to provide secure configuration and operations. • Implements a robust Change Management process to govern modifications made to the system environment. Changes to the ImmuNet application are managed by Gainwell using a structured, secure process to safeguard system integrity.
Implementation Timeline	Project 1: Gainwell designed and implemented the architectural components of AWS to host the ImmuNet application and services in the cloud. In addition, we migrated the ImmuNet codebase to operate on Red Hat JBoss Enterprise Application Platform (EAP) running on the Linux operating system. Project 2: Implemented multiple enhancements to support the State's response to the COVID-19 pandemic, ongoing fall respiratory vaccine-preventable diseases, and State-funded vaccine program.
Length of Time in Operation	We have supported ImmuNet for more than 14 years.

Table 6. Reference 2 – North Carolina

Organization Name	North Carolina Department of Health and Human Services
Project Goals and Objectives	The North Carolina Immunization Registry (NCIR) is a secure, web-based clinical tool which is the official source for North Carolina immunization information. The NCIR takes the place of outdated handwritten charting of immunizations administered in the state. Immunization providers may access recorded immunizations administered in North Carolina, regardless of where the immunizations were given.
General Functionality	• Gives patients, parents, health care providers, schools, and childcare facilities timely access to complete, accurate and relevant immunization data • Assists in the evaluation of a child's immunization status and identifies children who need (or are past due for) immunizations

	- Assists communities with assessing their immunization coverage and identifying areas of under-immunization - Fulfills federal and state immunization reporting needs
Implementation Timeline	Began 2013 through 2026 (new contract for new DIIS system in progress)
Length of Time in Operation	We have supported NCIR for over 13 years.

Table 7. Reference 3 – New York

Organization Name	New York Department of Health
Project Goals and Objectives	Gainwell has been a trusted partner in supporting New York State's Immunization Information System (NYSIIS) since the system's inception, enhancing NYSIIS to adapt to evolving program needs and public health requirements. We are responsible for the ongoing maintenance and updates of NYSIIS. While the servers are hosted and maintained by the New York State Department of Health (NYS DOH), the Gainwell team coordinates closely with our internal Information Technology Services (ITS) staff to provide optimal server performance, reliability, and timely updates. Gainwell supports a broad range of activities, including: - Maintaining and updating infrastructure and software components - Installing new modules and implementing enhancements based on user and program requirements - Supporting upgrades to the latest HL7 standards - Adapting to evolving data transport mechanisms for secure and efficient data exchange - Expanding dashboards, tracking capabilities, and reporting tools for internal staff and external users - Improving data quality, completeness, and usability
General Functionality	Offered solution products installed and operational, including: - Base IR product - Lead module - Connection for Hearing - Data exchange enhancements and dashboard reporting - Assessment, Feedback, Incentives, and eXchange (AFIX) and Immunization Quality Improvement for Providers (IQIP) - Data tracking (enhanced job monitor and reporting for data exchange) - Multiple reports (ad hoc, reminder recall etc.) - Vaccines For Children (VFC) ordering and prebooking - VFC reporting - VFC enrollment - Vaccine Tracking System (VTrckS) - Vaccine inventory – auto deduction - Vaccine maintenance (module to enable easy addition and modification of vaccine codes) - Temperature logs (for user to enter into IIS) - School reports

	• Health maintenance organization (HMO) query • Mass vaccination entry • HL7/data exchange: Unsolicited Vaccination Record Update (VXU), Query for Vaccination Record (QBP)
Implementation Timeline	Initial contract implementation began in December 2006. At that time, Gainwell operated under the name EDS and played a key role in the development of NYSIIS throughout 2007. The system officially went live in January 2008.
Length of Time in Operation	We have supported NYSIIS for more than 18 years.

4.3.2. Mandatory Qualification/Experience Requirements

Mandatory Qualification/Experience Requirements - The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. The Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below

Gainwell affirms that we meet the mandatory qualifications and experience requirements identified in this solicitation.

4.3.2.1. Organizational Experience with Immunization Information Systems (IIS)

The Vendor must demonstrate organizational experience with Immunization Information Systems (IIS) or similar large-scale public health data systems in enterprise healthcare or public health settings, in compliance with all federal and state regulations within the five (5) years prior to this bid opening. Vendors may use one (1) or more of the references provided in response to Section 4.3.1.5. To satisfy this requirement.

Gainwell demonstrates extensive and ongoing organizational experience delivering, maintaining, and enhancing large-scale Immunization Information Systems (IIS) and public health data systems in enterprise healthcare and public health environments, fully compliant with applicable federal and state regulations. This experience spans multiple jurisdictions and includes continuous operational support within the five (5) years preceding this bid opening.

Maryland Department of Health – Center for Immunization (ImmuNet)

Gainwell has supported Maryland's Immunization Information System, ImmuNet, for more than 14 years and continues to provide end-to-end system support within the last five years. Gainwell maintains, supports, and enhances ImmuNet to align with evolving federal and State program requirements. The system is hosted in the AWS Cloud through a third-party supplier, with Gainwell responsible for installation, upgrades, enhancements, monitoring, and ongoing operations.

ImmuNet delivers a fully functional IIS that meets CDC IIS Functional Standards, expands provider access to immunization records, strengthens data quality, and supports secure, scalable operations through clearly separated development, testing, and production environments. Gainwell also enforces a robust change management process to confirm system integrity and regulatory compliance.

North Carolina Department of Health and Human Services (NCIR)

Gainwell has supported the North Carolina Immunization Registry (NCIR) for over 13 years, including continuous support during the past five years. NCIR is the State's official, secure, web-based immunization registry, providing healthcare providers, schools, childcare facilities, and public health stakeholders with timely access to complete and accurate immunization data.

Gainwell's support enables NCIR to meet federal and State reporting requirements, assess immunization coverage, identify under immunized populations, and replace legacy, paper based immunization tracking. Support has been continuous from 2013 through 2026, with a new DIIS system currently in progress.

New York Department of Health (NYSIIS)

Gainwell has served as a trusted partner supporting the New York State Immunization Information System (NYSIIS) since its inception and has provided uninterrupted support for more than 18 years, including the most recent five-year period. Gainwell is responsible for the ongoing maintenance, enhancement, and modernization of NYSIIS while coordinating closely with New York State Department of Health IT staff.

Support includes infrastructure and software maintenance, HL7 upgrades, secure data exchange enhancements, reporting and dashboard expansion, vaccine inventory management, VFC program support, mass vaccination entry, and improvements to data quality and usability. NYSIIS has been operational since January 2008 and continues to evolve to meet changing public health demands.

Summary

Across Maryland, North Carolina, and New York, Gainwell demonstrates proven, recent, and sustained experience delivering IIS solutions that support millions of records, diverse user communities, complex integrations, and stringent regulatory requirements. These engagements clearly satisfy the requirement for organizational experience with Immunization Information Systems or similar large scale public health data systems within the five (5) years prior to this bid opening.

Appendix A – Contract Exceptions and Clarifications

RFP Reference: RFP: Section 2.22, p. 14

22. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

Gainwell respectfully requests discussion concerning the following RFP items and General Terms and Conditions in an effort to clarify each parties responsibilities with regard to contractual obligations.

Table 8. Gainwell Contract Exceptions and Clarifications

RFP Requirement, Term, or Condition	Proposed Modification, Alternative, or Exception	Reason for Proposed Modification, Alternative, or Exception
Section 3 – General Terms and Conditions	<u>"Subcontractor" means any individual or entity that enters into a contract with the Vendor to perform either a material portion or all of Vendor's obligations under the contract. Notwithstanding the foregoing, a Subcontractor is not:</u>	Suggested edit to clarify which entities should not be considered contractors.
Section 2 Definitions	<u>1.an individual or entity that is engaged by Vendor to provide (a) services on a leveraged basis either globally or regionally for multiple Vendor customers; (b) IT Infrastructure, network, storage, hosting, or telecommunications services; (c) software or software support services; (d) contingent or supplemental staff; (e) professional services; or (f) back office services;</u>	
New Definition	<u>2. a Vendor affiliate; or</u>	
	<u>3. an ordinary course of business vendor</u>	
Section 3 – General Terms and Conditions	<u>"Vendor Confidential Information" means all non-public information provided by Vendor under this Contract which would be reasonably understood to be confidential under the circumstances of disclosure and includes without limitation all materials, processes and process flows, programs, software systems and documentation, information management systems, code, logic, analytical methodologies and algorithms, reports, analyses, data, associated proprietary forms of data organization and reports, all Vendor Pre-Existing Material, or any other information, or other work product whether or not disclosed to the State by or on behalf of Contractor pursuant to this Contract.</u>	Suggested edit to add a definition of Vendor Confidential Information.
Section 2 – Definitions		
New Definition		

RFP Requirement, Term, or Condition	Proposed Modification, Alternative, or Exception	Reason for Proposed Modification, Alternative, or Exception
Section 3 – General Terms and Conditions	<u>"Vendor Pre-existing Materials" means software, intellectual property or other proprietary data owned by Vendor prior to the effective date of this Contract, intellectual property in any works developed by Vendor independently of this Agreement and any derivatives or modifications.</u>	Suggested edit to add a definition of Vendor Pre-existing materials.
Section 2 – Definition		
New Definition		
Section 3 – General Terms and Conditions	<u>"Work Product" means the tangible and intangible results of the work, whether finished or unfinished, including drafts. Work Product includes, but is not limited to, documents, text, software (including source code), research, reports, proposals, specifications, plans, notes, studies, data, images, photographs, negatives, pictures, drawings, designs, models, surveys, maps, materials, ideas, concepts, know-how, and any other results of the work, that are created solely and exclusively for the State and paid for with the intent that the State will own the results of the work. "Work Product" does not include any (i) Vendor Pre-Existing Material; (ii) any other material that was developed prior to the Effective Date or that is improved or modified thereafter that is used in the performance of the work; (iii) any deliverable that is specifically intended by the Parties not to be owned by the State; (iv) Vendor Confidential Information; (v) any third party product(s) utilized by Vendor in providing the services.</u>	Suggested edit to add a definition of Work Product.
Section 2- Definitions		
New Definition		
Section 3 – General Terms and Conditions	Cyber Liability Insurance in an amount of: \$10,000,000.00 per occurrence <u>claim</u> .	Edit made to align with Vendor's Cyber Liability insurance policy that is on a "claims made" basis.
Section 8 - Insurance		
Section 3 – General Terms and Conditions	ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated. <u>Vendor hereby</u>	Suggested edit to clarify that Vendor has presented exceptions for consideration as part of its RFP response.
Section 12 - Acceptance		

RFP Requirement, Term, or Condition	Proposed Modification, Alternative, or Exception	Reason for Proposed Modification, Alternative, or Exception
	<u>otherwise indicates Vendor's exceptions to certain Terms and Conditions and RFP statements in its Exceptions Document and Vendor's signature on its proposal is submitted subject to considerations of its Exceptions.</u>	
Section 3 – General Terms and Conditions	Time – Time is of the essence regarding all matters of time and performance in this Contract	Edit made to align with Vendor's understanding that all applicable deadlines are articulated in the applicable contract documents.
Section 20 - Time		
Section 3 – General Terms and Conditions	ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent (said consent not to be unreasonably withheld) of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments. <u>Vendor may assign to a qualified affiliate, or by virtue of sale, merger, corporate reorganization or operation of law upon at least thirty (30) days advance written notice to the State.</u>	Edit made to allow for certain permitted assignments through corporate transactions or operation of law.
Section 27 - Assignment		
Section 3 – General Terms and Conditions	WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; <u>and</u> (b) be merchantable and fit for the purpose intended. <u>The Vendor disclaims all other warranties, including those of merchantability and fitness for a particular purpose;</u> and (c) be free from defect in material and workmanship.	Edit made to align the Indemnification provision with an existing agreement between the State and Vendor
Section 28 - Warranty		
Section 3 – General Terms and Conditions	<u>The State shall keep confidential, and cause its agents, employees, contractors, and others under its control, to keep confidential, all Vendor Confidential Information, and the State shall not, without prior written approval of the Contractor, use, publish, copy, disclose to any third party, or permit the use by any third party of any Vendor Confidential Information, except as required by law.</u>	Edit made to provide for the protection of Vendor Confidential Information.
Section 30 – Privacy, Security and Confidentiality		
Add a new Section		

RFP Requirement, Term, or Condition	Proposed Modification, Alternative, or Exception	Reason for Proposed Modification, Alternative, or Exception
Section 4 – Project Specifications 4.2.3.13.4	Formal Acceptance: Upon successful completion of all Acceptance activities, the Agency will issue a written Notice of Acceptance. Only upon issuance of this Notice may the Vendor invoice for implementation-related fees. No annual, recurring, subscription, hosting, or maintenance fees may begin prior to Acceptance. <u>If, upon completion of the acceptance testing time period, the Agency fails to provide written notice to Vendor confirming successful testing completion, then Vendor may provide the Agency with a written notice notifying the Agency that the time has passed and providing the Agency with ten (10) days to submit any errors or objections. If the Agency fails to respond to such notice, then Acceptance shall have been deemed to occur without further notification from the Agency.</u>	Edit made to provide for default acceptance.
Attachment C - Service Level Agreements Section 1(b) and (c)	b. Performance Standard: Monthly uptime must be $\geq$ 99.9 <u>99.5</u>% (Down less than 43 minutes and 50 seconds per month). c. Retainage: 99.0%–99.89 <u>99.5</u>% uptime: 5 <u>1</u>% of monthly invoice 95.0%–98.99% uptime: 25 <u>5</u>% of monthly invoice < 95.0% uptime: 400 10% of monthly invoice	Edit made to align with industry practice.
Attachment C - Service Level Agreements New Definition	<u>At Risk Amount: "At Risk Amount" shall mean fifteen percent (15%) of the Monthly Charges for such month, which is the maximum amount the Vendor will have at risk for Services Levels as set forth in Attachment C for such month.</u>	Edit made to a maximum "at risk" amount.
Attachment C - Service Level Agreements New Definition	<u>Excused Performance: Vendor shall not be responsible for a failure to meet any Service Level to the extent provided below:</u> <u>1. State or State's third-party contractor's acts, errors or omissions. State and State third party contractors will include other contractors.</u> <u>2. Willful misconduct or violations of law by the State or its third-party contractors.</u>	Edit made to provide excused performance as to events outside of Vendor's control.

RFP Requirement, Term, or Condition	Proposed Modification, Alternative, or Exception	Reason for Proposed Modification, Alternative, or Exception
	<u>3. Service or resource reductions requested or approved by the State and agreed to by the Parties through the Change Control Process; provided that Contractor has previously notified State in writing as part of such Change Control Process that the implementation of such request would result in such failure to meet the Service Level.</u>	
Attachment C - Service Level Agreements New Definition	<u>Single Incident: If a single incident results in the failure of Vendor to meet more than one (1) Service Level Agreement (SLA), the State shall have the right to select any one of such multiple SLA defaults for which it will be entitled to receive Retainage. The State shall not be entitled to a Retainage for each of such SLA default. For purposes of this metric a "Single Incident" means the occurrence of something that results in an unplanned interruption to or a quality reduction of a service.</u>	Edit made to provide clarification in dealing with multiple SLAs failures arising from a single event.

Appendix B – Bidder Certification and Authorization

REQUEST FOR PROPOSAL

CRFP MIS2700000001-Immunization Information System

Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $\$1,000,000 / \$1,000,000 = \text{Cost Score Percentage of } 1 (100\%)$
Step 2 – $1 \times 30 = \text{Total Cost Score of } 30$

Proposal 2: Step 1 – $\$1,000,000 / \$1,100,000 = \text{Cost Score Percentage of } 0.909091 (90.9091\%)$
Step 2 – $0.909091 \times 30 = \text{Total Cost Score of } 27.27273$

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Gainwell Technologies LLC

(Company)

 President and CEO

(Representative Name, Title)

Phone 703.245.4600 / Fax 469.320.5153

(Contact Phone/Fax Number)

August 18, 2026

(Date)

Appendix C – Designated Contact and Certification Signature

Please see the following page for Gainwell's Designated Contact and Certification Signature.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Adam Moyer, Account General Manager

(Address) 225 East John Carpenter Freeway, Suite 500, Irving, TX 75062

(Phone Number) / (Fax Number) 712.308.0598 / 469.320.5153

(email address) amoyer@gainwelltechnologies.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through WV OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Gainwell Technologies LLC

(Company)

(Signature of Authorized Representative)

Mark Knickrehm, President and CEO August 18, 2026

(Printed Name and Title of Authorized Representative) (Date)

703.245.4600 / 469.320.5153

(Phone Number) (Fax Number)

mark.knickrehm@gainwelltechnologies.com

(Email Address)

Appendix D – Federal Funds Addendum

Please see the following pages for Gainwell's signed Federal Funds Addendum.

FEDERAL FUNDS ADDENDUM

REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

The State of West Virginia Department of Administration, Purchasing Division, and the Vendor awarded this Contract intend that this Contract be compliant with the requirements of the Procurement Standards contained in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements found in 2 C.F.R. § 200.317, et seq. for procurements conducted by a Non-Federal Entity. Accordingly, the Parties agree that the following provisions are included in the Contract.

1. MINORITY BUSINESSES, WOMEN'S BUSINESS ENTERPRISES, AND LABOR SURPLUS AREA FIRMS: (2 C.F.R. § 200.321)

- a. The State confirms that it has taken all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. Those affirmative steps include:
 - (1) Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
 - (2) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
 - (3) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
 - (4) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;
 - (5) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and
 - (6) Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (1) through (5) above.
- b. Vendor confirms that if it utilizes subcontractors, it will take the same affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible.

2. DOMESTIC PREFERENCES: (2 C.F.R. § 200.322)

- a. The State confirms that as appropriate and to the extent consistent with law, it has, to the greatest extent practicable under a Federal award, provided a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United

States (including but not limited to iron, aluminum, steel, cement, and other manufactured products).

b. Vendor confirms that will include the requirements of this Section 2. Domestic Preference in all subawards including all contracts and purchase orders for work or products under this award.

c. Definitions: For purposes of this section:

(1) "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

(2) "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

3. BREACH OF CONTRACT REMEDIES AND PENALTIES:

(2 C.F.R. § 200.327 and Appendix II)

(a) The provisions of West Virginia Code of State Rules § 148-1-5 provide for breach of contract remedies, and penalties. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

4. TERMINATION FOR CAUSE AND CONVENIENCE:

(2 C.F.R. § 200.327 and Appendix II)

(a) The provisions of West Virginia Code of State Rules § 148-1-5 govern Contract termination. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

5. EQUAL EMPLOYMENT OPPORTUNITY:

(2 C.F.R. § 200.327 and Appendix II)

Except as otherwise provided under 41 CFR Part 60, and if this contract meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3, this contract includes the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

6. DAVIS-BACON WAGE RATES:
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this Contract includes construction, all construction work in excess of \$2,000 will be completed and paid for in compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must:

- (a) pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.
- (b) pay wages not less than once a week.

A copy of the current prevailing wage determination issued by the Department of Labor is attached hereto as Exhibit B. The decision to award a contract or subcontract is conditioned upon the acceptance of the wage determination. The State will report all suspected or reported violations to the Federal awarding agency.

7. ANTI-KICKBACK ACT:
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that it will comply with the Copeland Anti-KickBack Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). Accordingly, Vendor, Subcontractors, and anyone performing under this contract are prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The State must report all suspected or reported violations to the Federal awarding agency.

8. CONTRACT WORK HOURS AND SAFETY STANDARDS ACT
(2 C.F.R. § 200.327 and Appendix II)

Where applicable, and only for contracts awarded by the State in excess of \$100,000 that involve the employment of mechanics or laborers, Vendor agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Vendor is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

9. RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT.
(2 C.F.R. § 200.327 and Appendix II)

If the Federal award meets the definition of “funding agreement” under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency.

10. CLEAN AIR ACT
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this contract exceeds \$150,000, Vendor is to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251–1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

11. DEBARMENT AND SUSPENSION
(2 C.F.R. § 200.327 and Appendix II)

The State will not award to any vendor that is listed on the governmentwide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

12. BYRD ANTI-LOBBYING AMENDMENT
(2 C.F.R. § 200.327 and Appendix II)

Vendors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

13. PROCUREMENT OF RECOVERED MATERIALS

(2 C.F.R. § 200.327 and Appendix II; 2 C.F.R. § 200.323)

Vendor agrees that it and the State must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

14. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

(2 C.F.R. § 200.327 and Appendix II; 2 CFR § 200.216)

Vendor and State agree that both are prohibited from obligating or expending funds under this Contract to:

- (1) Procure or obtain;
- (2) Extend or renew a contract to procure or obtain; or
- (3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115–232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
 - (i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
 - (ii) Telecommunications or video surveillance services provided by such entities or using such equipment.
 - (iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

In implementing the prohibition under Public Law 115–232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

State of West Virginia

Vendor Name: Gainwell Technologies LLC

By: _____

By:  _____

Printed Name: _____

Printed Name: Mark Knickrehm

Title: _____

Title: President and CEO

Date: _____

Date: August 18, 2026

	Matching Factor 90% or higher		
	<i>Matched</i>	<i>Blank*</i>	<i>Totals</i>
<i>Admin System</i>	61	0	61
<i>Manage orgs</i>	83	0	83
<i>Manage users</i>	35	0	35
<i>Interop</i>	65	0	65
<i>Data quality - Deduplication</i>	32	0	32
<i>Eval forecast</i>	64	0	64
<i>Manage pt iz record</i>	83	0	83
<i>Manage vaccine inv</i>	87	0	87
<i>Data Access</i>	65	0	65
<i>Nonfunctional</i>	99	0	99
Totals	674	0	674

**Blanks = The confidence matching algorithm was less than 90%*

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

Guidance: Using the RTM	Step-by-step guidance and helpful hints/notes for using the RTM as part of a procurement process.
Functional Model	Draft IIS Functional Model (FM), a visual depiction of IIS functions and capabilities and attributes.
FM Descriptions	Descriptions of the IIS Functional Model functions and capabilities and attributes; also provides an indication of total requirements by function/category
RTM Format	Description of how the RTM is structured for presentation of the requirements.
Requirements by Function/Grouping:	
Admin System	Requirements related to the function: Administer System
Manage Orgs	Requirements related to the function: Manage Organizations and Facilities
Manage Users	Requirements related to the function: Manage Users
Interop	Requirements related to the function: Support Interoperability
Data Quality	Requirements related to the function: Ensure Data Quality
Eval Forecast	Requirements related to the function: Evaluate & Forecast
Manage Pt Iz Record	Requirements related to the function: Manage Patient & Immunization Records
Manage Vaccine Inventory	Requirements related to the function: Manage Vaccine Inventory
Data Access	Requirements related to the function: Provide Data Access
Non-functional	Technical requirements across key attributes
Glossary	List of terms used in requirements and their definitions
Crosswalk to FS	Compare the Functional Model to the IIS Functional Standards (FS)

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

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.

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

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.
- **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

-- On each tab, high-level requirements are shaded in blue; rows beneath each high level requirement provide further detail.

requirements, label with 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 cycle.

may be warranted to 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 reference to the statute/rule.



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 phil.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	Manage Organizations & Facilities	Manage Users
- Hierarchy configuration - System configuration - User roles & permissions - System alerts	- Organization/facility search - Add, edit, inactivate organization/facility - VFC/vaccine program enrollment - Organization/facility outreach	- User search - Add, edit, inactivate user - Authentication & authorization - Password management
Support Interoperability	Ensure Data Quality	Evaluate & Forecast
- Onboarding - Interfaces - Data exchange	- Patient matching & deduplication - Vaccination event matching & deduplication	- Clinical decision support - Reminder/recall - Coverage reports
Manage Patient & Immunization Records	Manage Vaccine Inventory	Provide Data Access
- Patient search - Add, edit patient demographics - Patient status - Patient consent - Add, edit patient immunization - Print/export record - Mass vaccination	- Vaccine inventory search - Add, edit vaccine inventory - Vaccine ordering - Review/approve order - Vaccine decrementing - Vaccine inventory reconciliation - Vaccine transfer - Vaccine wastage - Vaccine expiration	- 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/hmc-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 phil.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 System Configuration User Roles and Permissions System Alerts	– ability to create hierarchy that informs the association between geographical levels within the jurisdiction and among organizations, facilities, – ability to define system-wide settings, such as management of code tables – ability to define and manage user roles and use role permissions to perform a function, activity or task – 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 Add, Edit, Inactivate VFC/Vaccine Program Organization/Facility User Search	– ability to look up and retrieve an organization or facility account – ability to add, edit or inactivate an organization or facility; ability for an organization to initiate enrollment and re-enrollment in the IIS – ability to enroll and re-enroll a provider organization in VFC and/or other vaccine program(s) – ability to communicate with organization/facility representatives
Manage Users	35	Manage Users	Management of user accounts.	Add, Edit, Inactivate User Authentication and Password Management Onboarding Interfaces Data Exchange	– ability to define parameters to look up and retrieve a user account – ability to add, edit or inactivate a user account – ability to validate a user's identity, entity and system permissions – ability to administer, change and reset user passwords – ability to establish/re-establish/modify an interface with another information system for the electronic exchange of demographic and/or – ability to facilitate electronic data exchange with other information systems, including EHRs, VTrckS, jurisdictional vital records, and the IZ Gateway – ability to exchange data electronically and monitor and troubleshoot data exchange
Interop	65	Support Interoperability	Manage interfaces to exchange data between the IIS and other systems.	Patient Matching and Vaccination Event Matching Clinical Decision Support Reminder/Recall Coverage Reports	– ability to identify and manage duplicate and potential duplicate patient records – ability to identify and manage duplicate and potential duplicate vaccination entries – ability to evaluate and forecast immunizations for a patient per ACIP guidelines and in alignment with CDSi specifications – ability to identify and notify patients who are due for upcoming immunizations (reminder) and/or are past due (recall) – ability to create reports to support immunization coverage assessment at the provider and geographic levels including reports for the CDC's VFC
Data Quality	32	Ensure Data Quality	Deduplication and consolidation of records.	Patient Search Add, Edit Patient Patient Status Patient Consent Add, Edit Patient Print/Export Report Mass Vaccination	– ability to look up and retrieve a patient record – ability to add, edit or inactivate a patient record – ability to manage the assignment of a specific patient to a provider organization or jurisdiction – ability to manage patient agreement to participate in the IIS in accordance with jurisdictional policy – ability to add, edit an immunization record – ability to print or export either a patient or immunization record – ability to capture a large volume of demographic and immunization data in emergency situations
Eval Forecast	64	Evaluate and Forecast	Determine the validity of past immunizations administered as a basis for determining	Vaccine Inventory Search Add, Edit Vaccine Inventory Vaccine Ordering Review/Approve Order Vaccine Dose Decrementing Vaccine Inventory Vaccine Transfer Vaccine Wastage Vaccine Expiration Standard Reports Ad Hoc Queries and Reports Print/Export Report Consumer Access	– ability to look up and retrieve vaccine doses in inventory – ability to manage vaccine inventory, including ordering, storing and handling, and reconciliation of vaccine doses – ability to order publicly funded vaccines as authorized – ability to review, edit, and authorize an organization's vaccine order for approval, submission and fulfillment – ability to automatically decrement vaccine doses from inventory when matched vaccine doses are reported as administered – ability to maintain an accurate count of vaccine doses available based on doses administered, wasted, transferred, and expired – ability to transfer vaccine from one VFC provider organization to another in certain situations – ability to manage nonviable vaccine reporting – ability for notification and management of vaccine inventory expired and due to expire – ability to generate pre-configured reports available and accessible in the IIS – ability to create, save and schedule data queries and customized reports on demand – ability to generate data to print or use in other systems – ability for authorized consumers to directly access IIS data for which they are authorized
Manage Pt Iz Record	83	Manage Patient and Immunization Records	Manage patient demographics and patient immunization record.		
Manage Vaccine Inv	87	Manage Vaccine Inventory	Order publicly-purchased vaccine and manage vaccine inventory.		
Data Access	65	Provide Data Access	Provision of access to data and information.		
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 Resource utilization Capacity Operability User error protection Accessibility Availability Fault tolerance Recoverability Confidentiality Non-repudiation Accountability	– degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements – degree to which the amounts and types of resources used by a product or system, when performing its functions, meet requirements – degree to which the maximum limits of a product or system parameter meet requirements – degree to which a product or system has attributes that make it easy to operate and control – degree to which a system protects users against making errors – 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 – degree to which a system, product or component is operational and accessible when required for use – degree to which a system, product or component operates as intended despite the presence of hardware or software faults – 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 – degree to which a product or system ensures that data are accessible only to those authorized to have access – degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later – degree to which the actions of an entity can be traced uniquely to the entity
		Usability	Degree to which a product or system can be used by specified users to achieve specified goals		
		Reliability	Degree to which a system, product or component performs specified functions under		
		Security	Degree to which a product or system protects information and data so that persons or other		

IIS Functional Model descriptions

[Return to Cover Page](#)

Tab Name	# of Reqs	Function	Function Description	Capability	Capability Description
			products or systems have the	Authenticity	– degree to which the identity of a subject or resource can be proved to be the one claimed
		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
		Portability	Degree of effectiveness and	Adaptability	– degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or
			efficiency with which a system,	Installability	– degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment
674					

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)
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

Status	Req. #	Capability	Requirement: The IIS must/should...	Comments	Reviewer notes	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
		Hierarchy Configuration	ability to establish the IIS hierarchy to associate and manage relationships between entities			E	Yes	The solution provides configurable hierarchy management that enables authorized administrators to establish and maintain organizational and facility relationships within the IIS. Parent-child relationships can be defined and managed through the Facility Hierarchy function, providing a visual representation of hierarchical relationships and supporting administration, reporting, security, and operational workflows across the organization.
		Hierarchy Configuration	ability to associate user(s) to a facility			E	Yes	The solution enables authorized administrators to associate users with one or more facilities through configurable role-based security. User assignments determine facility access, permissions, and operational responsibilities, ensuring users have appropriate access to perform activities within their assigned facilities.
		Hierarchy Configuration	ability to associate clinician(s) to a facility			E	Yes	The solution enables authorized administrators to associate clinicians with one or more facilities through the facility profile. Clinician assignments support vaccine administration, ordering, clinical documentation, and reporting while maintaining active/inactive status and clinician role designations.
		Hierarchy Configuration	ability to associate facility/facilities to an organization			E	Yes	The solution supports configurable organizational hierarchies that associate one or more facilities with an organization through parent-child relationships. Administrators can establish and maintain facility relationships, and the Facility Hierarchy visualization provides a graphical representation of the organizational structure to support administration, reporting, and operational management.
		Hierarchy Configuration	ability to establish geographic jurisdictional hierarchy			E	Yes	The solution supports establishment of geographic and jurisdictional hierarchies through configurable organizational structures, districts, counties, jurisdictions, and facility relationships. Facilities may be associated with jurisdiction-defined geographic areas, enabling administration, security, reporting, vaccine management, and operational oversight based on jurisdictional boundaries. Geographic attributes, including county and district, are maintained as part of the facility profile, and integrated geocoding services support address validation and geographic classification.
		Hierarchy Configuration	ability to aggregate data across user-defined hierarchies			E	Yes	The solution supports aggregation of data across user-defined organizational, facility, geographic, demographic, and program hierarchies through both Custom Reports and a comprehensive library of standard reports. Authorized users can define report criteria using configurable filters such as facility, district, county, jurisdiction, patient demographics, priority groups, vaccine information, dates, status, and other available data elements to produce aggregated results that meet operational, clinical, and public health reporting needs.
		System Configuration	ability to maintain inventory availability in IIS visible to authorized users			E	Yes	The solution provides real-time visibility into vaccine inventory for authorized users through role-based security. Users can view current inventory availability, including vaccine, manufacturer, lot number, funding source, funding program, quantity on hand, expiration date, days until expiration, ordering intent, and inventory status. Inventory availability is automatically updated through vaccine administration, shipments, transfers, reconciliation, borrowing/repayment, and inventory adjustments to ensure users have an accurate view of available inventory.
		System Configuration	ability for jurisdictional admin to maintain separate VFC supplied inventory in the IIS			E	Yes	The solution maintains VFC-supplied vaccine inventory separately through configurable funding sources and funding programs. Inventory is tracked at the lot level and associated with the appropriate funding program, supporting independent inventory management, ordering, reconciliation, reporting, borrowing/repayment, and accountability for VFC vaccine.
		System Configuration	ability for jurisdictional admin to maintain separate jurisdiction supplied inventory			E	Yes	The solution maintains jurisdiction-supplied vaccine inventory separately through configurable funding sources and funding programs (e.g., State, Section 317, Pandemic, and other jurisdiction-defined programs). Inventory is tracked independently at the lot level, supporting program-specific ordering, inventory management, reporting, and reconciliation.
		System Configuration	ability for jurisdictional admin to maintain separate private stock inventory			E	Yes	The solution maintains private vaccine inventory independently from publicly funded inventory using configurable funding sources and funding programs. Private inventory is managed separately throughout the inventory lifecycle, including ordering, administration, transfers, borrowing/repayment, reporting, and reconciliation, ensuring appropriate inventory accountability.
		System Configuration	ability for jurisdictional admin to manage code sets			E	Yes	The solution maintains vaccine reference data through an automated integration with CDC-maintained reference services. Gainwell imports vaccine code updates directly from the CDC using CDC APIs, ensuring vaccine groups, CVX codes, manufacturer (MVX) codes, and other nationally standardized reference data remain current without requiring manual jurisdiction maintenance. This automated approach reduces administrative burden, improves data consistency, and ensures timely adoption of newly released vaccines and manufacturers.
		System Configuration	ability for jurisdictional admin to update NDC codes			E	Yes	The solution maintains vaccine reference data through an automated integration with CDC-maintained reference services. Gainwell imports vaccine code updates directly from the CDC using CDC APIs, ensuring vaccine groups, CVX codes, manufacturer (MVX) codes, and other nationally standardized reference data remain current without requiring manual jurisdiction maintenance. This automated approach reduces administrative burden, improves data consistency, and ensures timely adoption of newly released vaccines and manufacturers.
		System Configuration	ability for jurisdictional admin to update CVX codes			E	Yes	The solution maintains vaccine reference data through an automated integration with CDC-maintained reference services. Gainwell imports vaccine code updates directly from the CDC using CDC APIs, ensuring vaccine groups, CVX codes, manufacturer (MVX) codes, and other nationally standardized reference data remain current without requiring manual jurisdiction maintenance. This automated approach reduces administrative burden, improves data consistency, and ensures timely adoption of newly released vaccines and manufacturers.

		System Configuration	ability for jurisdictional admin to update MVX codes			E	Yes	The solution maintains vaccine reference data through an automated integration with CDC-maintained reference services. Gainwell imports vaccine code updates directly from the CDC using CDC APIs, ensuring vaccine groups, CVX codes, manufacturer (MVX) codes, and other nationally standardized reference data remain current without requiring manual jurisdiction maintenance. This automated approach reduces administrative burden, improves data consistency, and ensures timely adoption of newly released vaccines and manufacturers.
		System Configuration	ability to configure default values to minimize data input			E	Yes	The solution utilizes configurable default values and automated field population throughout the application to minimize manual data entry and improve user efficiency. Based on the workflow being performed, the solution automatically populates information such as current date, patient demographics, vaccine manufacturer, lot number, funding source, funding program, dose size, dose quantity, Vaccine Information Statement (VIS), facility information, inventory selection, and other contextual data. Gainwell will configure default values in collaboration with the State to align with jurisdiction's business processes, reducing data entry, improving consistency, and minimizing user errors.
		System Configuration	ability to display an error message in the user interface when minimum information required is not complete			E	Yes	The solution provides configurable user interface validation that displays clear error messages when required information has not been completed. Required fields are identified throughout the application, and users receive immediate feedback identifying missing or invalid information before records can be saved or submitted. Gainwell will configure validation rules in collaboration with the State to support jurisdiction's business and data quality requirements.
		System Configuration	ability to standardize addresses per US Postal conventions and codes			E	Yes	The solution standardizes patient and organization addresses using near real-time address validation through Smarty (formerly SmartyStreets). During data entry, addresses are validated against United States Postal Service (USPS) conventions and standardized to USPS-compliant formatting, including address components, abbreviations, ZIP+4, and associated geographic information where applicable. Validated addresses are flagged within the patient record, and the solution records the date of the most recent address verification, improving data quality, reducing duplicate records, and supporting accurate mail delivery and jurisdictional reporting.
		System Configuration	ability to verify validity of addresses (as valid USPS addresses) in the IIS through electronic means (e.g., SmartyStreets)			E	Yes	The solution electronically verifies patient and organization addresses through near real-time integration with Smarty (formerly SmartyStreets). During address entry and maintenance, the solution validates addresses against United States Postal Service (USPS) reference data to confirm address validity and deliverability. Successfully validated addresses are identified as USPS-verified, and the solution records the address verification status and the date of the most recent verification, improving data quality, patient matching, and mail delivery accuracy.
		System Configuration	ability to geocode addresses			E	Yes	The solution supports geocoding of patient and organization addresses through near real-time integration with Smarty (formerly SmartyStreets). Following address validation, the solution assigns geographic coordinates and associated geographic attributes, such as latitude, longitude, county, census tract, legislative district, and other jurisdictional boundaries, as available. Geocoded information supports jurisdiction assignment, patient matching, reporting, mapping, reminder/recall activities, and public health analytics.
		System Configuration	ability to validate accurate assignment of address to an individual through electronic means (e.g., LexisNexis)			O	Yes	Gainwell's Residency Verification tool, an optional add-on, allows for an individual's address to be validated for assignment to that individual.
		System Configuration	ability for jurisdictional admin to modify facility types according to immunization program descriptions and CDC VFC Program descriptions			E	Yes	The solution supports configurable facility types and related reference data. Gainwell maintains nationally standardized reference values, including CDC-supported program classifications, while working with the Jurisdiction to configure jurisdiction-specific facility types, enrollment classifications, and operational values that support immunization program administration and reporting.
		System Configuration	ability for jurisdictional admin to configure rules governing data validation of incoming HL7 messages			E	Yes	The solution provides configurable DFI rules governing validation of incoming HL7 messages. Gainwell can configure validation rules to verify required fields, message structure, code values, and business logic before data is accepted into the IIS, improving data quality and reducing manual correction efforts.
		System Configuration	ability to configure an authorization agreement as per jurisdictional policy			O	Yes	The solution supports configurable authorization agreements that can be tailored to jurisdiction's policies. Jurisdiction administrators may configure agreement content, presentation frequency etc. using a built rich text editor feature.
		System Configuration	ability to configure a user agreement as per jurisdictional policy			O	Yes	The solution supports configurable authorization agreements that can be tailored to jurisdiction's policies. Jurisdiction administrators may configure agreement content, presentation frequency etc. using a built rich text editor feature.
		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	The proposed solution includes the patient's age in year/month/day format both in the user interface (UI) and respective reports.
		System Configuration	ability to provide optional calendar to select a date in a web client			O	Yes	The solution provides an integrated calendar control throughout the web application, allowing users to select dates through a graphical calendar or manual entry while supporting consistent date validation and formatting.
		System Configuration	ability to add patient priority group indicators	Particularly relevant for mass vaccination.		E	Yes	The solution supports configurable patient priority groups. Authorized users can assign, modify, and maintain jurisdiction-defined priority group indicators to support targeted vaccination programs, reporting, reminder/recall activities, and public health response efforts.
		System Configuration	ability to modify patient priority group indicators	Particularly relevant for mass vaccination.		E	Yes	The solution supports configurable patient priority groups. Authorized users can assign, modify, and maintain jurisdiction-defined priority group indicators to support targeted vaccination programs, reporting, reminder/recall activities, and public health response efforts.
		System Configuration	ability for jurisdictional admin to manage business rules related to data quality			E	Yes	The solution provides configurable data quality management capabilities that allow jurisdiction administrators to define and maintain business rules governing data completeness, validation, consistency, and acceptance. These configurable rules support automated validation and improve overall data quality throughout the IIS.
		System Configuration	ability for jurisdictional admin to specify business rules for monitoring data quality			E	Yes	The proposed Solution allows for monitoring of incoming data and allows Jurisdictional Administrators to provide access for vendors or facilities via Role-Based Access Control (RBAC) to view and address data errors.

	System Configuration	ability for jurisdictional admin to modify business rules for monitoring data quality			E	Yes	The solution provides configurable data quality management capabilities that allow jurisdiction administrators to define and maintain business rules governing data completeness, validation, consistency, and acceptance. These configurable rules support automated validation and improve overall data quality throughout the IIS.
	System Configuration	ability to configure the organization enrollment form			E	Yes	The solution provides a configurable electronic enrollment workflow. Gainwell will configure enrollment forms, required questions, statuses, workflows, approval processes, agreement requirements, and renewal schedules in collaboration with the State to support jurisdiction's operational and program requirements.
	System Configuration	support rules-based logic to suggest approval or rejection of enrollment form based on review of completed fields			E	Yes	The solution provides a configurable rules-based enrollment workflow that automatically evaluates enrollment submissions against jurisdiction-defined business rules. Required fields, supporting documentation, electronic signatures, and other configured validation criteria are reviewed to recommend approval or rejection before administrative review. This automated validation improves data quality, reduces manual review effort, and promotes consistent application of jurisdiction's enrollment policies.
	System Configuration	ability to manage rules-based logic for approval or rejection of enrollment form			E	Yes	The solution supports enrollment approval workflows, documentation requirements, approval criteria, and workflow logic in collaboration with jurisdiction to ensure enrollment recommendations align with jurisdictional policies and operational requirements.
	System Configuration	ability for jurisdictional admin to create enrollment forms based on program requirements			E	Yes	Gainwell will configure electronic enrollment forms to support jurisdiction's program requirements. Enrollment forms may be tailored to capture jurisdiction-specific demographic information, program participation, required documentation, electronic acknowledgments, certifications, and other information necessary to support provider enrollment and ongoing program administration.
	System Configuration	ability for jurisdictional admin to modify an enrollment form			E	Yes	Gainwell will configure and maintain electronic enrollment forms in collaboration with jurisdiction. As program requirements evolve, enrollment forms, required fields, workflow steps, validation rules, certifications, and supporting documentation requirements can be updated to support changing jurisdictional and program needs.
	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	The solution automatically populates available existing user and facility information during the enrollment process to minimize duplicate data entry. Existing demographics, contact information, and other available IIS information are reused where appropriate, improving data quality and streamlining facility enrollment.
	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	The solution automatically populates available organization and facility information during the enrollment process to reduce manual data entry and improve consistency. Information submitted through the electronic enrollment workflow can be used to create or update organization and facility records, supporting efficient onboarding while maintaining data integrity through configurable validation and approval workflows.
	System Configuration	ability for jurisdictional admin to configure vaccine forecasting business rules			E	Yes	The solution automatically imports and maintains the baseline CDC Clinical Decision Support for Immunization (CDSI) schedules, recommendations, and forecasting rules, ensuring alignment with current CDC guidance without manual rule creation. Building on this baseline, Gainwell's Flexible Forecaster provides a configurable forecasting framework that enables authorized jurisdiction administrators to create and manage jurisdiction-specific forecasting schedules while preserving the underlying CDSI logic. Administrators can configure vaccine series, dose definitions, age recommendations, dose intervals, cessation rules, conflict rules, invocation rules, skip-dose logic, and other jurisdiction-specific forecasting rules through a comprehensive schedule management interface. The solution also provides complete version control, audit history, schedule comparisons, and a read-only CDSI viewer to maintain transparency and simplify ongoing schedule management.
	System Configuration	ability to apply effective dates to vaccine rules			O	Yes	The solution automatically imports and maintains the baseline CDC Clinical Decision Support for Immunization (CDSI) schedules, recommendations, and forecasting rules, ensuring alignment with current CDC guidance without manual rule creation. Building on this baseline, Gainwell's Flexible Forecaster provides a configurable forecasting framework that enables authorized jurisdiction administrators to create and manage jurisdiction-specific forecasting schedules while preserving the underlying CDSI logic. Administrators can configure vaccine series, dose definitions, age recommendations, dose intervals, cessation rules, conflict rules, invocation rules, skip-dose logic, and other jurisdiction-specific forecasting rules through a comprehensive schedule management interface. The solution also provides complete version control, audit history, schedule comparisons, and a read-only CDSI viewer to maintain transparency and simplify ongoing schedule management.
	System Configuration	ability to incorporate new vaccines per ACIP into the forecasting algorithm			E	Yes	The solution automatically imports and maintains the baseline CDC Clinical Decision Support for Immunization (CDSI) schedules, recommendations, and forecasting rules, ensuring alignment with current CDC guidance without manual rule creation. Building on this baseline, Gainwell's Flexible Forecaster provides a configurable forecasting framework that enables authorized jurisdiction administrators to create and manage jurisdiction-specific forecasting schedules while preserving the underlying CDSI logic. Administrators can configure vaccine series, dose definitions, age recommendations, dose intervals, cessation rules, conflict rules, invocation rules, skip-dose logic, and other jurisdiction-specific forecasting rules through a comprehensive schedule management interface. The solution also provides complete version control, audit history, schedule comparisons, and a read-only CDSI viewer to maintain transparency and simplify ongoing schedule management.
	System Configuration	ability to support a record search algorithm to return "best matches"			E	Yes	The IIS supports the ability to return best matches as defined within the user input. It will also take into consideration the swapping of names (i.e., first name entered as last or last entered as first) to return the best possible match.
	System Configuration	ability for jurisdictional admin to configure the number of search results to be displayed per jurisdictional policy			E	Yes	The solution enables authorized Jurisdiction Administrators to configure the maximum number of patient search results returned by the system in accordance with jurisdictional policy. Administrators may define the maximum number of potential matches displayed before requiring users to further refine their search criteria, balancing user efficiency with patient matching accuracy and system performance. This configurable setting helps reduce ambiguous search results while supporting jurisdiction's patient matching and privacy policies.
	System Configuration	ability for jurisdictional admin to modify required parameters for patient searches			E	Yes	Gainwell will configure the required patient search parameters, including which search fields are mandatory, in collaboration with jurisdiction to support the State's patient matching policies and operational requirements.

	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	The solution includes a variety of standard reports that are designed to appropriately limit or exclude sensitive demographic information based on the report's intended purpose. For example, the Confidential Immunization Record is designed to provide immunization history while limiting the inclusion of sensitive demographic data. Gainwell will work with jurisdiction during implementation to configure report content and available data elements to meet the State's privacy, security, and operational requirements, ensuring sensitive information (such as addresses, telephone numbers, mother's maiden name, Medicaid ID, and other protected data) is included only where appropriate and authorized.
	System Configuration	ability to open multiple screens simultaneously within the application			O	Yes	The solution allows users to work efficiently with multiple reports, generated documents, reference materials, and external resources simultaneously by opening them in separate browser tabs or downloading them for side-by-side review. This enables users to reference supporting information while continuing their work within the IIS. To protect data integrity and system security, the solution intentionally restricts multiple concurrent transactional application sessions under the same user credentials. This design reduces the risk of duplicate transactions, conflicting updates, and session misuse and aligns with secure session management best practices consistent with NIST SP 800-63B Digital Identity Guidelines. This approach provides users with the flexibility to access supporting information concurrently while preserving the integrity of transactional workflows.
	User Roles and Permissions	ability for jurisdictional admin to manage user roles and permissions by task per jurisdictional policy			E	Yes	The solution provides comprehensive Role-Based Access Control (RBAC) that enables authorized Jurisdiction Administrators to manage user roles and permissions at a task level. Administrators can configure access to specific application modules, menus, pages, reports, administrative functions, and individual actions (e.g., view, create, edit, delete, approve) in accordance with Jurisdiction's jurisdictional security policies. Role permission changes are maintained through built-in audit capabilities and role access reporting.
	User Roles and Permissions	ability for jurisdictional admin to add user roles with distinct permissions			E	Yes	The solution enables authorized Jurisdiction Administrators to create new user roles with distinct, configurable permission sets. Each role may be configured with unique access to application modules, pages, reports, workflows, administrative functions, and data, allowing jurisdiction to establish security roles that align with operational responsibilities while enforcing the principle of least privilege.
	User Roles and Permissions	ability for jurisdictional admin to modify user roles with distinct permissions			E	Yes	The solution enables authorized Jurisdiction Administrators to modify existing user roles by updating their associated permissions and access rights. Permission changes are centrally managed through the configurable Role/Page Access administration component and are automatically applied to all users assigned to the role. All role modifications are captured through the built-in audit history and can be reviewed using the Role/Page Access Report and Role Audit Report, supporting security, compliance, and governance.
	User Roles and Permissions	ability for jurisdictional admin to inactivate user roles			E	Yes	The solution enables authorized Jurisdiction Administrators to create, modify, activate, and inactivate user roles through the configurable Role Management component. Jurisdiction Administrators can also delegate responsibility by granting designated administrative roles the authority to manage, and assign user roles within their authorized scope. Roles may be configured with distinct permission sets governing access to application pages, reports, administrative functions, workflows, and data. Inactivated roles are retained for historical and audit purposes but are no longer available for assignment until reactivated. All role configuration changes are captured through the built-in audit history and Role/Page Access reporting to support security, compliance, and governance.
	User Roles and Permissions	ability for jurisdictional admin to modify permissions to IIS processes and data for specific user roles			E	Yes	Once user accounts are established, Jurisdiction Administrators can refine the user account by designating one or more roles. Further, Jurisdiction Administrators can configure the processes and data that users are permitted to access by selecting the appropriate Solution pages/tasks by role via the Role/Page Access configuration matrix.
	User Roles and Permissions	ability for jurisdictional admin to restrict system functionality by user role			E	Yes	The solution provides comprehensive, configurable Role-Based Access Control (RBAC) that enables authorized Jurisdiction Administrators to manage permissions for individual user roles. Administrators can configure access to specific menus, pages, functions, and data elements, allowing security to be tailored to jurisdiction's operational and security requirements. Changes to role permissions are tracked through an audit history and may be reviewed using built-in role access and audit reports.
	User Roles and Permissions	ability for jurisdictional admin to restrict authorized user access to data based on user role			E	Yes	The solution enables Jurisdiction Administrators to restrict system functionality at a granular level by user role. Access may be controlled for individual application pages, menus, administrative functions, reports, configuration options, and operational workflows. This configurable approach ensures users only have access to the functions necessary to perform their assigned responsibilities.
	User Roles and Permissions	ability for jurisdictional admin to enable access to standard reports based on user role			E	Yes	The solution enables Jurisdiction Administrators to control access to standard reports through configurable Role-Based Access Control (RBAC). Report visibility and execution permissions are assigned by role, allowing jurisdictions to determine which users may view, generate, export, or administer specific reports while protecting sensitive information and supporting jurisdiction's security policies.
	User Roles and Permissions	ability to automatically update all users assigned to a role based on changes made to the "master" role attributes			E	Yes	The solution utilizes a centralized Role-Based Access Control (RBAC) model in which permissions are managed at the role level. When authorized administrators modify the permissions, privileges, or attributes of a role, the changes are automatically inherited by all users assigned to that role, eliminating the need to update individual user accounts. This centralized approach simplifies security administration, ensures consistent access controls, and supports compliance with jurisdiction's security policies.

		System Alerts	ability for jurisdictional admin to manage system alerts			E	Yes	The solution enables authorized jurisdictional administrators to directly manage system alerts and notifications through configurable administrative tools. Jurisdictions can create and maintain system banner messages and control whether communications are displayed pre-login and/or post-login , allowing timely communication of system maintenance, program updates, emergencies, or other important information without requiring Gainwell intervention. The solution also provides configurable notification management that allows the jurisdiction to determine which system events generate notifications and which user roles receive them. This gives jurisdictions direct control over operational communications and enables alerts and notifications to evolve with program needs and workflows.
		System Alerts	ability to view global messages upon logging into the application			E	Yes	Banner messages can be configured to be displayed on the sign-in page for global messaging on the home page and other solution pages. Banners can be displayed to specific or multiple users or groups based on configurable criteria. Viewable messages are targeted to users' organization, role, or another cohort (e.g., vaccine management user roles view one banner upon login, while inventory management user roles view another). Banners display prominently at the top of the page.
		System Alerts	ability for jurisdictional admin to add system alerts for specific IIS users to view when logging into application			O	Yes	Authorized users can create and modify banner messages to be displayed on the sign-in page for global messaging and by role(s) on the home page and other Solution pages.
		System Alerts	ability for jurisdictional admin to add global messages			E	Yes	Authorized users can create and modify banner messages to be displayed on the sign-in page for global messaging on the home page and other Solution pages.
		System Alerts	ability for jurisdictional admin to edit global messages			E	Yes	Authorized users can create and modify banner messages to be displayed for global messaging.
		System Alerts	ability for jurisdictional admin to inactivate global messages			E	Yes	Authorized Jurisdictional can activate/inactivate global messages.

Status	Req. #	Capability	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)
		Organization/Facility Search	ability to search organization/facility information stored in the IIS			E	Yes	Authorized users can search organizations and facilities using configurable search criteria, including organization name, facility name, PIN, enrollment status, organization type, vaccine program participation, address, and other jurisdiction-defined attributes. Search results support sorting, filtering, and direct navigation to organization and facility records.
		Organization/Facility Search	ability for jurisdictional admin to search organizations/facilities by user-defined parameters			E	Yes	Authorized administrators can also view the User Facilities table to search, view, and edit organizations/facilities, their status, and associated roles.
		Organization/Facility Search	ability to clear and re-enter search criteria when searching for an organization/facility			E	Yes	Jurisdictional administrators can view or sort by facility Name, PIN, Enrollment Type, Enrollment Year, Status, Action Notes, and Last Updated Date.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized (non-participating/enrolled) organization to enroll electronically for participation in the IIS			E	Yes	Configurable Enrollment Workflows: The solution allows administrators to create configurable enrollment workflows tailored to their specific requirements, capturing essential information such as facility and personnel details, training history, and program requirements. Online Agreement Submission: Providers can conveniently submit their enrollment agreements online through a secure web portal, eliminating the need for paper-based forms and manual data entry. Automated Workflows: Automated workflows guide Providers through the enrollment process step by step, providing prompts and reminders for incomplete or missing information to confirm applications are submitted accurately and on time. Document Uploads and Verification: Providers can upload supporting documents, such as transcripts, certificates, and identification proof, directly within the solution. Administrators can then verify and review these documents digitally, expediting the application review process. Communication Tools: Built-in communication tools enable administrators to send automated notifications, updates, and reminders to applicants via email and system notification and messaging, keeping them informed about the status of their agreements and additional requirements.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized organization to add IIS enrollment information online			E	Yes	The proposed Solution has a validated (via email confirmation) and protected page that allows for unenrolled users/facilities to submit electronic enrollment. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized org to submit IIS enrollment information online			E	Yes	The proposed Solution has a validated (via email confirmation) and protected page that allows for unenrolled users/facilities to submit electronic enrollment. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized org to save partially complete IIS enrollment information			O	Yes	The solution allows for a partially completed enrollment to be saved in a draft status.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized org to return to a partially complete IIS enrollment information			O	Yes	The solution allows for a partially completed enrollment to be saved in a draft status to return for completion.
		Add, Edit, Inactivate Organization	ability to prevent submission of incomplete IIS enrollment information when required field(s) are missing			E	Yes	We apply business-rules-based data quality edits to verify completeness of information. Rules are configurable to allow authorized users to define rules for what constitutes "complete" by identifying required and optional data.
		Add, Edit, Inactivate Organization	ability to electronically notify the applicant of incomplete IIS enrollment information specifying the missing required fields			E	Yes	Based on the configured data quality rules, the proposed solution automatically validates the data submission and returns the appropriate response, including notifying applicants when required enrollment information is missing. Error messages are prominently displayed at the top of the screen so users can quickly pinpoint the error and make the necessary correction.
		Add, Edit, Inactivate Organization	ability to electronically notify applicant that IIS enrollment information has been submitted			E	Yes	Confirmation messages are displayed to users upon submission of enrollment information. The confirmation messages are user-friendly and easy to understand, providing plain-language text and prompting the user to confirm before proceeding.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized org to edit rejected IIS enrollment information			E	Yes	The applicant will receive an email notification of the rejected enrollment to allow them to edit and resubmit it for approval. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Add, Edit, Inactivate Organization	ability for applicant from unauthorized org to resubmit a rejected IIS enrollment			E	Yes	Our proposed Solution will email the applicant of the rejected IIS enrollment to allow them to edit and resubmit for approval.
		Add, Edit, Inactivate Organization	ability to capture electronic signature for enrollment, for an authorization agreement			O	Yes	The proposed Solution's provider enrollment process is fully automated and provides e-signature capabilities and an automated workflow for jurisdictional approval.
		Add, Edit, Inactivate Organization	ability for jurisdictional admin to manage organization/facility IIS enrollment			E	Yes	Our proposed Solution allows for the Jurisdictional Administrator to configure and manage the facility enrollment and reenrollment requirements.
		Add, Edit, Inactivate Organization	ability for jurisdictional admin to manage organization/facility IIS enrollment status			E	Yes	The solution allows quick view, view, and print of enrollments by status; mass exports of enrollments will be configured.
		Add, Edit, Inactivate Organization	ability for jurisdictional admin to inactivate an organization			E	Yes	Authorized administrators can perform deactivation within the Add/Edit facility tile, administrators can search to locate facilities/organizations to deactivate or reactivate the account by toggling the Active field. The Status drop-down menus and available values are configurable within the solution.
		Add, Edit, Inactivate Organization	ability for jurisdictional admin to reactivate an organization			E	Yes	Authorized administrators can search to locate one or more facilities/organizations and deactivate or reactivate the account by updating the Status field to Active or Inactive.

	Add, Edit, Inactivate Organization	ability to store IIS enrollment status for an organization/facility		E	Yes	The solution allows for clinic status to be active or inactive.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to inactivate a facility		E	Yes	Authorized administrators can search to locate one or more facilities/organizations and deactivate or reactivate the account by updating the Status field to Active or Inactive
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to reactivate a facility		E	Yes	Authorized administrators can search to locate one or more facilities/organizations and deactivate or reactivate the account by updating the Status field to Active or Inactive
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to electronically approve IIS enrollment		E	Yes	Authorized users can review and approve enrollment forms.
	Add, Edit, Inactivate Organization	ability to include reason for rejecting IIS enrollment of an organization		E	Yes	The solution allows for a Jurisdictional Administrator to provide a reason and notes related to enrollment rejections.
	Add, Edit, Inactivate Organization	ability to electronically notify the organization that the submitted enrollment was rejected along with the reason		E	Yes	The applicant will receive an email notification of the rejected enrollment to allow them to edit and resubmit it for approval.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to manage organization and facility records within the IIS		E	Yes	Authorized administrators can search, view, add, and update organization/facility records according to role-based access defined for them.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to add an organization		E	Yes	Authorized administrators can search, view, add, and update organization/facility records according to role-based access defined for them.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to modify an organization record		E	Yes	Authorized administrators can search, view, add, and update organization/facility records according to role-based access defined for them.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to add a facility		E	Yes	Authorized administrators can search, view, add, and update organization/facility records according to role-based access defined for them.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to modify a facility record		E	Yes	Authorized administrators can search, view, add, and update organization/facility records according to role-based access defined for them.
	Add, Edit, Inactivate Organization	ability to automatically generate unique facility IIS ID		E	Yes	The proposed solution can generate and assign unique facility IIS IDs.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to associate a facility to an organization		E	Yes	Jurisdictional Administrators can associate facilities and organizations to establish parent and child relationships and hierarchy via the Facility Hierarchy function.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to edit association between a facility an organization		E	Yes	Jurisdictional Administrators can edit facilities' and organizations' parent/child relationships and hierarchy.
	Add, Edit, Inactivate Organization	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	The proposed Solution can capture and identify multiple facility IDs to allow for matching between data systems.
	Add, Edit, Inactivate Organization	ability to capture a facility's mailing address		E	Yes	The solution allows for wildcard searches within facility as well as throughout the solution. The proposed Solution captures and validates the facility's mailing address using Smarty.
	Add, Edit, Inactivate Organization	ability to capture a facility's shipping address		E	Yes	The proposed Solution captures and validates the facility's shipping address using Smarty.
	Add, Edit, Inactivate Organization	ability to enter contact information for the facility contact		E	Yes	The proposed Solution captures facility contact information and has the ability for updates.
	Add, Edit, Inactivate Organization	ability to enter contact information for an optional contact		E	Yes	The proposed Solution allows for multiple contacts and their contact information as well as edits.
	Add, Edit, Inactivate Organization	ability to indicate if an organization/facility is a site where immunizations are administered	Particularly relevant for mass vaccination.	E	Yes	Whether a facility or organization is a site where immunizations are being administered can be captured within the solution's facility/organization demographics information.
	Add, Edit, Inactivate Organization	ability to indicate if an organization/facility is a site where vaccines are stored for redistribution	Particularly relevant for mass vaccination.	O	Yes	The proposed Solution captures if a facility/organization is a site where vaccines are stored for redistribution on the facility demographics.
	Add, Edit, Inactivate Organization	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	The solution includes the ability to upload, download, and view files to support jurisdictional needs, including storage and handling, borrowing (if allowed), temperature logs, digital data logger reports, interior vaccine storage units (pictures), exterior vaccine storage units (pictures) DDL certificate of calibration, FQHC or RHC cortication, do not unplug (picture), and other documents as needed. These are stored within the facility documents component. The Jurisdiction Administrator can easily view related documents using the facility explorer.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to retrieve electronic files from provider file folder		E	Yes	The proposed solution allows for authorized users to retrieve electronic files from the provider file folder.
	Add, Edit, Inactivate Organization	ability for jurisdictional admin to record notes related to a organization/facility		E	Yes	Notes can be captured within the organization/facility.
	Add, Edit, Inactivate Organization	ability to flag an organization as participating in VFC and/or other user-defined vaccine program(s)		E	Yes	The proposed Solution provides the ability to flag a facility/organization as participating in VFC or other user-defined vaccine programs within the facility demographics and within enrollment.
	Add, Edit, Inactivate Organization	ability to retrieve organization/facility information from scanned forms and automatically fill required data fields with retrieved information		O	Yes	The solution can use Amazon Textract, which extracts text, handwriting, layout elements, and data from scanned documents. There is an additional expense for this service that is dependent on the number of pages that need to be scanned. Gainwell will need to have State volumes provided to add the additional expense for this service.
	VFC/Vaccine Program Enrollment	ability for an organization to submit vaccine program enrollment information electronically		E	Yes	The solution allows for an organization to entirely complete, submit, and e-sign enrollment forms.

		VFC/Vaccine Program Enrollment	ability to capture electronic signature for vaccine program enrollment			E	Yes	Electronic signatures can be captured for the vaccine enrollment. The Solution also allows for a user to send an electronic request for signature for a signing authority that is not an authorized user. Example Vaccine coordinator (IIS authorized user) completes vaccine enrollment and request medical director (not an authorized user) to e-sign.
		VFC/Vaccine Program Enrollment	ability to access the vaccine program agreement in a separate window from the vaccine program enrollment			E	Yes	A viewable and printable version of the completed vaccine provider agreement is available in a separate window.
		VFC/Vaccine Program Enrollment	ability to provide link to the blank formatted vaccine program enrollment form			E	Yes	Blank formatted enrollment forms can be downloaded and printed.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to assign a VFC pin number to a newly enrolled VFC site			E	Yes	Authorized Jurisdictional Administrators can assign a VFC PIN to a newly enrolled VFC site.
		VFC/Vaccine Program Enrollment	ability to select the type of certified monitoring device being used to record temperatures			E	Yes	The proposed Solution captures unit type, temperature scale, and style and can capture temperature monitoring device being used.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to document that a facility has a certificate of calibration for the temperature monitoring device			O	Yes	Facility-specific documentation can be uploaded to support the VFC program, including certificates of calibration.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to approve a vaccine program enrollment			E	Yes	Jurisdictional Administrators can approve or reject a vaccine program enrollment.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to enter an expiration date for a vaccine program enrollment			E	Yes	Jurisdictions can enter an expiration date for vaccine program enrollment at an overall level or at a facility/organization if the jurisdiction would like to manage the vaccine enrollment facilities at an individual level.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to document that the vaccine program facility has a routine and emergency vaccine management plan			E	Yes	An electronic enrollment workflow enables a vaccine storage, handling, and accountability plan. Within the plan, the user is expected to include details about their emergency plans such as power outages.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to document that a facility participating in VFC has a VFC Coordinator annual training certificate			E	Yes	Annual training can be marked complete with a date of completion for the primary VFC coordinator.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to document that a facility participating in VFC has a Backup Coordinator annual training certificate			E	Yes	Annual training can be marked complete with a date of completion for the backup VFC coordinator.
		VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to add comments during the vaccine program enrollment approval process			O	Yes	The proposed Solution allows for notes/comments to be added during the vaccine program enrollment approval process.
		VFC/Vaccine Program Enrollment	ability to require the vaccine program facility to indicate the number of vaccine storage units being monitored			O	Yes	The proposed Solution captures the units being monitored by unit name, unit type, temp scale, and style.
		VFC/Vaccine Program Enrollment	ability to require the vaccine program facility to indicate the types of vaccine storage units being monitored			O	Yes	The proposed Solution captures the units being monitored by unit name, unit type, temp scale, and style.
		VFC/Vaccine Program Enrollment	ability to require the vaccine program facility to indicate whether they store Varicella and MMRV vaccine			E	Yes	Authorized users can indicate whether the facility is frozen vaccine eligible.
		VFC/Vaccine Program Enrollment	ability to enter contact information for the facility Primary Vaccine Coordinator			E	Yes	Authorized users can indicate and modify the primary vaccine coordinator and their contact information.
		VFC/Vaccine Program Enrollment	ability to enter contact information for the facility Backup Vaccine Coordinator			E	Yes	Authorized users can indicate and modify the backup vaccine coordinator and their contact information.
		VFC/Vaccine Program Enrollment	ability to enter contact information for the facility vaccine program Agreement Signatory			E	Yes	The proposed Solution allows the documentation of multiple facility contacts and signatory. It also allows for the signatory to be emailed a copy of the agreement to sign digitally without requiring the signatory to have a user login.
		VFC/Vaccine Program Enrollment	ability to capture the day of the week that a vaccine program facility may receive vaccine shipments			E	Yes	The facility/organization can indicate their availability by day and time (AM and PM) to receive vaccine shipments.
		VFC/Vaccine Program Enrollment	ability to capture the time that a vaccine program facility may receive vaccine shipments			E	Yes	The facility/organization can indicate their availability by day and time (AM and PM) to receive vaccine shipments.
Updated		VFC/Vaccine Program Enrollment	ability to automatically turn off vaccine ordering capabilities for a facility that does not have an up-to-date vaccine program enrollment			E	Yes	Authorized users can configure the Solution to disallow ordering when a vaccine enrollment is not up to date or not in an approved status.
		VFC/Vaccine Program Enrollment	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	The proposed Solution captures the first, last, title, medical license number, NPI, facility association, signing authority, and specialty during the enrollment process.

	VFC/Vaccine Program Enrollment	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	Facility-specific documentation can be uploaded within the document management component.
	VFC/Vaccine Program Enrollment	ability for IIS staff to retrieve electronic files from organization/facility file folder			O	Yes	The proposed Solution allows for authorized users to retrieve electronic files from the organization/facility file folder.
	VFC/Vaccine Program Enrollment	ability to automatically validate clinician license number against Professional Licensing Agency record database			O	Yes	We support NPI API - for NPI verification we would need a state API or other connectivity to verify as there is no federal licensing available. There is not a federal licensing board to verify medical license numbers.
	VFC/Vaccine Program Enrollment	ability to submit vaccine program re-enrollment data electronically			E	Yes	A fully electronic enrollment workflow allows facilities/organizations to submit expected vaccine enrollment information for jurisdictional approval. The proposed Solution allows for enrollment and re-enrollment within the vaccine program entirely electronically.
	VFC/Vaccine Program Enrollment	ability to electronically notify a facility VFC/vaccine program coordinator of an upcoming need for VFC/vaccine program re-enrollment			O	Yes	The proposed Solution has the ability for jurisdictional users to send system messages to facilities about upcoming program requirements, including re-enrollment.
	VFC/Vaccine Program Enrollment	ability for the jurisdictional vaccine program admin to modify the date for online renewal electronic notifications for each vaccine program facility			E	Yes	Jurisdictional Administrators can configure enrollment periods, including the enrollment window and associated renewal dates. Notifications are generated based on the configured enrollment period.
	VFC/Vaccine Program Enrollment	ability to suspend ordering capabilities for a facility pending approval of vaccine program enrollment			E	Yes	The Solution supports automatic suspension of vaccine ordering for facilities without an approved enrollment agreement. Ordering can be suspended automatically at the enrollment period end date or managed manually by jurisdictional administrators.
	VFC/Vaccine Program Enrollment	ability to re-activate ordering capabilities for a facility when a vaccine program enrollment is approved			E	Yes	The Solution automatically restores ordering capabilities once the vaccine program enrollment is approved.
	Organization/Facility Outreach	ability to send electronic communications to organization/facility contacts			E	Yes	Electronic notifications can be sent to facility/organization contacts.
	Organization/Facility Outreach	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	Electronic notifications can be sent to facilities for renewals that needed to be completed by their expiration date.
	Organization/Facility Outreach	ability to send electronic communications directly from the IIS			O	Yes	The proposed Solution has the ability to electronically send communications directly from Immunization Solution. Gainwell has incorporated this functionality into the core Immunization Solution product.
	Organization/Facility Outreach	ability to send electronic communications directly from the IIS to multiple recipients			O	Yes	The proposed Solution has the ability to electronically send communications directly from Immunization Solution. Gainwell has incorporated this functionality into the core Immunization Solution product.
	Organization/Facility Outreach	ability to notify more than one user at a participating vaccine program facility of any vaccine program notification			O	Yes	The proposed Solution can electronically send communications through global banners, notifications (role/facility), and direct messages (role/facility).
	Organization/Facility Outreach	ability for the jurisdictional vaccine program admin to customize vaccine program enrollment alerts to participating vaccine program facilities when needed			O	Yes	The proposed Solution can electronically send communications through global banners, notifications (role/facility), and direct messages (role/facility).
	Organization/Facility Outreach	ability for the jurisdictional vaccine program admin to modify the date for online renewal electronic notifications for each participating vaccine program facility			O	Yes	Jurisdictional Administrators can configure vaccine program enrollment periods, including renewal windows and the timing of electronic renewal notifications for participating vaccine program facilities. Notifications are generated based on the configured renewal schedule.
	Organization/Facility Outreach	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	The proposed Solution can electronically send communications through global banners, notifications (role/facility), and direct messages (role/facility).

Function: Manage Users

[Return to Cover Page](#)

Status	Req. #	Capability	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)
		User Search	ability for jurisdictional admin to search for user accounts by user-defined criteria			E	Yes	The solution enables authorized Administrators to search for user accounts using configurable search criteria, including user name, organization, facility, role, status, email address, user type, and other jurisdiction-defined attributes. Search results can be refined, sorted, and filtered to efficiently locate user accounts for administration and management activities.
		User Search	ability for jurisdictional admin to view all user accounts			E	Yes	The solution enables authorized Administrators to view and manage all user accounts within their assigned jurisdiction based on role-based security permissions. User account information includes associated organizations, facilities, assigned roles, account status, and other administrative details necessary to support user management.
		User Search	ability for organization admin to search all user accounts associated with their organization			E	Yes	The solution enables Organization Administrators to search for and manage user accounts associated with their organization. Search capabilities support configurable criteria and return only those users within the administrator's authorized organizational scope, ensuring appropriate security and administrative oversight.
		User Search	ability for organization admin to view all user accounts associated with their organization			E	Yes	The solution enables Organization Administrators to view all user accounts associated with their organization through configurable role-based security. User account information includes assigned facilities, roles, account status, and other administrative details necessary to manage organizational access.
		User Search	ability to sort users by user defined-criteria			O	Yes	The solution enables authorized administrators to search, sort, and filter user accounts using configurable criteria such as user name, organization, facility, role, account status, email address, and other jurisdiction-defined attributes. These capabilities allow administrators to efficiently locate and manage user accounts while supporting role-based access control.
		Add, Edit, Inactivate User	ability for admin to manage user accounts			E	Yes	The solution provides comprehensive user lifecycle management through configurable role-based administration. Authorized administrators can search, view, create, modify, activate, deactivate, and manage user accounts, including facility associations, assigned roles, account status, password management, and organizational access. Complete account history and administrative actions are maintained to support auditing, security, and compliance.
Added		Add, Edit, Inactivate User	ability to track the progress of a new user registration			O	Yes	This is currently part of the Provider Registration process, available from the login screen for jurisdictions who choose to utilize it. When a new facility chooses to register, a new user is automatically created as part of that process, which is monitored through the steps both automatically and then manually within the Pending Facilities section of the Create/Edit facilities page.
		Add, Edit, Inactivate User	ability for admin to add new users			E	Yes	The solution enables authorized administrators to create new user accounts through a secure, role-based user administration workflow. During user creation, administrators capture user demographic and contact information, assign facilities and roles, configure account status, and optionally generate and electronically distribute initial passwords. The solution also supports bulk creation of multiple users assigned to the same facility and role, significantly reducing administrative effort during onboarding.
		Add, Edit, Inactivate User	ability for admin to modify user accounts			E	Yes	The solution enables authorized administrators to modify user accounts through a centralized user administration interface. Administrators can update user demographic information, contact information, assigned facilities, roles, account status, passwords, and security settings. The solution also supports activation and deactivation with configurable deactivation reasons while maintaining a complete account history of administrative actions, modifications, and status changes to support auditing and compliance.
		Add, Edit, Inactivate User	ability for admin to inactivate user accounts			E	Yes	The solution enables authorized administrators to inactivate user accounts when access is no longer appropriate or required, supporting secure user lifecycle management and jurisdictional control over system access.
		Add, Edit, Inactivate User	ability for jurisdictional admin to inactivate multiple accounts in one transaction			O	Yes	Authorized Jurisdictional Administrators can view and modify account status through the Add/Edit User function. Authorized administrators can also view and modify the User Facilities table described previously to search, view, and edit organizations/facilities, their status, and associated roles. Update capabilities include allowing authorized users to change the status for one account, multiple accounts, or all accounts in one transaction.
		Add, Edit, Inactivate User	ability for organization admin to inactivate user accounts associated with their organization			E	Yes	The solution enables authorized Administrators to inactivate user accounts associated with their organization based on role-based security permissions. Inactivation immediately removes system access while preserving user information, facility assignments, account history, and audit records.
		Add, Edit, Inactivate User	ability to store reason for inactivation of user account			E	Yes	The solution enables authorized administrators to document and retain the reason for user account inactivation, supporting accountability, auditability, and administrative oversight of user access changes.
		Add, Edit, Inactivate User	ability for jurisdictional admin to reactivate an inactivated account			E	Yes	Authorized Administrators can reactivate previously inactivated user accounts through the user administration interface. Reactivation restores user access while preserving account history, assigned roles, facility associations, and audit information.
		Add, Edit, Inactivate User	ability to electronically notify a user that their account is locked (inaccessible) as per jurisdictional security policy			O	Yes	The proposed solution can notify users that their account is inaccessible.
		Add, Edit, Inactivate User	ability to electronically notify a user that their account is inactive			O	Yes	The solution supports electronic notification to inform users when their account has been inactivated, providing timely communication of account status changes and reducing administrative follow-up.
		Add, Edit, Inactivate User	capture clinician activity status (out of state, loss of certification, change of practice status, other)			O	Yes	The proposed solution has an Application Programming Interface (API) with the National Provider Identification (NPI) system to capture license status.
		Add, Edit, Inactivate User	ability for jurisdictional admin to assign a role to authorized users			E	Yes	The solution enables authorized Administrators to assign and manage user roles through configurable Role-Based Access Control (RBAC). Administrators can assign one or more jurisdiction-defined roles to users, associate roles with one or more facilities, and modify permissions as organizational responsibilities change. Role assignments determine the user's access to application functions, data, and administrative capabilities while supporting jurisdiction's security and governance requirements.
		Add, Edit, Inactivate User	ability for organization admin to assign a role to authorized users within their organization			E	Yes	The solution enables authorized Administrators to assign and manage user roles for users within their organization based on configurable Role-Based Access Control (RBAC) permissions. Organization Administrators may assign organization-approved roles, associate users with one or more facilities, and update user access as responsibilities change, while remaining within the administrative authority granted by the jurisdiction.

	Authentication & Authorization	ability to authenticate user		E	Yes	Identity Federation/Single Sign-on (SSO) will occur through integration with the jurisdiction's Identity and Access Management (IAM) capabilities to identify and authenticate users.
	Authentication & Authorization	ability to access the system through an authorized username and password		E	Yes	Authorized users log into the solution by entering a valid username and password. Users will have forgotten-username and forgotten-password services available on the sign on page.
	Authentication & Authorization	ability to support access via single-sign in for jurisdictional users		O	Yes	Solution integrates with the SSO capability using jurisdiction standards for login and authentication.
	Authentication & Authorization	ability to switch between multiple organizations		O	Yes	A user account can be assigned to more than one role, and roles can be assigned to more than one user account. When the user logs in, they select the facility/organization account they are logging into from a drop-down menu of organizations associated to their user account via the Switch Facility Screen. When the user selects their organization for the first time, they are presented with the user agreement. After accepting the agreement, they are presented with the solution features and functions associated with the user permissions set up for their role by the Organizational Administrator. What a user can see and do within the solution differs based on the organization the user logs into and the role-based permissions defined for that organization.
	Authentication & Authorization	ability to view jurisdictional policy agreements		E	Yes	Configurability allows the proposed solution to be easily tailored to meet state-specific needs. Examples of this configurability include updating the login process to specify whether or not the user agreement appears, how often it appears, and the text that is displayed. At a minimum, users see the jurisdictional policy agreement upon first logging in.
	Authentication & Authorization	support multi-factor authentication per jurisdictional policy		O	Yes	The proposed Solution provides NIST compliant multi-factor authentication (MFA) for privileged/administrative and other identified access.
	Password Management	ability to generate electronic notification to authorized user of account credentials		E	Yes	Electronic notifications can be issued for user credentials for authorized users.
	Password Management	ability to electronically notify authorized users of their username		E	Yes	Electronic notifications can be issued for authorized users of their username.
	Password Management	ability to electronically notify authorized users of their temporary password in a separate notification		E	Yes	Electronic notifications can be issued for auto-generated temporary passwords.
	Password Management	ability to generate electronic notification at periodic intervals to authorized users of their pending account password expiration		E	Yes	Electronic notifications can be issued for pending account password expiration, and timing of notifications can be configured by the Jurisdictional Administrator.
	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	The proposed Solution has the ability for the jurisdiction to manage notifications for users nearing account expiration.
	Password Management	ability to support temporary password which will be required to change during initial log in		E	Yes	The proposed solution supports required password changes at initial login.
	Password Management	ability to support temporary password which will expire in X number of days determined by policy		E	Yes	The proposed solution supports jurisdictional policies for password expirations.
	Password Management	ability for users to change their own passwords per program/jurisdiction security policy		E	Yes	Users can change their own password based on jurisdiction password policies.
	Password Management	ability for users to reset their password per program/jurisdiction security policy		E	Yes	The solution enables users to securely reset their passwords in accordance with applicable program and jurisdiction security policies. Password management controls can be configured to align with jurisdiction-defined requirements for password security, expiration, and account protection.
	Password Management	ability to prompt users to change their password at time intervals per program/jurisdiction security policy		E	Yes	Users can reset their own password based on jurisdiction password policies.

Status	Req. #	Capability	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)
		Onboarding	ability to onboard organizations/facilities to facilitate electronic data exchange			E	Yes	Facilities/organizations can exchange data using CDC's WSDL following the HL7 2.5.1 guide.
		Onboarding	ability to track an organization's/facility's progress through the onboarding process			O	Yes	The Immunization Solution proposed leverages the enrollment function to track facility onboarding activities and expectations.
		Onboarding	ability to capture EHR system specification details			E	Yes	The solution captures and maintains EHR and interface-specific configuration details for participating organizations, including EHR vendor and software version, submission type, file exchange go-live date, HL7 settings, web service credentials, facility identifiers, and designated file exchange contacts.
		Onboarding	ability to create a unique username to assign to the organizations/facilities during the test phase			E	Yes	During the test phase, the solution makes sure usernames are unique and can create and send the username to the identified email user.
		Onboarding	ability to create a unique password to assign to the organizations/facilities during the test phase			E	Yes	The proposed solution can create and electronically send unique passwords to facilities/organizations during their testing phase.
Updated		Onboarding	ability to electronically alert the vendor/organization when the certificate for transport is going to expire in X time period			E	Yes	The proposed Solution centrally manages transport security and does not rely on organization-specific transport certificates. Where transport certificates are utilized, certificate lifecycle management and expiration monitoring are supported through the hosting and integration infrastructure.
Updated		Onboarding	ability to store digital certificate information			E	Yes	The proposed Solution does not rely on individual organization transport certificates. Transport security is managed centrally, eliminating the need for organization-specific certificate expiration notifications.
		Onboarding	ability to validate that the transport layer between the test site and IIS is functional			E	Yes	The proposed solution can validate the transport layer between the test site and the IIS.
		Onboarding	ability to validate system connectivity prior to the submission of test data			E	Yes	The proposed solution can validate connectivity prior to facilities/organizations submitting test data.
		Onboarding	ability to identify data formatting errors during testing			E	Yes	Robust reporting and analytics capabilities allow for easy identification and exporting of results of errors for any data submission.
Updated		Onboarding	ability to provide test message submission summary report to the EHR vendor			E	Yes	The proposed solution enables exportable HL7 Job Statuses for specified dates (Today, Past 7, Past 14, Past 30, Past 90 days) and custom date ranges.
Updated		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	The proposed solution provides the ability for exportable HL7 Job Statuses (VXU, QBP) for specified dates (Today, Past 7, Past 14, Past 30, Past 90 days) and custom date ranges. These exportable reports allow for an additional search ability to view detailed information about errors and warnings.
		Onboarding	ability for IIS authorized staff to review and approve onboarding forms			E	Yes	Authorized users can review and approve enrollment forms.
		Onboarding	ability for IIS staff to review and reject onboarding forms			E	Yes	Authorized users can review and approve enrollment forms.
		Onboarding	ability for applicant to edit a rejected onboarding application			E	Yes	The applicant will receive an email notification of the rejected enrollment to allow them to edit and resubmit it for approval. Authorized users can edit rejected enrollments.
		Onboarding	ability for applicant to save a rejected onboarding application			E	Yes	Our proposed solution will email the applicant of the rejected IIS enrollment to allow them to edit, save, and resubmit for approval. Authorized users can save and edit rejected enrollments.
		Onboarding	ability for applicant to resubmit a rejected onboarding application			E	Yes	Authorized users can edit and resubmit rejected enrollments.
		Onboarding	ability to compare onboarding application information to current records to determine most current data			E	Yes	The proposed solution can view prior enrollment information to compare records and make determinations.
		Interfaces	ability to interface with other systems to facilitate electronic data sharing/exchange per jurisdictional policy			E	Yes	The proposed Solution supports secure interoperability with external systems through standards-based interfaces, including HL7, SOAP/WSDL, APIs, batch file exchange, and some jurisdiction-defined integrations.
		Interfaces	ability to interface with electronic health record systems			E	Yes	Near- and real-time data exchange capabilities and interactions with external systems occur in accordance with our preferred method using the CDC's WSDL.
		Interfaces	ability to interface with the Immunization Gateway			E	Yes	The proposed Solution supports all applicable CDC Immunization (IZ) Gateway connections and services, enabling secure bidirectional data exchange in accordance with CDC IZ Gateway standards and specifications.
Updated		Interfaces	ability to interface with an application that facilitates patient scheduling	Particularly relevant for mass vaccination.		E	Yes	The proposed Solution is fully compliant with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, using SOAP-based transport by using the standard CDC WSDL for exchanging vaccine administration data.
		Interfaces	ability to exchange data with CDC Vaccine Tracking System (VTrckS) based on most current CDC ExIS Specifications			E	Yes	Data exchange with the national VTrckS occurs via an ExIS interface following current specifications. One of the solution's core functional areas, Vaccine Inventory Management and Accountability, is tightly integrated with VTrckS to order and manage doses for the VFC population. It also adapts to new VTrckS specifications as they are released.
		Interfaces	ability to order vaccine via electronic interface with VTrckS			E	Yes	The Vaccine Inventory Management and Accountability component is enabled through integration with VTrckS, as described in the previous response. VTrckS integration facilitates the retrieval of Provider Master Data, inventory data, order and shipment dates, and vaccine return and wastage data. It supports Providers and jurisdictions in ordering, managing, and distributing doses.

		Interfaces	ability to receive vaccine inventory/shipping information			E	Yes	The solution provides a single point of reference for vaccine-related inventory and supports the following functions: • Request vaccines • Manage vaccine inventories • Manage vaccine transfers • Manage vaccine wastage/disposal • Create/submit vaccine inventory reports • Communicate and support CDC-requested initiatives The Vaccine Orders function displays sort and filter options and supports multiple vaccine ordering through the Vaccine Order Screen. Information from VTrckS is uploaded in the solution when orders are shipped from the CDC warehouse or other manufacturer warehouse. To prevent Provider acceptance of a shipment before the shipment is delivered, the solution displays the tracking status, such as In Transit or Delivered. The solution also automatically notifies Providers when an order is shipped and includes tracking information so the Provider can track the shipment until received and confirmed. When a shipment is physically received, they can compare the information to the original order and confirm receipt via the UI. If the information received in the shipment differs from what is in the order, there is an option to edit the information (e.g., different lot number). After verifying receipt, the user confirms the shipment, and the information is added to their inventory.
Updated		Interfaces	ability to batch export vaccine inventory for submission to VTrckS			E	Yes	The proposed solution can interface with VTrckS to batch export vaccine inventory.
Updated		Interfaces	ability to batch export vaccine ordering information for submission to VTrckS			E	Yes	The proposed Solution has the ability to batch export vaccine ordering information for submission to VTrckS.
		Interfaces	ability to batch export facility information			E	Yes	Authorized users can batch export facility/organization information.
		Interfaces	ability to export vaccine return and wastage data to VTrckS			E	Yes	Integration with VTrckS enables exchange of vaccine return and wastage data. Jurisdiction benefits from improvements on the current HIR's capabilities for order processing, reviewing/approving orders, dose decrementing, inventory reconciliation, transfers, wastage, and expiration. To provide the best user experience, reduce the need for manual entry, and mitigate the opportunity for mistakes, the solution's inventory management component includes automatic decrementing when a vaccine is administered, received, returned, or in the case of wastage. In addition, the proposed solution helps minimize wastage from occurring in the first place. The vaccine order forecasting function calculates the recommended order quantity for each NDC each time a Provider initiates a new order. The calculation is based on various essential parameters, including the average number of doses administered, order frequency, lead time, demand uncertainty, safety stock requirements, and the current inventory. Using this forecasting tool, healthcare Providers can maintain adequate stock levels without excessive ordering, effectively preventing wastage and optimizing vaccine distribution. It also incorporates expiration dates to actively manage inventory and prevent administration of expired vaccines. By monitoring expiration dates, healthcare Providers can prioritize doses nearing expiration, reducing wastage and achieving optimal use of available vaccines.
Added		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	The proposed Solution is designed to support the CDC VTrckS API and can integrate with API-based VTrckS interfaces as they are made available by the CDC. Implementation of the VTrckS API is dependent upon CDC prioritization and availability for participating jurisdictions.
		Interfaces	ability to receive data through an interface with jurisdictional vital records system			E	Yes	The proposed Solution supports integration with Jurisdictional Vital Records systems through batch file exchange and HL7 Version 2.5.1 messaging. Gainwell works with jurisdictions to implement the appropriate integration approach based on the capabilities of the jurisdiction's Vital Records system and operational requirements.
		Interfaces	ability to update IIS data from Vital Records for birth events			E	Yes	Birth event data received via the interface with Vital Records (described above) is stored within the solution's relational data store, updating the patient record.
		Interfaces	ability to update IIS data from Vital Records for death events			E	Yes	Death event data received via the interface with Vital Records is stored within the solution's relational data store, updating the patient record.
		Interfaces	ability to update IIS data from Vital Records for adoption events			E	Yes	Adoption event data received via the interface with Vital Records is stored within the relational data store, updating the patient record.
		Interfaces	ability to update IIS data from Vital Records for name change events			E	Yes	Name change data received via the interface with Vital Records is stored within the relational data store, updating the patient record.
		Interfaces	ability to detect if a newborn record is a potential duplicate in the IIS			E	Yes	Deduplication of patient and immunization records occurs according to a matching algorithm that considers configurable criteria (e.g., which fields to compare) as well as performing phonetic comparison to identify duplicates. The solution permits quick merging as well as manual merges.
		Interfaces	ability to use new Vital Record data for matched records to update patient demographic data			E	Yes	Data received via the interface with Vital Records, including patient demographic data updates, is verified for data quality and stored within the relational data store, updating the patient record.
		Interfaces	ability to update the IIS with date of death from Vital Records data			E	Yes	Death event data received via the interface with Vital Records is stored within the relational data store, updating the patient record.
		Interfaces	ability to prevent updates to IIS records			O	Yes	The proposed solution can prevent updates to IIS records if the information supplied does not meet specifications.
		Data Exchange	ability to support real-time data exchange per the CDC HL7 implementation guide			E	Yes	The solution supports secure, real-time bidirectional immunization data exchange in accordance with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging. Organizations can be configured to submit VXU immunization updates, QBP queries, or both, based on their approved exchange capabilities.
		Data Exchange	ability to process an HL7 message			E	Yes	The proposed solution is fully compliant with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, including the ability to process incoming Query by Parameter (QBP) and Unsolicited Vaccination Record Update (VXU) messages.
		Data Exchange	ability to respond to an HL7 message			E	Yes	The solution processes inbound HL7 transactions and returns the appropriate HL7 response, including acknowledgments and query responses, based on the message type and processing outcome. Transaction status and processing information are retained to support operational monitoring and troubleshooting.
		Data Exchange	ability to create an HL7 message			E	Yes	The proposed solution provides the ability to create HL7 messages.
		Data Exchange	ability to capture IIS Core Data Elements			E	Yes	Data is captured and stored in accordance with the data requirements of the Core Data Elements for IIS Functional Standards v5.0 and the requirements defined in the joint CDC and AIRA RTM.

		Data Exchange	ability to store IIS Core Data Elements			E	Yes	Data is captured and stored in accordance with the data requirements of the Core Data Elements for IIS Functional Standards v5.0 and the requirements defined in the joint CDC and AIRA RTM.
Updated		Data Exchange	ability to accept last prior version of HL7 messages	In the event a new HL7 version is released		E	Yes	The proposed Solution currently supports HL7 Version 2.5.1 and will support jurisdiction-defined transition periods when future HL7 versions are adopted.
		Data Exchange	ability to manually correct a submitted record and resubmit for processing			O	Yes	The solution enables authorized users to identify transactions requiring attention, review associated processing errors, and support correction and reprocessing of submitted data. Detailed error information, including HL7 error codes, error locations, application errors, severity, and user messages, assists users in identifying and resolving data quality issues.
		Data Exchange	ability to support data exchange in non-HL7 format			E	Yes	The proposed solution is compliant with the CDC HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, using Simple Objects Access Protocol (SOAP)-based transport by using the standard CDC and Immunization (I2) Gateway Web Services Description Language (WSDL). In addition, the solution is built on the FHIR framework to deploy easily when CDC and AIRA publish an IIS FHIR Implementation Guide. The solution uses HL7 and FHIR. The solution also allows batch file imports via flat file submissions.
		Data Exchange	ability to import bulk patient demographic information into IIS	Particularly relevant for mass vaccination.		E	Yes	The proposed Solution supports bulk import of Immunization data through HL7 messaging, batch import capabilities, and other supported data exchange methods for updating patient Immunization histories.
		Data Exchange	ability to import bulk immunization information into IIS	Particularly relevant for mass vaccination.		E	Yes	The proposed Solution supports bulk import of Immunization data through HL7 messaging, batch import capabilities, and other supported data exchange methods for updating patient Immunization histories.
Added		Data Exchange	ability to export routine, seasonal, and emergency vaccination files (aggregate and de-identified)			E	Yes	The solution supports the generation and export of aggregate and de-identified vaccination data files for routine, seasonal, and emergency vaccination reporting. Export criteria and data content can be configured to meet applicable jurisdictional and CDC reporting requirements while protecting patient-level information.
Added		Data Exchange	ability to export routine, seasonal, and emergency vaccination files (aggregate and de-identified) automatically via CDC approved system			O	Yes	The solution supports automated generation and transmission of aggregate and de-identified routine, seasonal, and emergency vaccination data through CDC-approved exchange mechanisms. Automated processing reduces manual effort and supports timely, consistent submission of required public health data in accordance with applicable CDC specifications and jurisdictional reporting requirements.
		Data Exchange	ability to monitor and troubleshoot data exchange			E	Yes	The proposed Solution provides dashboards, file exchange monitoring, processing status, error reporting, acknowledgements, and drill-down capabilities to monitor and troubleshoot data exchange activities.
		Data Exchange	ability to view VXU messages submitted by an organization			E	Yes	The Immunization Solution proposed provides easy-to-understand visual dashboards to show the results of HL7 and other file exchange processing. Authorized users can view dashboards showing the rates of acceptance/rejection along with other pertinent data.
		Data Exchange	ability to view HL7 messages for an organization within a defined date range per jurisdictional policy			E	Yes	The solution enables authorized users to search and review an organization's HL7 transactions within a defined date range, subject to jurisdictional access and retention policies. Users can further refine results by facility, job status, message control ID, vaccine information, funding information, HL7 error code, severity, and other transaction criteria to support interface monitoring, troubleshooting, and data quality management.
		Data Exchange	ability to view HL7 ACK messages generated for an organization			E	Yes	HL7 messaging (VXU or QBP or ACK response) is provided in accordance with CDC-defined standards and encoding rules.
		Data Exchange	ability to view incoming HL7 QBP messages submitted by an organization			E	Yes	HL7 messaging (VXU or QBP or ACK response) is provided in accordance with CDC-defined standards and encoding rules.
		Data Exchange	ability to view RSP messages generated for an organization			E	Yes	HL7 RSP messaging is provided in accordance with CDC-defined standards and encoding rules.
		Data Exchange	ability to log acknowledgement messages indicating warnings and errors			E	Yes	The proposed solution tracks the status of submissions and submission warnings and errors and retains this data according to jurisdictional policy. Gainwell uses this information as part of its overall data quality analytics to identify common or recurring errors responsible for data quality issues. This helps inform additional opportunities for improvement in onboarding processes, training, and other quality initiatives.
		Data Exchange	ability to retrieve error messages within a specified date range by organization			E	Yes	Information on submission warnings and errors is retained in the solution according to jurisdictional policy. This data is made available for data quality analysis and is searchable by date range, organization, and other criteria with the File Exchange dashboards. There are robust drill-down abilities to view and address errors easily.
		Data Exchange	ability to retrieve acknowledgment messages within a specified date range by organization			E	Yes	Acknowledgement messages are retained in the solution according to jurisdictional policy. This data is made available for data quality analysis and is searchable by date range, organization, and other criteria.
		Data Exchange	ability to filter error messages			E	Yes	Authorized users can filter, sort, and drill down to view error messages.
		Data Exchange	ability to filter acknowledgement messages			E	Yes	Authorized users can filter, sort, and drill down to view acknowledgment messages.
		Data Exchange	ability to sort error messages			E	Yes	Authorized users can filter, sort, and drill down to view error messages.
		Data Exchange	ability to sort acknowledgement messages			E	Yes	Authorized users can filter, sort, and drill down to view acknowledgment messages.

Status	Req. #	Capability	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)
		Patient Matching & Deduplication	ability to prevent duplicate patient records in the IIS database			E	Yes	Deduplication is accomplished using a scoring algorithm that uses defined criteria to compare available data. The fields used for comparison are configurable. An innovative feature of the solution is that it also employs phonetic logic to identify sound-alikes as part of the deduplication process. The timeliness of the deduplication approach is markedly faster than that of legacy solutions and many competitors' systems. Automated solution logic identifies suspected duplicates and can automatically merge them using the quick-merge feature or present them for merging by authorized users. Solution functionality includes using prebuilt screens to enable the end user to view matched/pended patients and merge or make distinct records. Patient records display on the Patients Needing Review page. To further drill down from the Patients Needing Review list, authorized users click the View Merge Details button. After viewing the records and confirming that they should be merged, authorized users can use the solution's quick merge process. Quick Merge and Manual Merge capabilities exist as well.
Updated		Patient Matching & Deduplication	ability to automatically identify incoming patient records as potential duplicates			E	Yes	The proposed Solution automatically compares incoming patient records against existing patient records using configurable matching criteria, scoring algorithms, and phonetic matching logic to identify potential duplicate patient records.
Updated		Patient Matching & Deduplication	ability to automatically identify existing patient records as potential duplicates			E	Yes	The proposed Solution continuously evaluates existing patient records using configurable matching criteria, scoring algorithms, and phonetic matching logic to identify potential duplicate patient records. Suspected duplicates are automatically resolved based on configured business rules or presented to authorized users for review and resolution.
		Patient Matching & Deduplication	ability to automatically consolidate two or more duplicate records			E	Yes	The proposed Solution automatically consolidates duplicate patient records based on configurable matching criteria and business rules. Records that cannot be automatically consolidated are presented to authorized users for manual review and merge.
		Patient Matching & Deduplication	ability to generate electronic notification of potential duplicates for manual review			E	Yes	The proposed Solution's deduplication process generates a list of suspected duplicates and presents it for authorized users to review and merge.
		Patient Matching & Deduplication	ability to automatically match an incoming patient record with existing records to avoid a duplicate record being created			E	Yes	The proposed Solution automatically compares incoming patient records against existing patient records using configurable matching criteria, scoring algorithms, and phonetic matching logic to identify existing patients and prevent duplicate records from being created.
		Patient Matching & Deduplication	ability to set thresholds for patient matching			E	Yes	Gainwell can configure patient matching thresholds in collaboration with the jurisdiction based on approved business rules and matching policies.
Updated		Patient Matching & Deduplication	ability to view all potential duplicate patient records for an individual patient simultaneously			E	Yes	Authorized users can view potential duplicate patient records for an individual simultaneously on the Patients Needing Review tile. From this page, users can choose to merge one or more records via the Solution's easy-to-use merge features.
		Patient Matching & Deduplication	ability for jurisdictional admin to edit thresholds to increase the probability of a match			E	Yes	The Jurisdiction and Gainwell can determine recommendations and needs for updated thresholds.
		Patient Matching & Deduplication	ability for jurisdictional admin to edit thresholds to reduce the probability of a match			E	Yes	The Jurisdiction and Gainwell can determine recommendations and needs for updated thresholds.
		Patient Matching & Deduplication	ability to flag potential duplicate patient records for manual review that cannot be resolved automatically			E	Yes	The solution provides a view of duplicates and an individual view of clients needing to be merged. Unmerge functionality can view data received since the patients were merged.
Updated		Patient Matching & Deduplication	ability to view all potential duplicate patient records simultaneously			E	Yes	Authorized users can view identified potential duplicate patient records for an individual simultaneously on the Patients Needing Review tile. From this page, users can choose to merge one or more records via the solution's easy-to-use merge features.
		Patient Matching & Deduplication	ability for admin to manually merge patient records			E	Yes	Authorized users can choose from a quick-merge and a manual merge capability, in addition to having the option to automatically merge duplicate records.
		Patient Matching & Deduplication	ability for organizational/facility user to manually merge patient records from their own organization/facility			E	Yes	The solution enables authorized organizational or facility users to manually review and merge duplicate patient records associated with their own organization or facility. Access to this functionality is controlled through configurable role-based permissions, allowing the jurisdiction to determine which user roles are authorized to perform patient merges while maintaining appropriate security, accountability, and organizational boundaries.
		Patient Matching & Deduplication	ability to manually flag two or more patient records as potential duplicates			E	Yes	The proposed solution allows for flagging of two or more patients identified as potential duplicates.
		Patient Matching & Deduplication	ability to prevent manual review of records previously indicated as "not a duplicate"			E	Yes	Authorized users can mark records as permanently different (e.g., not duplicate), so that they are not presented again in the Patients Needing Review page as possible duplicates.
		Patient Matching & Deduplication	ability to flag a patient as "not a duplicate" during manual review			E	Yes	Authorized users can mark records as permanently different, so that they are not presented again in the Patients Needing Review page as possible duplicates.
		Patient Matching & Deduplication	ability to maintain "not a duplicate" flag for resolved patient records			E	Yes	The solution enables authorized users to designate evaluated patient records as "Not Duplicates" when review determines that the records represent distinct individuals. The determination is retained to document the resolution and help prevent the same records from being repeatedly identified for duplicate review, improving both data quality and operational efficiency.

		Patient Matching & Deduplication	ability to select data elements from the patient records to maintain within the consolidated record		E	Yes	Authorized users can use a quick pick merge or select data elements for the consolidated record.
		Patient Matching & Deduplication	ability to retain "pre-merged" records for reference		E	Yes	The proposed Solution maintains full traceability including patient record data before and after merging. Authorized users can view the audit history and see the exact point in time when the records were merged and view the individual original unmerged records.
		Patient Matching & Deduplication	ability to separate patient records that were incorrectly merged		E	Yes	The Unmerge feature allows a designated user to access a patient's prior merge history and determine if the patient had inadvertently been merged.
		Vaccination Event Matching & Deduplication	ability to prevent potential duplicate vaccination events at the immunization level		E	Yes	The solution applies immunization-level deduplication logic to identify potential duplicate vaccination events before they are added to the patient's immunization history. When a potential duplicate is detected, the solution alerts the authorized user and requires confirmation before proceeding, helping prevent inadvertent duplicate vaccination records while allowing appropriate exceptions when the event is determined to be valid.
Updated		Vaccination Event Matching & Deduplication	ability to automatically identify incoming vaccination event as potential duplicates		E	Yes	The proposed solution has immunization deduplication logic to assist in identifying an incoming vaccination event as possible duplicate.
		Vaccination Event Matching & Deduplication	ability to automatically select the most accurate vaccination event based on deduplication rules		E	Yes	The proposed solution can deduplicate based on algorithm and/or ownership.
Updated		Vaccination Event Matching & Deduplication	ability to automatically identify existing vaccination events as potential duplicates		E	Yes	The proposed solution has immunization deduplication logic to assist in identifying an incoming vaccination event as possible duplicate.
Updated		Vaccination Event Matching & Deduplication	ability to manually flag potential duplicate vaccination events for manual review		E	Yes	The solution displays potential vaccine duplicates and warns the user if entered in the UI. Additionally, interface exchanges will provide ACKS back to the facility when duplicates are identified.
Updated		Vaccination Event Matching & Deduplication	ability to display potential duplicate vaccine records for an individual patient		E	Yes	Users can receive a notification that a vaccine is identified as being a duplicate upon UI entry of the vaccination event.
		Vaccination Event Matching & Deduplication	ability to manually merge a duplicate vaccination event		E	Yes	The solution displays potential vaccine duplicates and warns the user if entered in the UI. Additionally, interface exchanges provides ACKS back to the facility when duplicates are identified.
		Vaccination Event Matching & Deduplication	ability to manually delete a duplicate vaccination event		E	Yes	The proposed solution allows for manual merging of vaccine events via the solution's merge ability. It also allows for unmerging of vaccine events.
		Vaccination Event Matching & Deduplication	ability to automatically consolidate two or more duplicate vaccination events		E	Yes	The solution supports identification and consolidation of duplicate vaccination events using matching logic. Authorized users can also manually review, merge, or delete vaccination events when intervention is required to maintain an accurate and consolidated immunization history.
Added		Vaccination Event Matching & Deduplication	ability to retain "pre-merged" or "pre-consolidated" vaccination events for reference		E	Yes	The solution maintains the underlying source and historical information associated with consolidated records to support traceability, auditability, and review of data as it existed prior to consolidation
Added		Vaccination Event Matching & Deduplication	ability to separate vaccination events that were incorrectly merged or consolidated		E	Yes	The solution enables authorized users to reverse an incorrect consolidation and restore the applicable underlying records when necessary. Unmerge functionality provides a controlled mechanism for correcting consolidation decisions while preserving record integrity and auditability.

Status	Req. #	Capability	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)
Updated		Clinical Decision Support	ability to provide immunization clinical decision support according to ACIP recommendations			E	Yes	The solution provides immunization clinical decision support based on current ACIP recommendations, evaluating a patient's immunization history and applicable clinical criteria to determine vaccine validity and identify recommended, due, and overdue immunizations across the lifespan.
		Clinical Decision Support	ability to support a vaccine clinical decision support algorithm aligned with the CDC CDSi logic specifications			E	Yes	The solution's vaccine forecasting algorithm is aligned with CDC Clinical Decision Support for Immunization (CDSi) logic and specifications. Gainwell maintains and validates forecasting rules as CDC/ACIP guidance evolves, including applicable vaccine series, age requirements, dose intervals, validity rules, indications, contraindications, and other clinical criteria. The solution also supports effective-dated rules and jurisdiction-specific configuration where appropriate.
		Clinical Decision Support	ability for jurisdictional admin to update the CDS rules			E	Yes	The proposed Solution automatically imports CDC CDSi rules. Jurisdiction-specific forecasting requirements are supported through configurable schedules and business rules where applicable; however, core CDC CDSi logic remains aligned with CDC specifications.
		Clinical Decision Support	ability to evaluate a patient's immunization history according to the ACIP Child and Adolescent Immunization Schedule			E	Yes	The solution evaluates a patient's immunization history against the current ACIP Child and Adolescent Immunization Schedule, applying applicable vaccine, age, dose, interval, and series rules to determine the patient's immunization status and future vaccination needs.
		Clinical Decision Support	ability to evaluate a patient's immunization history according to the ACIP Recommended Catch-up Immunization Schedule for Children and Adolescents			E	Yes	The proposed Solution supports jurisdiction-specific schedules through configurable forecasting schedules while maintaining alignment with CDC CDSi recommendations.
		Clinical Decision Support	ability to evaluate a patient's immunization history according to the ACIP Adult Immunization Schedule			E	Yes	The solution evaluates a patient's immunization history against the current ACIP Adult Immunization Schedule, considering applicable vaccine history, age, dose and interval requirements, and other configured clinical criteria to determine immunization status.
Updated		Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Child and Adolescent Immunization Schedule and a patient's immunization history			E	Yes	The proposed Solution supports jurisdiction-specific schedules through configurable forecasting schedules while maintaining alignment with CDC CDSi recommendations.
Updated		Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Recommended Catch-up Immunization Schedule for Children and Adolescents and a patient's immunization history			E	Yes	The proposed Solution supports jurisdiction-specific schedules through configurable forecasting schedules while maintaining alignment with CDC CDSi recommendations.
Updated		Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Adult Immunization Schedule and a patient's immunization history			E	Yes	The solution generates patient-specific vaccine forecasts based on the ACIP Adult Immunization Schedule and the patient's documented immunization history, identifying applicable recommended, due, and overdue vaccinations. Forecasting rules are maintained as clinical guidance evolves and can incorporate jurisdiction-specific requirements as applicable.
		Clinical Decision Support	ability to display and highlight vaccines that are due			E	Yes	Historical and forecasted patient information are viewable by authorized solution users. Information highlighted on the historical and forecasted patient information page includes vaccines Due Now, Recommended, Overdue, Future, and Not Recommended.
		Clinical Decision Support	ability to display and highlight vaccines that are overdue			E	Yes	The solution displays historical and forecasted patient information based on the forecasting model. Overdue vaccines are specifically highlighted in their own column, making it easy for users to identify them quickly.
		Clinical Decision Support	ability to display an indication when a vaccine series is complete			E	Yes	The proposed solution displays the completeness of the series on various screens and reports.
		Clinical Decision Support	ability to display vaccine-specific contraindications according to CDC lists of vaccine contraindications			O	Yes	Contraindications and precautions are incorporated into the forecasting models used in the Immunization Forecasting module. The Not Recommended section of the solution's Historical and Forecasted Patient Information page shows how this logic is used to identify vaccines as not recommended for a given patient.
		Clinical Decision Support	ability to take into account contraindications and precautions in the vaccine forecast			E	Yes	Contraindications and precautions are incorporated into the forecasting models used in the Immunization Forecasting module. The Not Recommended section of the solution's Historical and Forecasted Patient Information page shows how this logic is used to identify vaccines as not recommended for a given patient.
		Clinical Decision Support	ability to take into account evidence of immunity in the vaccine forecast			E	Yes	The forecasting component considers contraindications such as immunity in its validation and forecasting of vaccinations.
		Clinical Decision Support	ability to generate a forecast of specific vaccines required for individuals who travel outside the US			O	Yes	The proposed Solution supports forecasting of vaccines required for persons traveling outside of the US. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Clinical Decision Support	ability to maintain historical records of effective dates of previous forecast schedules			O	Yes	The proposed Solution maintains historical records including previous forecast schedules with effective dates. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Clinical Decision Support	ability to review an immunization schedule that was appropriate at the time of administration			O	Yes	The proposed solution supports reviewing of immunization schedules appropriate at the time of submission.
		Clinical Decision Support	ability to apply an immunization schedule that was appropriate at the time of administration			O	Yes	The proposed solution supports reviewing of immunization schedules appropriate at the time of submission.

		Clinical Decision Support	ability to account for immune globulins in vaccine forecasting			E	Yes	The forecasting component considers the immune globulin events.
Updated		Clinical Decision Support	ability to create test cases for reuse during user acceptance testing			E	Yes	Gainwell provides support for jurisdictional staff throughout UAT, including providing training in readiness for commencement of UAT activities and assisting with test case creation or adaptation for use during UAT. Test cases created and used by Gainwell to perform system, integration, and/or regression testing can be made available for reuse by jurisdiction during UAT.
Updated		Clinical Decision Support	ability to save test cases for reuse during user acceptance testing			E	Yes	The proposed Solution supports saving test cases for reuse during UAT. Gainwell has incorporated this functionality into the core Immunization Solution product.
Updated		Clinical Decision Support	ability to compare the expected results of the forecasting test case to the actual results observed by the tester			E	Yes	The proposed Solution supports comparing expected versus actual test results for forecasting. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Reminder/Recall	ability to generate patient-specific reminder/recall notifications			E	Yes	Authorized users can configure reminders and recalls using definable criteria. Reminders and recall notifications can be set up to use age cohorts, vaccine information such as expiration dates and lot numbers, a CDC-imported immunization schedule, and other data to inform the distribution list, timing, method (email or mail), and content of the communication. Authorized users can configure reminders and recalls within the solution through the Reminder/Recall Configuration function.
Updated		Reminder/Recall	ability to select one or more vaccines for generating reminder/recall notifications			E	Yes	Reminders and recall notifications can be set up through the Reminder/Recall Configuration tile to apply vaccine information such as expiration dates and lot numbers, a CDC-imported immunization schedule, and other data to inform the distribution list, timing, method (email or mail), and content of the communication.
		Reminder/Recall	ability to view the date the reminder/recall notice was sent to a patient			O	Yes	The proposed solution retains a complete history of notices issued to patients. Authorized users can view the reminder/recall notice history, including the dates when communications were sent to the patient.
Updated		Reminder/Recall	ability to generate lists of patients in need of a reminder or recall notification by organization			E	Yes	Authorized users can configure reminder/recall notices within the Reminder/Recall Configuration tile to apply other criteria to define the target audience for the communication, including selecting patients by organization.
		Reminder/Recall	ability to generate reminder/recall notifications per consent designation			E	Yes	The proposed solution captures sharing consent to include or not include for reminder/recall notifications.
		Reminder/Recall	ability to generate patient-specific reminder/recall notices by user-defined parameters			E	Yes	Patient-specific reminder/recalls can be defined by the user.
		Reminder/Recall	ability to generate reminder/recall in user-defined format			E	Yes	The Reminder/Recall function includes reporting that allows for the user to define criteria for reminder/recall notices. Authorized users can manage templates such as reminder/recall form templates.
Updated		Reminder/Recall	ability to select the age of the cohort when generating reminder/recall notifications	Particularly relevant for mass vaccination.		E	Yes	Authorized users can configure the calendar/schedule for reminder/recall notices and apply other user-defined criteria such as target audience characteristics, including age cohorts.
		Reminder/Recall	ability to print patient-specific reminder/recall notices by user-defined parameters			E	Yes	Editable and exportable reminder/recall notices can be configured by user-defined parameters.
		Reminder/Recall	ability to generate patient specific reminder/recalls in a user-defined format			E	Yes	Authorized users can manage reminder/recall from templates. This is configurable within the Reminder/Recall function.
		Reminder/Recall	ability for an end user to generate patient specific reminder/recalls in accordance with HIPAA and jurisdictional law or policy			E	Yes	Gainwell is deeply familiar with HIPAA, policies, and law and will provide appropriate setup before configuring the solution.
		Reminder/Recall	ability for an end user to print patient specific reminder/recalls in accordance with HIPAA and jurisdictional law or policy			E	Yes	Gainwell is deeply familiar with HIPAA, policies, and law and will provide appropriate setup before configuring the solution.
Updated		Reminder/Recall	ability to generate vaccine recall notices by facility based on vaccine name, vaccination date range, and lot number			O	Yes	The reminder/recall function will allow for the creation of a user-defined exportable list and generation of email and mail based on vaccine name (vaccine recall), data range, lot number (recall lots), city, state, county, patient age, provider, and school.
Updated		Reminder/Recall	ability to generate vaccine recall notices by administering provider based on vaccine name, vaccination date range, and lot number			O	Yes	The reminder/recall function will allow for the creation of a user-defined exportable list and generation of email and mail based on vaccine name (vaccine recall), data range, lot number (recall lots), city, state, county, patient age, provider, and school.
Updated		Reminder/Recall	ability to set the limit/number of times a patient will receive a reminder/recall			O	Yes	This is a selectable filter option within the Reminder/Recall report creation.
Updated		Reminder/Recall	ability to modify the limit/number of times a patient will receive a reminder/recall			O	Yes	This is a selectable filter option within the Reminder/Recall report creation.
Updated		Reminder/Recall	ability to exclude a patient who has met the limit/number of times to receive a reminder/recall			O	Yes	A limit and time interval can be set for a patient to receive reminder/recall notices.
		Reminder/Recall	ability to generate a list of phone numbers for patients needing reminder/recall			O	Yes	The solution enables authorized users to identify patients needing reminder/recall and generate patient listings that include available contact information, including phone numbers, to support outreach activities. Patient populations can be targeted using configurable vaccine, age, provider/facility, geographic, demographic, and other criteria to support jurisdictional and provider-level reminder/recall efforts.
		Reminder/Recall	ability to manually review a patient list for a reminder/recall notification			E	Yes	The Reminder/Recall Configuration tile allows authorized users to configure the reminder/recall notices and apply other user-defined criteria for the target audience.

		Reminder/Recall	ability to flag patients to exclude before sending a reminder/recall notification		O	Yes	The reminder/recall function will exclude patients.
		Reminder/Recall	ability to establish a time interval between reminder/recall notices (e.g., 90 days or 60 days)		O	Yes	The proposed solution allows for a date (last notice date) to be chosen since the last reminder/recall was run.
		Reminder/Recall	ability to generate a reminder/recall notifications for patients with an active status for their organization		E	Yes	Authorized users can configure reminder/recall notices within the Reminder/Recall Configuration tile to apply other criteria to define the target audience for the communication, including selecting active patients by organization.
		Reminder/Recall	ability to generate reports that include reminder/recall history for specific date range		O	Yes	Custom date ranges can be used to generate reminder/recall reports for individuals.
		Reminder/Recall	ability to make all reminder/recall data accessible to authorized users for a predetermined period of time		O	Yes	Prior reminder/recalls are stored for authorized facility users to view for the prior 30 days.
		Reminder/Recall	ability to aggregate multiple notices going to the same address into one notification		O	Yes	The proposed solution provides the ability to aggregate notices to one address.
		Coverage Reports	ability to generate report(s) displaying information on immunization coverage rate(s) among select populations		E	Yes	Using the available consolidated immunization history data, authorized users can evaluate immunization coverage at the patient, organization, ZIP code, county, and state levels to assess coverage rates accurately for vaccine-preventable diseases. Users can generate reports to determine compliance, determine individuals or select populations who may be missing immunization requirements, or determine who is susceptible to a vaccine-preventable disease.
		Coverage Reports	ability to generate report(s) for organizations and facilities per CDC Immunization Quality Improvement for Providers program guidance on immunization coverage among an organization/facility patient population		E	Yes	Mandated federal and state reporting are available including organization/facility coverage reporting per CDC Immunization Quality Improvement for Providers guidance. Authorized users can access coverage reporting component from the Reports tile, and the selecting Coverage Dashboard from the Solution's Reports tile.
		Coverage Reports	ability to generate report(s) on immunization coverage for a user-defined geographic area		E	Yes	From the Reports tile, authorized users can access the reporting. Selecting the Coverage Dashboard option allows users to generate coverage reports by a number of criteria, including geographic region.
		Coverage Reports	ability to generate report(s) on immunization coverage for a patient cohort		E	Yes	Selecting the Coverage Dashboard option allows users to generate coverage reports by a number of criteria, including patient cohort.
		Coverage Reports	ability to view and modify list of patients to be included in immunization coverage report		O	Yes	The proposed Solution allows for user defined criteria to generate an immunization coverage report.
		Coverage Reports	ability to generate report(s) displaying immunization coverage trends over time, over a selected timeframe		E	Yes	Vaccine coverage dashboards provide visualizations within the UI and exportable options for vaccine coverage trends.
		Coverage Reports	ability to generate report(s) that display the number of missed opportunities for vaccination		E	Yes	The Missed Opportunity Report displays the number of missed opportunities for vaccination at a facility over a user-defined time period. This report also displays a list of patients who were counted as having had a missed opportunity.
Updated		Coverage Reports	ability to generate report(s) displaying the number of patients late up-to-date for immunization who are up-to-date as of today		E	Yes	The Late Up to Date Report will display the number of patients who are late up to date for immunization, but up to date as of a user-defined date. This report will also display a list of patients who were counted as having had a missed opportunity.
		Coverage Reports	ability to generate report(s) that display the number of invalid vaccine doses		E	Yes	A custom report will allow the user to select invalid doses as a parameter to be included in the count report.
		Coverage Reports	ability to generate report(s) displaying vaccine exemption rates		E	Yes	A custom report will allow the user to select to select vaccine exemption to be included in the count report.
		Coverage Reports	ability to generate report(s) displaying immunization coverage by user-defined parameters		E	Yes	Immunization coverage reporting is accessible to authorized users through the Reports tile.
		Coverage Reports	ability to generate report(s) displaying immunization coverage by vaccine type		E	Yes	The Included Custom Coverage Report will allow the user to select vaccine type as a parameter when generating the report.
		Coverage Reports	ability to generate report(s) displaying immunization coverage by age range		E	Yes	The Custom Coverage Report will allow the user to select an age or age range as a parameter when generating the report.
		Coverage Reports	ability to generate report(s) displaying immunization coverage by ethnicity		E	Yes	The Custom Coverage Report will allow the user to select ethnicity as a parameter when generating the report.
		Coverage Reports	ability to generate report(s) displaying immunization coverage by race		E	Yes	The Custom Coverage Report will allow the user to select race as a parameter when generating the report.
Updated		Coverage Reports	ability to generate report(s) displaying immunization coverage by patient sex		O	Yes	The Custom Coverage Report will allow the user to select gender as a parameter when generating the report.

Status	Req. #	Capability	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)
		Patient Search	ability to search for patient records			E	Yes	The solution provides comprehensive patient search capabilities that enable authorized users to locate patient records using configurable search criteria. Users can perform searches using one or more demographic identifiers, with search behavior and required search parameters configurable by the jurisdiction to support patient matching policies and operational needs.
		Patient Search	ability to search patient record based on one or multiple user-defined parameters			E	Yes	The solution enables authorized users to search for patient records using one or multiple search parameters, including patient name, date of birth, mother's name, medical record number, IIS patient ID, and other available identifiers. Multiple criteria can be combined to refine search results and efficiently locate the appropriate patient record. The solution also supports 2D barcode scanning to streamline patient identification and data capture, reducing manual data entry and helping improve the speed and accuracy of patient record retrieval.
		Patient Search	ability to re-search for a patient record by modifying existing search parameters			E	Yes	The solution enables users to refine and repeat patient searches by modifying existing search parameters without restarting the search process. Users may broaden or narrow search criteria based on jurisdiction-configured search rules to improve patient identification while supporting efficient workflow.
		Patient Search	ability to display the list of returned possible patient matches per jurisdictional policy			E	Yes	The solution returns a ranked list of potential patient matches based on patient matching criteria. Search results display key demographic information to assist users in identifying the appropriate patient record. Jurisdictions can configure search thresholds, and the maximum number of potential matches returned (e.g., 100, 300, or other jurisdiction-defined limits) to align with state-specific patient matching policies and operational requirements.
		Patient Search	ability to select a patient record from the list of possible patient matches			E	Yes	The solution returns a ranked list of potential patient matches based on patient matching criteria. Search results display key demographic information to assist users in identifying the appropriate patient record. Jurisdictions can configure search thresholds, and the maximum number of potential matches returned (e.g., 100, 300, or other jurisdiction-defined limits) to align with state-specific patient matching policies and operational requirements.
		Add, Edit Patient Demographics	ability to add demographic information to a patient record			E	Yes	Demographic data is retrieved through automated system interfaces, may be updated manually within the UI, and is stored in the patient record. Demographic updates can be made automatically via system interfaces and manually through the UI.
		Add, Edit Patient Demographics	ability to create a new patient record			E	Yes	Authorized users can create a new patient record through web services, flat file, vitals, and manually.
		Add, Edit Patient Demographics	ability to edit demographic information in a patient record			E	Yes	The proposed solution allows for editing of patient demographics automatically through web services and manually through the UI.
		Add, Edit Patient Demographics	ability to insert permanent comments in a patient's record that can be viewed based on role/permission			E	Yes	The Immunization Solution can insert patient comments based on user role/permission managed through role/page access.
		Add, Edit Patient Demographics	ability to display the user who created the permanent comment in a patient's record			E	Yes	The solution provides a history of who created a permanent comment in a patient's record.
		Add, Edit Patient Demographics	ability to prevent a patient record from being saved unless required fields are completed, per jurisdictional policy			E	Yes	Gainwell works with the jurisdiction to determine the definition of "completeness" (required data elements) for a given record to configure business rules governing validation according to policy. Once these are configured, we employ rules-based validation and accept or reject records accordingly. For data entry through the UI, users are presented with on-screen error messages notifying them when required information is missing and are unable to save the page until the information is completed.
		Add, Edit Patient Demographics	ability to automatically notify a user when attempting to submit an incomplete patient record			E	Yes	Users are presented with on-screen error messages notifying them when required information is missing and are unable to submit incomplete information.
		Add, Edit Patient Demographics	ability to store CDC-endorsed core data elements for all patient records			E	Yes	The proposed solution is specifically designed to accommodate CDC-mandated Core Data Elements for IIS Functional Standards v 5.0 for patient demographics as well as vaccination events.
		Add, Edit Patient Demographics	ability to store multiple of reported names for each patient to include: first name, middle name, last name, alias, maiden name			E	Yes	The solution supports management of multiple patient names, including first name, middle name, last name, aliases, maiden names, and other alternate names. Multiple surnames are maintained as part of the patient record and are incorporated into configurable patient search and matching functionality to improve patient identification and reduce duplicate records.
		Add, Edit Patient Demographics	ability to store multiple patient addresses			O	Yes	The solution supports multiple patient addresses, including international addresses, with configurable address types. Address records include country information and support jurisdiction-defined address designations, including configuration options such as "On File with School."
		Add, Edit Patient Demographics	ability to support multiple patient address type designations (e.g. primary address, vacation address)			O	Yes	The solution supports multiple address type designations for each patient, including configurable address classifications such as Primary, Mailing, Vacation, Temporary, and other jurisdiction-defined address types.
		Add, Edit Patient Demographics	ability to identify effective dates for use of a patient address			O	Yes	The solution stores effective and end dates for patient addresses, enabling users to identify the period during which each address was valid and supporting historical address management.
		Add, Edit Patient Demographics	ability to store all historic addresses for a patient			O	Yes	The solution maintains a complete history of patient addresses, preserving prior addresses with associated effective and end dates to support historical inquiry and auditing.
		Add, Edit Patient Demographics	ability to store country information related to where the patient was born			O	Yes	The solution stores patient birthplace information, including country of birth, as part of the patient demographic record.
		Add, edit patient demographics	ability to flag patient address as a verified United States Postal Service address (e.g., via SmartyStreets)			O	Yes	The solution records the date on which a patient address was last successfully verified through USPS-compatible address validation services Smarty, providing users with the most recent verification status and verification date.
		Add, edit patient demographics	ability to record date patient address last verified as a United States Postal Service address (e.g., via SmartyStreets)			O	Yes	The solution records the date on which a patient address was last successfully verified through USPS-compatible address validation services Smarty, providing users with the most recent verification status and verification date.
		Add, Edit Patient Demographics	ability to automatically create a unique patient ID number			E	Yes	The proposed solution creates a unique patient ID for each patient.
		Add, Edit Patient Demographics	ability to automatically associate patient ID number to the patient's record			E	Yes	The proposed creates, associates, and displays the patient ID with the patient's record.
		Add, Edit Patient Demographics	ability to track patients of all ages per jurisdictional law or policy			E	Yes	The proposed accommodates patient and immunization record data for patients of ages as appropriate with jurisdictional law or policy.
		Add, Edit Patient Demographics	ability to store mother's HBsAg status for a patient			O	Yes	The solution enables authorized users to capture and maintain the mother's HBsAg status as part of the patient record, supporting perinatal hepatitis B identification, monitoring, and related jurisdictional workflows.

Status	Req. #	Capability	Requirement: The IIS must/should have...	Comments	Reviewer notes	Priority: E, O (essential, optional)	Vendor response: Yes, with customization*, No *Comment required	Vendor comment(s)
		Add, Edit Patient Demographics	ability to store a patient's occupation	Particularly relevant for mass vaccination.		E	Yes	The proposed solution captures patient occupation.
		Add, Edit Patient Demographics	ability to designate patient as belonging to a priority group for vaccination	Particularly relevant for mass vaccination.		O	Yes	The proposed solution provides the ability to designate a patient belonging to a priority group as defined per jurisdiction.
		Add, Edit Patient Demographics	ability to store multiple patient identifiers			E	Yes	The solution supports the capture and maintenance of multiple patient identifiers within a single consolidated patient record, including multiple Medical Record Numbers (MRNs), Driver's License/State IDs, email addresses, Medicaid ID, Lead Registry ID, IIS-assigned patient ID, and other applicable identifiers. This flexibility supports patient identification and record matching across multiple providers, organizations, and external data sources.
		Add, Edit Patient Demographics	ability to assign patient records to a cohort	Particularly relevant for mass vaccination and school reports.		E	Yes	Our configurable solution can assign patient records to one or more cohorts.
		Add, Edit Patient Demographics	ability to assign patient records to multiple cohorts	Particularly relevant for mass vaccination and school reports.		E	Yes	Our configurable Solution has the ability to assign patient records to multiple cohorts.
		Add, Edit Patient Demographics	ability to view patient records by cohort	Particularly relevant for mass vaccination and school reports.		E	Yes	Our configurable solution provides the ability for authorized users to view patients by cohort.
		Add, Edit Patient Demographics	ability to remove patient records from a cohort	Particularly relevant for mass vaccination and school reports.		E	Yes	Our configurable solution can remove patients from a cohort.
		Patient Status	ability to manage patient status at the organization/facility level			E	Yes	Status can be managed at the patient/facility/organization level.
		Patient Status	ability to store active patient status at the organization/facility level			E	Yes	Status can be stored at the patient/facility/organization level.
		Patient Status	ability to store inactive patient status at the organization/facility level			E	Yes	Inactive status can be stored at the patient/facility/organization level.
		Patient Status	ability to edit active patient status at the organization/facility level			E	Yes	Editing of status information can be performed and stored at the patient/facility/organization level.
		Patient Status	ability to edit inactive patient status at the organization/facility level			E	Yes	Editing of status information can be performed and stored at the patient/facility/organization level.
		Patient Status	ability to store reason for inactive status of patients at the organizational/facility level			E	Yes	A reason can be noted for the Inactive status of patients.
		Patient Status	ability to edit multiple patients status in one action			O	Yes	The proposed Solution allows editing of multiple patients' statuses in one action. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Patient Status	ability to manage patient status at the geographic jurisdictional level			E	Yes	Authorized users can capture and manage the patient's address and county information including active/inactive patient status to correlate geographic location with the patient's status.
		Patient Status	ability to store active patient status at the geographic jurisdictional level			E	Yes	Authorized users can capture and manage the patient's address and county information including active/inactive patient status to correlate geographic location with the patient's status.
		Patient Status	ability to store inactive patient status at the geographic jurisdictional level			E	Yes	Authorized users can capture and manage the patient's address and county information including active/inactive patient status to correlate geographic location with the patient's status.
		Patient Status	ability to edit active patient status at the geographic jurisdictional level			E	Yes	Authorized users can capture and manage the patient's address and county information including active/inactive patient status to correlate geographic location with the patient's status.
		Patient Status	ability to edit inactive patient status at the geographic jurisdictional level			E	Yes	Authorized users can capture and manage the patient's address and county information including active/inactive patient status to correlate geographic location with the patient's status.
		Patient Status	ability to store reason for inactive status of patients at the geographic jurisdictional level			O	Yes	The proposed solution provides the ability to store the reason for Inactive status. It allows for these statuses: Active, Inactive-Unspecified, Inactive-Lost to follow-up (cannot contact), Inactive-Moved or gone elsewhere (transferred), Inactive, Permanently Inactive (do not reactivate), and Unknown.
		Patient Status	ability to restrict access to patient records that have been placed in an inactive status			O	Yes	Access to inactive patient records is controlled through jurisdiction-managed, role-based security permissions. Authorized administrators can configure user roles and permissions to determine which users may view inactive patient records, ensuring access aligns with Oregon's security policies and operational requirements.
		Patient Status	ability to restrict edits to patient records that have been placed in an inactive status			O	Yes	Access to inactive patient records is controlled through jurisdiction-managed, role-based security permissions. Authorized administrators can configure user roles and permissions to determine which users may view inactive patient records, ensuring access aligns with Oregon's security policies and operational requirements.
		Patient Consent	ability to manage patient consent per jurisdictional policy			E	Yes	The solution has two options for this, one being the Patient Consent option in patient demographics and the other being a Patient Locked option, also on the patient demographics screen. The solution adheres to jurisdictional policy with regard to default consent.
		Patient Consent	ability to update patient consent on a patient's record			E	Yes	The solution supports patient consent and opt-out designations within the patient record. Gainwell will work directly with the jurisdiction to configure and apply consent rules in accordance with its applicable policies, laws, and program requirements.
		Patient Consent	ability to opt out a patient from participating in the IIS			E	Yes	The proposed solution allows for a patient to be opted out. If the jurisdiction allows, the solution can hash the patient to match at a later time in the event the patient would like to opt in.
Added		Patient Consent	ability to opt in a patient for participation in the IIS			E	Yes	The proposed solution allows for a patient to be opted out. If the jurisdiction allows, the solution can hash the patient to match at a later time in the event the patient would like to opt in.
		Patient Consent	ability to enable access to a patient record per consent designation			E	Yes	The solution supports restricting or locking patient record viewing based on the patient's consent designation. Configurable roles and permissions provide an additional layer of access control, allowing the jurisdiction to determine which authorized users may access restricted patient information. Gainwell will work with the jurisdiction to align these controls with its specific consent and opt-out requirements.
		Patient Consent	ability to enable updates to a patient record per consent designation			E	Yes	The solution supports role- and permission-based controls governing who may update patient information, including records subject to consent or opt-out restrictions. Gainwell will work directly with the jurisdiction to configure the appropriate combination of patient consent rules, record restrictions, roles, and permissions to ensure updates are handled in accordance with jurisdictional requirements.

Status	Req. #	Capability	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)
		Add, Edit Patient Immunization	ability to add vaccination event information to a patient record			E	Yes	The solution enables authorized users to add vaccination event information directly to a patient record, including administered, non-inventory, and historical immunizations. The solution captures applicable vaccination details such as administration date, vaccine and lot information, manufacturer, route, body site, ordering and administering provider, funding source and eligibility, dose quantity, and VIS information. When applicable, administered doses can be linked directly to facility inventory to support accurate dose decrementing and vaccine accountability.
		Add, Edit Patient Immunization	ability to edit vaccine information in a patient record			E	Yes	The solution enables authorized users to edit vaccine administration information within a patient's immunization record. Users can update vaccine administration details, including administration date, manufacturer, lot number, funding source, eligibility, dose quantity, route, anatomic injection site, administering provider, ordering provider, and Vaccine Information Statement (VIS) information, in accordance with role-based security permissions. All changes are maintained as part of the patient's permanent immunization record and support auditability and data integrity.
		Add, Edit Patient Immunization	ability to mark vaccine information in a patient record for deletion			O	Yes	The solution enables authorized users to mark vaccine administration records for deletion in accordance with role-based security permissions. Vaccine records remain subject to audit and data integrity controls to preserve the accuracy of the permanent immunization record.
		Add, Edit Patient Immunization	ability to add reason for deletion of vaccine information in a patient record			O	Yes	The solution requires documentation of the reason when a vaccine administration record is marked for deletion.
		Add, Edit Patient Immunization	ability to capture vaccine eligibility by vaccine dose for publicly purchased vaccine			E	Yes	The solution captures vaccine eligibility at the individual dose level for publicly purchased vaccines. Eligibility information is recorded during vaccine administration and associated with the administered dose to support inventory management, funding accountability, reporting, and compliance with public vaccine program requirements.
		Add, Edit Patient Immunization	ability to store vaccine eligibility by vaccine dose for publicly purchased vaccine			E	Yes	The solution permanently stores vaccine eligibility information for each administered publicly purchased vaccine dose as part of the patient's immunization record, supporting funding accountability, inventory reconciliation, clinical review, and reporting.
		Add, Edit Patient Immunization	ability to report multiple doses administered to the same patient on the same administration date via the UI			E	Yes	The solution supports entry and management of multiple vaccine doses administered to the same patient on the same administration date through the user interface. Each administered dose is captured as an individual immunization event with its own vaccine-specific administration details, including manufacturer, lot number, funding source, eligibility, route, anatomic site, dose quantity, VIS information, and other required clinical documentation, ensuring accurate patient records and reporting.
		Add, Edit Patient Immunization	ability to store all CDC-endorsed core data elements related to vaccine events			E	Yes	The solution stores CDC-endorsed immunization event data elements as part of the permanent patient immunization record. Vaccine event records support nationally recognized immunization data standards and include vaccine product information, administration details, manufacturer, lot number, funding source and eligibility, administering and ordering provider, Vaccine Information Statement (VIS) information, clinical administration details, and other CDC-recommended immunization event data elements required for clinical care, inventory management, reporting, and interoperability.
		Add, Edit Patient Immunization	ability to enter vaccination substandard or otherwise compromised flag			E	Yes	The solution supports documentation of substandard or otherwise compromised vaccine administrations by allowing authorized users to designate an administered dose as suboptimal. This flag is maintained as part of the immunization event and identifies vaccine doses that may be ineffective due to conditions such as expiration, improper storage, handling, or administration. The designation is permanently associated with the vaccination record to support clinical review, revaccination decisions, forecasting, and reporting.
		Add, Edit Patient Immunization	ability to view submitted vaccination event information on a patient's record			E	Yes	The solution maintains a complete, permanent immunization history for each patient. Authorized users can view submitted vaccination event information, including vaccine product, administration date, manufacturer, lot number, funding source, eligibility, administering provider, clinical documentation, and associated immunization details as part of the patient's comprehensive immunization record.
		Add, Edit Patient Immunization	ability to store adverse reactions in accordance with Vaccine Recommendations and Guidelines of the ACIP			E	Yes	The solution supports documentation and storage of adverse reactions associated with vaccine administrations. Adverse reactions are recorded using standardized clinical terminology consistent with ACIP recommendations and national immunization standards, allowing reactions to be permanently associated with the patient's immunization record to support clinical decision-making, future vaccination assessments, and reporting.
		Add, Edit Patient Immunization	ability to flag an adverse reaction as having been reported to VAERS			E	Yes	The solution enables authorized users to indicate whether a documented adverse reaction has been reported to the Vaccine Adverse Event Reporting System (VAERS). The VAERS reporting status is maintained as part of the patient's adverse reaction record, supporting clinical documentation, regulatory reporting, and follow-up activities.
		Add, Edit Patient Immunization	ability to store patient vaccination event funding eligibility information			E	Yes	The solution captures and permanently stores patient funding eligibility for each vaccine administration event. Funding eligibility is recorded at the individual vaccine dose level and maintained as part of the patient's permanent immunization record, supporting public and private vaccine program requirements, inventory accountability, reporting, interoperability, and auditability.
		Add, Edit Patient Immunization	ability to print form for signature of vaccine refusal by patient for each individual vaccine antigen			O	Yes	The solution prints a Vaccine Refusal Form that supports individual antigen-specific vaccine refusals, providing separate signature lines for each vaccine antigen along with patient demographics, refusal documentation, patient/provider signatures, and acknowledgement of informed refusal.
		Add, Edit Patient Immunization	ability to ensure that the default lot number is from the oldest lot when entering an administered dose from inventory			E	Yes	The solution automatically defaults vaccine selection to the oldest available inventory lot (first-to-expire) when administering vaccines from inventory. This approach promotes appropriate inventory rotation, minimizes vaccine wastage, and supports best practices for vaccine inventory management while allowing authorized users to select a different eligible lot when clinically or operationally appropriate.
		Add, Edit Patient Immunization	ability to record administration of vaccination regardless if vaccine has since expired in inventory			E	Yes	The solution supports documentation of vaccine administrations regardless of the current inventory expiration status. Authorized users may enable the "Show Expired Inventory Lots" option to select and record an administered dose from an expired inventory lot when clinically or operationally appropriate. This preserves the historical accuracy of the immunization record while maintaining the association with the original inventory lot, manufacturer, funding source, and expiration date for complete auditability and inventory tracking.
		Add, Edit Patient Immunization	ability to track vaccinations that require adjuvant	Particularly relevant for mass vaccination.		E	Yes	The solution supports tracking of vaccines that require an adjuvant through vaccine product and clinical decision support. Vaccine records maintain product-specific characteristics, including adjuvant requirements where applicable, enabling accurate inventory management, administration, forecasting, and clinical decision-making.

Status	Req. #	Capability	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)
		Print/Export Record	ability to securely print a patient immunization record			E	Yes	The solution enables authorized users to securely view, print, and export patient immunization records through role-based security. Patient reports are currently available in English, Spanish, French, and German, supporting multilingual communication with patients and providers. Gainwell will work with the State of Oregon to configure and implement additional languages as requested to meet jurisdictional business, school, and public health communication requirements. Report layouts and content are configurable to support Oregon-specific forms, certificates, and reporting needs while maintaining consistency across printed and exported patient records.
		Print/Export Record	ability to include evaluated history in the printable version of the patient record			E	Yes	The solution supports inclusion of the patient's evaluated immunization history within printable immunization reports. Report content is configurable by Gainwell to align with Oregon's reporting requirements and provide clinicians, schools, and patients with a comprehensive immunization history.
		Print/Export Record	ability to include the forecast in the printable version of the patient record			E	Yes	The solution supports inclusion of the patient's forecasted immunizations within printable patient immunization reports. Gainwell will configure report content to include immunization forecasting information consistent with Oregon's clinical and reporting requirements.
		Print/Export Record	ability to include immunity in the printable version of the patient record			E	Yes	The solution supports inclusion of documented evidence of immunity within printable patient immunization records where applicable. Gainwell will configure report content to include immunity information in accordance with Oregon's reporting requirements.
		Print/Export Record	ability to securely export a patient immunization record			E	Yes	The solution enables authorized users to securely view, print, and export patient immunization records through role-based security. Patient reports are currently available in English, Spanish, French, and German, supporting multilingual communication with patients and providers. Gainwell will work with the State of Oregon to configure and implement additional languages as requested to meet jurisdictional business, school, and public health communication requirements. Report layouts and content are configurable to support Oregon-specific forms, certificates, and reporting needs while maintaining consistency across printed and exported patient records.
		Print/Export Record	ability to export a patient record in user-defined format			O	Yes	The solution enables authorized users to securely view, print, and export patient immunization records through role-based security. Patient reports are currently available in English, Spanish, French, and German, supporting multilingual communication with patients and providers. Gainwell will work with the State of Oregon to configure and implement additional languages as requested to meet jurisdictional business, school, and public health communication requirements. Report layouts and content are configurable to support Oregon-specific forms, certificates, and reporting needs while maintaining consistency across printed and exported patient records.
		Mass Vaccination	ability to support mass vaccination operations	Necessary for mass vaccination.		E	Yes	The Mass Vaccination module includes processes to facilitate vaccination activities in response to a pandemic, disease outbreak, natural disaster, or another public health emergency, along with real-time tools for implementing those processes. The solution requires jurisdiction-defined patient demographic information offline and online during a mass vaccination clinic.
		Mass Vaccination	ability to rapidly capture patient demographic information offline during mass vaccination clinic for later upload/saving	Necessary for mass vaccination.		E	Yes	The Mass Vaccination module includes processes to facilitate vaccination activities in response to a pandemic, disease outbreak, natural disaster, or another public health emergency, along with real-time tools for implementing those processes. The solution requires jurisdiction-defined patient demographic information offline and online during a mass vaccination clinic. The Mass Vaccination module streamlines the ability to support real-time data entry during a mass vaccination event through rapid data entry of the minimum patient data requirements. Entry fields include First Name and Last Name, Date of Birth, and Gender/Sex. The two-dimensional bar-coding capability will assist in accurately capturing vaccine lot numbers and expiration dates, inventory management, and validating and forecasting vaccines. The solution supports the digital scanning of vaccine information to distribute needed immunizations rapidly. The module can process real-time data from HL7 messages and flat-file uploads to capture events offline.
		Mass Vaccination	ability to rapidly capture vaccine information offline during mass vaccination clinic for later upload/saving	Necessary for mass vaccination.		E	Yes	The solution supports offline mass vaccination operations through a Microsoft Excel-based offline data capture template designed for rapid use in high-volume vaccination clinics. Patient demographic and vaccine administration information can be entered directly into the Excel workbook without requiring users to create HL7 messages or transform data into flat files. The template includes reference tabs (e.g., vaccine inventory, eligibility, route, body site, gender, and dose quantity) to promote standardized data entry and reduce errors during mass vaccination events. Once connectivity is restored, the completed workbook can be uploaded to the IIS, where patient demographic and vaccination event information are validated and imported, providing an efficient and practical solution for jurisdictions conducting large-scale vaccination clinics in locations with limited or no internet connectivity.
		Mass Vaccination	ability to support rapid capture of patient demographic information during mass vaccination clinic	Necessary for mass vaccination.		E	Yes	The solution provides streamlined workflows optimized for high-volume mass vaccination events, enabling rapid capture of both patient demographic and vaccine administration information. Authorized users can quickly locate existing patients using multiple search methods or register new patients through an efficient demographic entry workflow. To further accelerate patient throughput, the solution supports 2D barcode scanning to automatically populate vaccine administration details, reducing manual data entry and improving accuracy. For clinics operating in locations with limited or no network connectivity, the solution also provides an offline Microsoft Excel data capture workbook that allows patient demographic and vaccination information to be entered using a familiar interface without requiring HL7 message creation or flat-file transformations. Built-in reference worksheets help standardize data entry, and upon restoration of connectivity, the completed workbook can be uploaded to the IIS where the information is validated and incorporated into the patient's permanent immunization record. Together, these capabilities support efficient, scalable, and accurate mass vaccination operations while minimizing administrative burden on providers and public health staff.

Function: Manage Patient and Immunization Records

[Return to Cover Page](#)

Status	Req. #	Capability	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)
		Mass Vaccination	ability to support rapid capture of vaccine information during mass vaccination clinic	Necessary for mass vaccination.		E	Yes	The solution provides streamlined workflows optimized for high-volume mass vaccination events, enabling rapid capture of both patient demographic and vaccine administration information. Authorized users can quickly locate existing patients using multiple search methods or register new patients through an efficient demographic entry workflow. To further accelerate patient throughput, the solution supports 2D barcode scanning to automatically populate vaccine administration details, reducing manual data entry and improving accuracy. For clinics operating in locations with limited or no network connectivity, the solution also provides an offline Microsoft Excel data capture workbook that allows patient demographic and vaccination information to be entered using a familiar interface without requiring HL7 message creation or flat-file transformations. Built-in reference worksheets help standardize data entry, and upon restoration of connectivity, the completed workbook can be uploaded to the IIS where the information is validated and incorporated into the patient's permanent immunization record. Together, these capabilities support efficient, scalable, and accurate mass vaccination operations while minimizing administrative burden on providers and public health staff.
		Mass Vaccination	ability to administer vaccines during public health emergency without impacting the patient's status at the organization/facility level	Necessary for mass vaccination.		O	Yes	The solution supports administration of vaccines during mass vaccination and public health emergency events without requiring changes to a patient's organization or facility affiliation. Vaccination events are associated with the mass vaccination clinic while preserving the patient's existing organizational relationships and demographic record within the IIS.
		Mass Vaccination	ability for jurisdictional admin to flag/indicate org/facility participation in mass vaccination event	Necessary for mass vaccination.		O	Yes	The solution enables jurisdiction administrators to create and manage mass vaccination events and associate participating organizations and facilities with each event. Event configuration includes management of participating locations, vaccine inventory, event status, and operational details, providing centralized oversight of jurisdiction-wide mass vaccination activities.

Status	Req. #	Capability	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)
		Vaccine Inventory Search	ability to search inventory by user-defined parameters			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management. The solution provides robust inventory search and filtering capabilities that enable users to quickly locate and manage vaccine inventory. Users may perform keyword searches or utilize advanced user-defined filters to refine inventory results by one or more criteria, including facility and organization, trade name, vaccine type, National Drug Code (NDC), lot number, funding source (e.g., public, private), funding program (e.g., VFC, 317, CHIP, State, Pandemic, Private), active/inactive inventory status, expiration date, minimum and maximum quantity on hand, ordering intent (where applicable), manufacturer, and packaging type. Search results are displayed in configurable, sortable inventory lists that provide real-time visibility into current inventory, including vaccine details, lot information, funding source and program, expiration date, manufacturer, quantity on hand, and associated facility. Users can further manage inventory directly from the search results through editing, repayment, transaction history, shipment acceptance, and inventory reconciliation workflows.
		Vaccine Inventory Search	ability to search the inventory by funding source			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management. The solution provides robust inventory search and filtering capabilities that enable users to quickly locate and manage vaccine inventory. Users may perform keyword searches or utilize advanced user-defined filters to refine inventory results by one or more criteria, including facility and organization, trade name, vaccine type, National Drug Code (NDC), lot number, funding source (e.g., public, private), funding program (e.g., VFC, 317, CHIP, State, Pandemic, Private), active/inactive inventory status, expiration date, minimum and maximum quantity on hand, ordering intent (where applicable), manufacturer, and packaging type. Search results are displayed in configurable, sortable inventory lists that provide real-time visibility into current inventory, including vaccine details, lot information, funding source and program, expiration date, manufacturer, quantity on hand, and associated facility. Users can further manage inventory directly from the search results through editing, repayment, transaction history, shipment acceptance, and inventory reconciliation workflows.
		Vaccine Inventory Search	ability to search inventory by vaccine type			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management. The solution provides robust inventory search and filtering capabilities that enable users to quickly locate and manage vaccine inventory. Users may perform keyword searches or utilize advanced user-defined filters to refine inventory results by one or more criteria, including facility and organization, trade name, vaccine type, National Drug Code (NDC), lot number, funding source (e.g., public, private), funding program (e.g., VFC, 317, CHIP, State, Pandemic, Private), active/inactive inventory status, expiration date, minimum and maximum quantity on hand, ordering intent (where applicable), manufacturer, and packaging type. Search results are displayed in configurable, sortable inventory lists that provide real-time visibility into current inventory, including vaccine details, lot information, funding source and program, expiration date, manufacturer, quantity on hand, and associated facility. Users can further manage inventory directly from the search results through editing, repayment, transaction history, shipment acceptance, and inventory reconciliation workflows.
		Vaccine Inventory Search	ability to search inventory by vaccine lot number			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management. The solution provides robust inventory search and filtering capabilities that enable users to quickly locate and manage vaccine inventory. Users may perform keyword searches or utilize advanced user-defined filters to refine inventory results by one or more criteria, including facility and organization, trade name, vaccine type, National Drug Code (NDC), lot number, funding source (e.g., public, private), funding program (e.g., VFC, 317, CHIP, State, Pandemic, Private), active/inactive inventory status, expiration date, minimum and maximum quantity on hand, ordering intent (where applicable), manufacturer, and packaging type. Search results are displayed in configurable, sortable inventory lists that provide real-time visibility into current inventory, including vaccine details, lot information, funding source and program, expiration date, manufacturer, quantity on hand, and associated facility. Users can further manage inventory directly from the search results through editing, repayment, transaction history, shipment acceptance, and inventory reconciliation workflows.
		Vaccine Inventory Search	ability to search inventory by vaccine NDC code			E	Yes	The solution enables authorized users to search and identify vaccine inventory using the vaccine National Drug Code (NDC). Inventory results provide associated vaccine and lot-level information, including trade name, lot number, expiration date, quantity on hand, funding source/program, manufacturer, and packaging information to support efficient inventory management and vaccine accountability.

Status	Req. #	Capability	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)
		Add, Edit Vaccine Inventory	ability to manage vaccine inventory			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
		Add, Edit Vaccine Inventory	ability to support visualization of current vaccine inventory			E	Yes	The solution provides real-time visualization of current vaccine inventory through comprehensive inventory views at both the organization and facility levels. Users can view inventory by vaccine, trade name, manufacturer, NDC, lot number, funding source and program, ordering intent, expiration date, packaging, active status, and quantity on hand. Sortable columns, configurable filters, and search capabilities enable users to quickly assess inventory status, identify expiring vaccine, monitor available quantities, and access inventory management actions such as editing, repayment, transactions, shipment acceptance, and reconciliation.
		Add, Edit Vaccine Inventory	ability to edit inventory funding source at the lot level			E	Yes	The solution allows authorized users to edit inventory records at the individual lot level, including updating the associated funding source and funding program as permitted by business rules. Funding source changes are maintained at the inventory lot record to ensure accurate inventory tracking, reporting, and accountability for public and private vaccine stock.
		Add, Edit Vaccine Inventory	ability to edit inventory funding source at the vaccine level			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
		Add, Edit Vaccine Inventory	ability to add vaccine information to inventory			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
		Add, Edit Vaccine Inventory	ability to support barcode scanning system to electronically upload vaccine inventory to the IIS	Particularly relevant for mass vaccination.		O	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
		Add, Edit Vaccine Inventory	ability to view current inventory list by facility			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
		Add, Edit Vaccine Inventory	ability to view current inventory list by organization			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
		Add, Edit Vaccine Inventory	ability for jurisdictional admin to edit organization/facility inventory			E	Yes	The solution provides comprehensive vaccine inventory management capabilities at the organization and facility levels. Vaccine inventory may be added through manual entry, electronic import via VTrck5, or 2D barcode scanning to streamline inventory intake and improve data accuracy. Users can view and manage real-time inventory through configurable on-screen inventory lists and search/filter inventory using user-defined criteria, including funding source, vaccine type, lot number, NDC, expiration date, facility, organization, inventory quantities, and additional inventory attributes. Authorized users can add, edit, and maintain inventory records, including updating vaccine and funding information at the appropriate inventory record (lot) level, while jurisdictional administrators can manage inventory across organizations and facilities. The solution also provides inventory transaction history, shipment acceptance, reconciliation workflows, and repayment functionality to support complete vaccine inventory lifecycle management.
Updated		Add, Edit Vaccine Inventory	ability to manage vaccine borrowed from lots belonging to one funding source to lots belonging to another funding source			O	Yes	The solution supports repayment/replacement workflows that allow users to reclassify borrowed vaccine inventory between Private and Public funding sources. During repayment, users can select the target funding source and applicable funding program, specify the quantity being repaid, and update inventory balances accordingly, ensuring accurate inventory accountability and funding source reconciliation.
		Add, Edit Vaccine Inventory	ability to reclassify funding source of borrowed vaccine from private to public or vice versa for replacement cases			O	Yes	The solution supports repayment/replacement workflows that allow users to reclassify borrowed vaccine inventory between Private and Public funding sources. During repayment, users can select the target funding source and applicable funding program, specify the quantity being repaid, and update inventory balances accordingly, ensuring accurate inventory accountability and funding source reconciliation.
		Add, Edit Vaccine Inventory	ability to view storage capability	Particularly relevant for mass vaccination.		E	Yes	The solution provides configurable vaccine storage unit management, allowing users to view and maintain storage locations and associated characteristics. Storage units include attributes such as unit name, storage type (e.g., refrigerator, freezer, ultra-cold freezer), temperature scale (Fahrenheit or Celsius), equipment style, and active status, providing visibility into available vaccine storage capacity.

[Return to Cover Page](#)

Status	Req. #	Capability	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)
		Add, Edit Vaccine Inventory	ability to document vaccine storage and handling events such as temperature excursions	Particularly relevant for mass vaccination.		E	Yes	The solution supports documentation of vaccine storage and handling activities through temperature log management. Users can record daily temperature readings, minimum and maximum temperatures, office open status, excursion reasons, and comments for individual storage units. The system supports identification and documentation of temperature excursions, maintains historical temperature records, and allows notification recipients to be configured for excursion-related alerts sent via email.
		Add, Edit Vaccine Inventory	ability to store storage capability	Particularly relevant for mass vaccination.		E	Yes	The solution maintains configurable storage unit records that define each vaccine storage location and its operational characteristics. Authorized users can add, edit, activate, and maintain storage units, including storage type, equipment style, temperature scale, and status, providing persistent storage configuration to support vaccine inventory management and temperature monitoring.
		Vaccine Ordering	ability for rule based logic to recommend vaccine order quantity			E	Yes	The solution uses rule-based logic to calculate and recommend vaccine order quantities based on actual provider utilization and inventory needs. The ROQ calculation considers factors such as recent vaccine administration, historical utilization for comparable periods, usable inventory on hand, pending vaccine orders, safety stock, wastage factors, and package size. Key calculation variables, including look-back periods, funding/eligibility criteria, expiration thresholds, and wastage factors to support jurisdictional business rules. Recommended quantities are adjusted to prevent negative values and rounded to appropriate package sizes. This data-driven approach helps providers maintain adequate vaccine supply while reducing the risk of stockouts, over-ordering, and unnecessary vaccine waste.
		Vaccine Ordering	ability to alert user when "reorder recommendation" Inventory level is reached			O	Yes	The solution supports configurable reorder recommendation alerts that notify users when vaccine inventory reaches the defined reorder threshold. Jurisdiction administrators can configure system notifications and manage which user roles receive reorder alerts, ensuring the appropriate inventory management personnel are notified when additional vaccine should be ordered. Reorder notifications work in conjunction with the Recommended Order Quantity (ROQ) functionality to promote timely replenishment, reduce the risk of stockouts, and support continuous vaccine availability.
Updated		Vaccine Ordering	ability to pre-populate order with recommended quantities based on inventory, doses reported as administered to IIS			E	Yes	The solution automatically pre-populates Recommended Order Quantities (ROQ) during vaccine ordering using configurable inventory management rules. ROQ calculations are based on historical vaccine utilization (including doses reported to the IIS), seasonal demand trends from the prior year, current on-hand inventory, pending vaccine orders, configurable safety stock levels, and a configurable wastage factor. The calculation excludes inventory nearing expiration based on configurable thresholds and supports jurisdiction-defined configuration of lookback periods, eligibility criteria, expiration windows, safety stock, and wastage values. Recommended quantities are automatically rounded to the appropriate package size, never return negative values, and display blank when insufficient data is available. Providers may review and adjust recommended quantities prior to order submission. In addition, jurisdiction administrators can configure system-level ordering rules, including automatic approval of vaccine orders that are at or below the calculated ROQ, while routing orders that exceed the ROQ for manual review and approval. Additional configurable controls allow jurisdictions to restrict ordering when expired publicly funded inventory exists, prevent duplicate or overlapping orders, define reconciliation eligibility windows, and require manual acceptance before inventory is added to on-hand stock.
		Vaccine Ordering	ability to edit pre-populated order quantity			E	Yes	The solution allows providers to modify system-generated recommended order quantities prior to order submission. Recommended Order Quantities (ROQ) are automatically calculated based on configurable inventory management rules; however, authorized users may increase or decrease the pre-populated order quantity to address operational needs, anticipated demand, or other jurisdiction-specific circumstances. User-entered quantities remain subject to configurable ordering rules and jurisdiction-defined approval workflows.
		Vaccine Ordering	ability to order vaccines			E	Yes	The solution provides a comprehensive vaccine ordering workflow that enables authorized providers to create, review, modify, and submit vaccine orders electronically. Users can select the appropriate order type, review available vaccines, Recommended Order Quantities (ROQ), minimum order quantities, package sizes, and product details, enter order quantities, provide justification when ordering above recommended levels, and manage orders through submission. The solution also supports maintenance of delivery addresses, vaccine program contacts, delivery hours, and special shipping instructions. Complete order history and lifecycle status (e.g., Draft, Submitted, Under Review, Approved, Declined, Sent to CDC, Cancelled) are maintained to provide full visibility into the ordering process. Jurisdiction-configurable approval workflows, including automatic approval for qualifying orders and manual review for exceptions, support efficient vaccine ordering while ensuring compliance with program policies.
		Vaccine Ordering	ability for jurisdictional admin to activate vaccines available for ordering			E	Yes	The solution enables jurisdiction administrators to inactivate vaccines available for ordering through centralized Order Set management. Administrators can define activation and deactivation dates, modify or remove vaccines from active Order Sets, and deactivate Order Sets when they are no longer valid. Changes to Order Sets immediately control vaccine ordering availability for assigned providers while preserving historical order and contract information for audit purposes.
		Vaccine Ordering	ability for jurisdictional admin to inactivate vaccines available for ordering			E	Yes	The solution enables jurisdiction administrators to inactivate vaccines available for ordering through centralized Order Set management. Administrators can define activation and deactivation dates, modify or remove vaccines from active Order Sets, and deactivate Order Sets when they are no longer valid. Changes to Order Sets immediately control vaccine ordering availability for assigned providers while preserving historical order and contract information for audit purposes.
		Vaccine Ordering	ability to order publicly-purchased vaccines			E	Yes	The solution provides a comprehensive vaccine ordering workflow that enables authorized providers to create, review, modify, and submit vaccine orders electronically. Users can select the appropriate order type, review available vaccines, Recommended Order Quantities (ROQ), minimum order quantities, package sizes, and product details, enter order quantities, provide justification when ordering above recommended levels, and manage orders through submission. The solution also supports maintenance of delivery addresses, vaccine program contacts, delivery hours, and special shipping instructions. Complete order history and lifecycle status (e.g., Draft, Submitted, Under Review, Approved, Declined, Sent to CDC, Cancelled) are maintained to provide full visibility into the ordering process. Jurisdiction-configurable approval workflows, including automatic approval for qualifying orders and manual review for exceptions, support efficient vaccine ordering while ensuring compliance with program policies.
		Vaccine Ordering	ability to view all orders by user-defined parameters			O	Yes	The solution provides comprehensive order capabilities that allow authorized users to search and view vaccine orders using user-defined search and filter criteria. Users can locate orders by parameters including order status, order type, creation date, approval date, submitting user, provider/facility, and other configurable order attributes. Search results are presented in sortable order history views that display the complete order lifecycle, enabling users to quickly identify, review, and manage vaccine orders.
		Vaccine Ordering	ability to update delivery hours to receive shipments			E	Yes	The proposed solution captures both the facility hours and the delivery hours to receive vaccine shipments.
		Vaccine Ordering	ability to enter a reason for vaccine orders outside the recommended order quantity			E	Yes	The solution allows providers to enter a justification when requesting vaccine quantities that exceed the system-calculated Recommended Order Quantity (ROQ). Jurisdictions can configure business rules to require a reason for orders outside the recommended quantity, providing reviewers with supporting information during the approval process and maintaining an audit trail of order exceptions.
		Vaccine Ordering	ability to search and view past vaccine orders by facility within a specified timeframe			E	Yes	Authorized users can search, view, and filter vaccine orders within a specified time frame.
		Vaccine Ordering	ability to verify contact information during each order without leaving ordering workflow			E	Yes	Authorized users can record and view the contact information and delivery hours during each ordering workflow.
		Vaccine Ordering	ability to update contact information during each order without leaving ordering workflow			E	Yes	Authorized users can record and view the contact information, facility information, and delivery hours during the ordering workflow. Configuration will allow authorized users to update their contact information without leaving the workflow.
		Vaccine Ordering	ability to save an unsubmitted order			E	Yes	An innovative component of the proposed solution is its virtual cart feature, which simplifies the ordering process and prevents Providers from creating multiple orders for one facility/organization. The cart can stay open for update by one or more authorized facility users. This prevents vaccine coordinators from creating duplicate orders, while allowing facilities to add vaccines over time until ready to place the entire order. When ready to submit, users can view the cart, review it, submit it, and the order is automatically routed to jurisdiction for program review and approval.

[Return to Cover Page](#)

Status	Req. #	Capability	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)
		Vaccine Ordering	ability to update organization/facility contact information before submitting a vaccine order			E	Yes	Authorized users can update facility contact information before submitting a vaccine order.
		Vaccine Ordering	ability to cancel unsubmitted or unprocessed vaccine orders			E	Yes	Authorized users can cancel unsubmitted or unprocessed vaccine orders using the Cancel button on the Edit Vaccine Order page.
		Vaccine Ordering	ability to edit unsubmitted or unprocessed vaccine orders			E	Yes	Authorized users can edit unsubmitted or unprocessed vaccine orders using the Cancel button on the Edit Vaccine Order page.
		Vaccine Ordering	ability to save an unsubmitted order after rejection			E	Yes	Authorized users can save rejected orders and filter to easily view rejected orders by create date.
		Vaccine Ordering	ability to verify order information before order submitted			E	Yes	Following the Vaccine Order workflow, orders undergo jurisdiction review and approval before release. This allows the jurisdiction to verify order information. If desired, users can cancel the unprocessed order or approve it for order processing.
		Vaccine Ordering	ability for jurisdictional admin to reject a vaccine order			E	Yes	Authorized users including Jurisdictional Administrators can reject a vaccine order from the Vaccine Orders State User page.
		Vaccine Ordering	ability for jurisdictional admin to select a reason code when rejecting an order			E	Yes	Jurisdiction users can choose from a list of different reasons for declining orders, therefore the jurisdiction need not spend time typing in the justification. Approvers use the Vaccine Orders State User page to review and approve a vaccine order and select the appropriate corresponding reason code.
		Vaccine Ordering	ability to edit an order after rejection			E	Yes	If declined, the Provider can edit the declined order and resubmit it with the correct information without having to create an entirely new order.
		Vaccine Ordering	ability to resubmit an order after rejection			E	Yes	If declined, the Provider can edit the declined order and resubmit it with the correct information without having to create an entirely new order.
		Vaccine Ordering	ability to electronically notify the facility of a rejected order			E	Yes	Providers receive notifications about actions the jurisdiction takes (e.g., approval, decline with reason). This makes it easy to communicate with Providers quickly and inform them about what they need to do for the order to be approved.
		Vaccine Ordering	ability to track the shipping status of orders			E	Yes	The solution seamlessly exchanges data with VTrackS, which facilitates the retrieval of inventory data, order information, and shipment data. Information from VTrackS is uploaded in the solution when orders are shipped from the CDC warehouse or other manufacturer warehouse. To prevent Provider acceptance of a shipment before the shipment is delivered, the solution displays the tracking status, such as In Transit or Delivered. Users can drill down to view additional shipment detail using a hyperlink displayed with the status. Clicking the link enables the user to see the actual shipment detail from the carrier. The solution also automatically notifies Providers when an order is shipped and includes tracking information so the Provider can track the shipment until received and confirmed.
		Vaccine Ordering	ability to verify packing slip information after order is shipped			O	Yes	The proposed solution, as part of the acceptance of inventory from VTrackS, will allow verification of the packing slip.
		Vaccine Ordering	ability to receive electronic notification when order quantity received does not match vaccine order			O	Yes	The proposed solution provides the ability to issue an automatic notification when the vaccine quantity received does not match the quantity ordered.
		Vaccine Ordering	ability to receive electronic notification when vaccine order received is damaged			O	Yes	The proposed solution provides the ability to distribute notifications/alerts to users about their vaccine order.
		Vaccine Ordering	ability to request shipping label(s) for nonviable vaccine subject to return			O	Yes	The proposed solution allows facilities to request labels and select label receipt method (email, mail, or pickup) per CDC requirements.
		Vaccine Ordering	ability to search for past vaccine returns within a specified timeframe			E	Yes	Authorized users can search, filter, and view past vaccine returns within a specified time frame, including by status, create date, approve date, vaccine type and/or user.
		Vaccine Ordering	ability to view past vaccine returns within a specified time frame			E	Yes	Authorized users can search, view, and filter vaccine orders within a specified time frame.
		Vaccine Ordering	ability to pre-book vaccine orders	Particularly relevant for mass vaccination.		E	Yes	Jurisdictional Administrators can set up and provide authorized users the ability to pre-book vaccine orders.
		Vaccine Ordering	ability for jurisdictional admin to allocate vaccine inventory per user defined parameters	Particularly relevant for mass vaccination.		E	Yes	Jurisdictional Administrators can allocate vaccine inventory per user-defined parameters.
		Vaccine Ordering	ability to activate vaccine ordering functionality for all designated organizations/facilities during a public health emergency	Particularly relevant for mass vaccination.		E	Yes	The mass vaccination module provides the ability for authorized users to activate ordering for the or designated facilities.
		Vaccine Ordering	ability for jurisdictional admin to create order sets	Particularly relevant for mass vaccination.		E	Yes	The solution enables jurisdiction administrators to create and manage configurable Order Sets that define the vaccines available for provider ordering. Administrators can create Order Sets by selecting vaccine products, funding programs, contracts, ordering intents, age groups, direct shipment options, and activation/deactivation dates. Order Sets may be assigned to individual providers or in bulk based on provider enrollment and facility type, allowing jurisdictions to centrally manage vaccine ordering eligibility and availability.
		Review/Approve Order	ability for jurisdictional admin to review order			E	Yes	The Vaccine Ordering workflow routes orders for jurisdiction review and approval.
		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	The proposed solution can support approval or rejection of an order if it is above or below the recommended order quantity.
		Review/Approve Order	ability for jurisdictional admin to approve order			E	Yes	The Vaccine Ordering workflow is configurable to require approvals before vaccines can be ordered.
		Review/Approve Order	ability for jurisdictional admin to adjust order			E	Yes	The Vaccine Ordering allows Jurisdictional Administrators to review and approve vaccine orders before the order can be processed. As part of this process, reviewers can click the pencil icon to edit order information.
		Review/Approve Order	ability for jurisdictional admin to electronically accept VFC vaccine into inventory			E	Yes	The proposed solution can electronically accept shipping reports to populate VFC inventory both manually and automatically.
		Review/Approve Order	ability to accept each vaccine product in the IIS after shipment is received			E	Yes	Inventory data is received via the VTrackS interface and populated in the system. Authorized users can immediately see the content of the shipment, so they know what is arriving. When a shipment is physically received, they can compare the information to the original order and confirm receipt via the solution's UI. If the information received in the shipment differs from what is in the order, there is an option to edit the information (e.g., different lot number). After verifying receipt, the user confirms the shipment, and the information is added to their inventory.
		Vaccine Dose Decrementing	ability to automatically decrement vaccine doses from inventory when matched vaccine doses are reported as administered			E	Yes	To provide the best user experience, reduce the need for manual entry, and mitigate the opportunity for mistakes, the solution's inventory management component includes a number of automations, including: - Automatic decrementing when a vaccine is administered, received, returned, or in the case of wastage - Automatic adding of vaccine data when the solution receives shipment info from the VTrackS interface - Auto-decrementing for vaccine transfers (i.e., Provider A transfers to Provider B) or for instances in which a vaccine is borrowed or returned from private stock into public stock
		Vaccine Dose Decrementing	ability to automatically match vaccine doses reported as administered to vaccine doses in inventory to facilitate dose decrementing			E	Yes	The inventory management component includes a number of automations to facilitate dose decrementing.
		Vaccine Dose Decrementing	ability to automatically decrement vaccine inventory in real-time via HL7 messaging			E	Yes	The solution's inventory management component includes a number of automations, including: - Automatic decrementing when a vaccine is administered, received, returned, or in the case of wastage - Automatic adding of vaccine data when the solution receives shipment info from the VTrackS interface - Auto-decrementing for vaccine transfers (i.e., Provider A transfers to Provider B) or for instances in which a vaccine is borrowed or returned from private stock into public stock
		Vaccine Dose Decrementing	ability to automatically decrement vaccine inventory in real-time via UI data entry			E	Yes	The inventory management component includes a number of automations to facilitate dose decrementing, regardless of the entry method or interface transfer protocol by which the vaccine administration data is received.

[Return to Cover Page](#)

Status	Req. #	Capability	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)
		Vaccine Inventory Reconciliation	ability to reconcile vaccine doses currently in physical storage with vaccine doses reflected in system inventory			E	Yes	The solution provides comprehensive inventory reconciliation capabilities that allow providers to reconcile physical vaccine inventory with inventory recorded in the system. Users can perform scheduled or on-demand reconciliations by reviewing on-hand inventory, documenting discrepancies, and submitting reconciliation results. The solution maintains reconciliation history, tracks submission status, supports multiple funding programs, and provides configurable reconciliation schedules and eligibility rules to help ensure inventory accuracy and accountability.
		Vaccine Inventory Reconciliation	ability to document reductions in vaccine inventory due to outgoing vaccine transfers			E	Yes	The solution electronically documents reductions in vaccine inventory resulting from outgoing vaccine transfers. Inventory transactions are automatically recorded and maintained with transaction type, vaccine, lot number, funding source, quantity, facility, and transaction date, providing a complete audit trail of inventory movement between facilities.
		Vaccine Inventory Reconciliation	ability to electronically document reductions in vaccine inventory due to outgoing vaccine wastage			E	Yes	The solution supports electronic documentation of vaccine wastage through configurable inventory adjustment workflows. Authorized users record vaccine wastage using standardized adjustment reason codes, and inventory quantities are automatically updated while maintaining a complete transaction history for reporting, auditing, and inventory reconciliation.
		Vaccine Inventory Reconciliation	ability to enter current number of vaccine doses on-hand in physical storage			E	Yes	The solution enables authorized users to maintain current on-hand vaccine inventory through inventory management and adjustment functions. Users may update inventory quantities using configurable adjustment reasons (e.g., shipment received, error correction, transfer, borrowing, repayment, wastage), ensuring the system accurately reflects the physical inventory on hand.
		Vaccine Inventory Reconciliation	ability to track and manage doses for vaccines: on hand, administered, wasted, expired, ordered, recalled, returned, transferred			E	Yes	The solution provides comprehensive vaccine inventory lifecycle management, enabling jurisdictions and providers to track and manage vaccine doses throughout their lifecycle. Inventory transactions capture and maintain the status of doses that are on hand, administered, wasted, expired, ordered, recalled, returned, borrowed, repaid, and transferred, with complete transaction history, inventory adjustments, shipment processing, reconciliation, and reporting to support inventory accountability and auditing.
		Vaccine Inventory Reconciliation	ability to enable removal of recalled lots from active inventory			E	Yes	Authorized users can remove recalled vaccine lots from active inventory through inventory maintenance and adjustment workflows. The solution maintains inventory transaction history and audit records while ensuring recalled vaccine is no longer available for administration or ordering.
		Vaccine Inventory Reconciliation	ability to print a reconciliation worksheet			O	Yes	The proposed solution allows for the printing of a reconciliation worksheet.
		Vaccine Transfers	ability for jurisdictional admin to approve vaccine transfers			O	Yes	The solution enables jurisdiction administrators to review and approve vaccine transfer requests through a configurable transfer workflow. Transfer requests display complete transaction details, including sending and receiving facilities, vaccine, lot number, funding source, funding program, quantity, expiration date, and transfer status, allowing administrators to approve transfers while maintaining a complete audit trail.
		Vaccine Transfers	ability for jurisdictional admin to initiate VFC vaccine transfers			O	Yes	The solution enables authorized jurisdiction administrators to initiate vaccine transfers, including VFC-funded vaccine, between eligible facilities. Transfer workflows preserve vaccine lot, funding source, funding program, quantity, and receiving facility information while maintaining complete transaction history and inventory accountability throughout the transfer process.
		Vaccine Transfers	ability to accept VFC vaccine transfers			O	Yes	The solution supports electronic acceptance of VFC vaccine transfers by authorized receiving facilities. Accepted transfers automatically update inventory records while preserving vaccine lot information, funding source, funding program, quantities transferred, and a complete audit trail of the transfer lifecycle.
		Vaccine Transfers	ability for jurisdictional admin to reject vaccine transfers			O	Yes	The solution enables jurisdiction administrators to review and reject vaccine transfer requests through the transfer approval workflow. Transfer status is updated accordingly, and all transfer decisions are maintained within the transfer history to provide complete visibility and auditability.
		Vaccine Transfers	ability to search and view past vaccine transfers within a specified timeframe			O	Yes	The solution provides comprehensive transfer inquiry capabilities that allow users to search, filter, sort, and view historical vaccine transfers using user-defined criteria. Transfer history may be queried by status, transfer type, create date range, ship date range, sending facility, receiving facility, user, and other configurable transfer attributes, providing complete visibility into current and historical vaccine transfer activity.
		Vaccine Transfers	ability for jurisdictional admin to allow for direct vaccine transfer between facilities without jurisdictional pre-approval, but with jurisdictional visibility/oversight.	Particularly relevant for mass vaccination.		O	Yes	The solution provides configurable jurisdiction-level transfer policies that determine whether external vaccine transfers require prior approval. Jurisdiction administrators can enable direct facility-to-facility transfers without pre-approval or require approval before shipment. Regardless of the configuration, all transfer activity is maintained within the centralized transfer history, providing jurisdictions with complete visibility, oversight, status tracking, and audit history of vaccine transfers.
		Vaccine Wastage	ability to manage vaccine wastage			E	Yes	The solution provides comprehensive vaccine wastage management capabilities that enable authorized users to create, submit, track, and manage vaccine wastage events. Wastage records capture funding source, vaccine, lot number, quantity, manufacturer, reason for wastage, preventive actions, status, and associated costs while maintaining a complete audit trail and supporting electronic submission via VTrack.
		Vaccine Wastage	ability to determine the total cost of wasted vaccine by user-defined parameters			E	Yes	The solution includes reporting capabilities that calculate and display the total cost of wasted vaccine using user-defined search and filter criteria. The Wasted Vaccines Cost Report summarizes wasted vaccine quantities and associated costs for selected organizations and reporting periods and supports filtering by date range, facility, funding source, user, and other configurable reporting parameters.
		Vaccine Wastage	ability for jurisdictional admin to modify inventory quantity to reflect wastage			E	Yes	The solution automatically updates vaccine inventory to reflect documented wastage through electronic inventory adjustment workflows. Authorized users record vaccine wastage quantities, and the corresponding inventory is reduced while preserving the associated vaccine lot, funding source, funding program, adjustment reason, and complete transaction history for audit and reconciliation purposes.
		Vaccine Wastage	ability for jurisdictional admin to assign reason for inventory wastage			E	Yes	The solution supports standardized assignment of vaccine wastage reasons during the wastage reporting process. Jurisdiction-approved reason codes may include examples such as Broken, Drawn into Syringe but Not Administered, Lost/Unaccounted, Non-Vaccine Product, Open Vial but Not Administered, Expired, Recall, Other, and additional jurisdiction-defined reasons as configured. Wastage reasons are maintained as part of the permanent inventory and reporting record.
		Vaccine Wastage	ability to determine the total doses of vaccine wasted by user-defined parameters			E	Yes	The solution provides configurable wastage inquiry and reporting capabilities that allow users to determine total wasted vaccine doses using user-defined search criteria. Wastage records and reports may be filtered by facility, funding source, reporting period, wastage reason, user, and other configurable parameters, enabling jurisdictions to analyze vaccine wastage trends, quantities, and operational impacts.
		Vaccine Expiration	ability to manage vaccine expiration			E	Yes	The solution provides comprehensive vaccine expiration management capabilities throughout the inventory lifecycle. Vaccine inventory records maintain expiration dates and display the number of days remaining until expiration, enabling users to proactively monitor expiring inventory. Jurisdiction administrators can configure role-based notifications for configurable expiration thresholds (e.g., 60 days, 30 days, and expiration day) to alert designated users of vaccines approaching or reaching expiration. Authorized users can update inventory records, process expired vaccine through standardized wastage workflows, adjust inventory quantities, and maintain complete transaction history to ensure expired vaccine is appropriately managed, removed from active inventory, and accurately reflected in inventory reconciliation and reporting.
		Vaccine Expiration	ability to alert users to vaccine nearing expiration			O	Yes	The solution provides configurable notifications for vaccine inventory approaching expiration and inventory that has already expired. Jurisdiction administrators can assign role-based notifications to alert designated users at configurable expiration intervals (e.g., 60 days, 30 days, and expiration day). In addition, inventory management screens display both the expiration date and the number of days remaining until expiration for each vaccine lot, enabling users to proactively identify expiring inventory, prioritize vaccine usage, process expired vaccine for wastage or removal from active inventory, and support inventory reconciliation while maintaining compliance with jurisdictional inventory management policies.

[Return to Cover Page](#)

Status	Req. #	Capability	Requirement: The IS must/should have...	Comments	Reviewer notes	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
		Vaccine Expiration	ability to provide alerts for inventory already expired			O	Yes	The solution provides configurable notifications for vaccine inventory approaching expiration and inventory that has already expired. Jurisdiction administrators can assign role-based notifications to alert designated users at configurable expiration intervals (e.g., 60 days, 30 days, and expiration day). In addition, inventory management screens display both the expiration date and the number of days remaining until expiration for each vaccine lot, enabling users to proactively identify expiring inventory, prioritize vaccine usage, process expired vaccine for wastage or removal from active inventory, and support inventory reconciliation while maintaining compliance with jurisdictional inventory management policies.
		Vaccine Expiration	ability for jurisdictional admin to modify inventory quantity removed from available inventory			E	Yes	The solution enables authorized jurisdiction administrators to modify the quantity of vaccine removed from available inventory through configurable inventory adjustment workflows. Inventory quantities can be adjusted using standardized adjustment reason codes (e.g., wastage, error correction, transfers, borrowing, repayment, shipment receipt, expiration, and other jurisdiction-defined reasons), ensuring inventory accurately reflects available vaccine. All adjustments are recorded with the associated vaccine, lot number, funding source, quantity, adjustment reason, user, and transaction date, providing a complete audit trail for inventory management, reconciliation, and reporting.

Status	Req. #	Capability	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)
Updated		Standard Reports	ability to generate a report that includes history and forecast			E	Yes	The proposed Solution provides a page-per-patient Immunization report that includes the patient's immunization history and forecast. Reports can be generated in supported languages, including English and Spanish, with additional languages configurable based on jurisdictional requirements.
		Standard Reports	ability to generate a data quality report displaying information on the quality of submitted data			E	Yes	The data analytics and reporting component enables authorized users to create reports and visualizations using available data elements across various record types within the solution to assist in error mitigation.
		Standard Reports	ability to generate a report that provides information on patient and vaccine matching and deduplication			E	Yes	The proposed Solution provides reports and dashboards identifying patient and vaccination event matching and deduplication activities, including suspected duplicates, merged records, unresolved duplicates, and records requiring manual review.
		Standard Reports	ability to generate a report that provides information on data quality of data at rest			E	Yes	The solution provides a number of reports regarding administration data, patient updates, and HL7 drill-downs for data at rest that are exportable in both Excel and PDF.
		Standard Reports	ability to generate data quality reports for HL7 submissions			E	Yes	Easy-to-understand visual dashboards are available to show the results of HL7 and other file exchange processing. HL7 File Exchange Analytics dashboards provide visibility for authorized users to view how many transactions processed successfully, how many have errors, what types of errors are being seen, and more.
		Standard Reports	ability to generate VFC reports			E	Yes	VFC Reports are available within the solution's data analytic and reporting components.
		Standard Reports	ability to generate a practice-level patient data report for VFC enrolled sites			E	Yes	Authorized users can use ad hoc reports to generate reports about their patient data including immunization, vaccine, and patient-specific demographics.
		Standard Reports	ability to generate a doses administered report to support accountability for publicly-purchased vaccine			E	Yes	Authorized users can generate a Doses Administered report for authorized users of a facility.
		Standard Reports	ability to generate a doses administered report for VFC enrolled sites			E	Yes	Authorized users can generate a Doses Administered report for authorized users of a VFC facility.
		Standard Reports	ability to generate VFC provider practice profiles			E	Yes	The proposed solution can display a VFC provider profile with demographics and VFC specific identifiers.
		Standard Reports	ability to generate a report showing the total number of select vaccines administered each month by facility			E	Yes	The proposed solution uses consumed data to provide metric dashboards and reports with pertinent information for immunization programs. These include vaccine rates, vaccine consumption, ordering system usage, and overall health. The solution's data analytics and reporting component can present a variety of visual formats and complies with federal, State, and local immunization reporting requirements.
		Standard Reports	ability to generate a report displaying a change in vaccine administration patterns over a selected timeframe			E	Yes	The Vaccine Dashboard, Vaccine Breakup, and Administrations dashboards provide visualizations of data over a period of time to understand ordering and administration trends.
		Standard Reports	ability to generate duplicate/merge record reports			E	Yes	The solution provides a view of duplicates and an individual view of clients needing to be merged. Unmerge functionality can view data received since the patients were merged.
		Standard Reports	ability to generate reports about IIS users			E	Yes	Authorized users can search for users by facility, name, or email and display name, username, email address, role, status, and last login date.
		Standard Reports	ability to generate vaccine management reports			E	Yes	The reporting component provides a number of vaccine-related dashboards that are exportable, including orders by status, orders by type, inventory running low, inventory about to expire, and inventory filtering and sort abilities.
		Standard Reports	ability to generate a report listing/identifying patients who received a recalled vaccine			E	Yes	The reminder/recall feature allows for an authorized user to create an exportable list of patients who received a recalled vaccine.
		Standard Reports	ability to generate a report of patients declining or refusing vaccinations			O	Yes	The patient comments allow for individual vaccines to be selected as declining or refusal including start and end times to assist in determining whether vaccines should be forecasted in the future. The refusal report will allow for an authorized user to generate a list of patients declining or refusing vaccines.
		Standard Reports	ability to generate a report to calculate a facility's average vaccine usage			O	Yes	The Immunization Solution proposed uses dashboards to allow for exportable data about the facility's average vaccine usage on administration and ordering.
		Standard Reports	ability to generate VFC accountability reports for managing VFC inventories and orders			E	Yes	Exportable vaccine and Inventory dashboards are available to manage vaccine Inventories.
		Standard Reports	ability to generate vaccine inventory reports			E	Yes	The proposed Solution allows for pinnable dashboards to detail inventory such as vaccine inventory running low and vaccines about to expire. The solution allows for filtering and dynamic search to view vaccine inventory by trade name, NDC, Active, Expiration Date (within 30 and/or 60 days and/or expired), inventory on hand min and max, public private funding programs.
		Standard Reports	ability to generate a report that provides/displays information about current inventory on hand			E	Yes	Authorized users can view one or many vaccine inventories and filter to view trade name, NDC, Active, expiration date, inventory on hand min and max, and funding program.
		Standard Reports	ability to generate a report that provides/displays information about inventory transactions			E	Yes	The reporting component provides an inventory transaction report by inventory type, quantity, and date.
		Standard Reports	ability to generate report(s) that display information about vaccine order history			O	Yes	The proposed solution has robust filtering to allow for reports on vaccine orders including status (approved, created, submitted), create date, approve date, vaccine type, user with each field also easily being sortable.
		Standard Reports	ability to generate report(s) that display information about vaccine wastage and returns			E	Yes	The proposed solution can generate reports about vaccine wastage and returns at both a facility and jurisdictional level.

Function: Provide Data Access

[Return to Cover Page](#)

Status	Req. #	Capability	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)
		Standard Reports	ability to generate a report that displays the vaccine orders submitted to VTrck5 within a specific timeframe			E	Yes	The solution has robust filtering to allow for reports on vaccine orders including status (approved, created, submitted) create date, approve date, vaccine type, user with each field also easily being sortable.
		Standard Reports	ability to generate a report providing information about influenza pre-book orders			E	Yes	The solution has robust filtering to allow for reports on vaccine orders including status (approved, created, submitted) create date, approve date, vaccine type, user with each field also easily being sortable. The solution also includes a dashboard providing facilities a view of their allocation, ordered and available.
		Standard Reports	ability to query vaccine ordering patterns over a selected timeframe to indicate trends			O	Yes	The vaccine dashboard provides graphs to show ordering trends over time for specific time intervals or other user-selected timelines.
		Standard Reports	ability to generate reports that provide information about organizations and facilities			O	Yes	The proposed solution can generate information about facility/organization hierarchy.
		Standard Reports	ability for jurisdictional admin to generate report that lists immunizing facilities			O	Yes	Authorized users can generate a report of facilities that are notated as immunization facilities.
		Standard Reports	ability for jurisdictional admin to generate a report that provides information on organizational/facility enrollment			O	Yes	Authorized Jurisdictional Administrators can filter, sort, and view enrollment status of one or many facilities using the facility explorer.
		Standard Reports	ability for jurisdictional admin to access utilization of report/usage statistics			O	Yes	The reporting component can be used to configure report/usage statistics and reporting. Gainwell has incorporated this functionality into the core Immunization Solution product.
		Standard Reports	ability to generate reports that provide information about students and their immunization histories for school compliance	Needed for school reports.		E	Yes	The solution enables authorized school and jurisdiction users to generate reports containing student immunization information to support school compliance activities. Reports include student listings, immunization histories, and students with immunizations due, helping users efficiently identify and manage compliance with jurisdictional school immunization requirements.
		Standard Reports	ability to generate report of student exemptions by type (medical, religious)	Needed for school reports.		E	Yes	The solution supports school and childcare compliance reporting by exemption type, including medical and religious exemptions. Exemption information can be captured and summarized by school, grade, childcare age group, and other applicable criteria to support jurisdictional monitoring and reporting requirements.
		Standard Reports	ability to generate a record of students' immunizations for school purposes	Needed for school reports.		E	Yes	The solution enables authorized users to generate a student immunization history record for school purposes, providing the student's associated immunizations in a readily accessible report to support verification of immunization status and school compliance.
		Standard Reports	ability to generate exclusion letters stating which vaccine(s) a student needs to come into compliance with requirements and be permitted to attend school	Needed for school reports.		E	Yes	The solution generates exclusion letters for students who are overdue or otherwise not compliant with applicable immunization requirements. Letters identify the vaccine(s) needed for the student to achieve compliance and can be generated directly through the school module to support timely communication with parents or guardians and the student's return to school in accordance with jurisdictional requirements.
		Standard Reports	ability to generate reports for individuals vaccinated during a mass vaccination event	Needed for mass vaccination.		E	Yes	Authorized users can generate reports of individuals vaccinated during a mass vaccination event.
		Standard Reports	ability to generate doses administered reports for priority groups during a public health emergency	Needed for mass vaccination.		E	Yes	Authorized users can generate a report of doses administered to patients belonging to a priority group as defined by the jurisdiction.
		Standard Reports	ability to generate a report that provides information about the status of the system in terms of total entities			E	Yes	The proposed solution can display the facilities and their active status.
		Ad Hoc Queries & Reports	ability to generate queries and reports based on user-defined parameters			E	Yes	The proposed solution can generate reports using user-defined criteria for custom reporting.
		Ad Hoc Queries & Reports	ability to schedule an ad hoc query to run on a predetermined interval (i.e., daily, weekly, monthly, quarterly or annual basis)			E	Yes	Reports can be scheduled to run on a specified cadence determined by the users.
		Ad Hoc Queries & Reports	ability to generate reports with a user-defined report format			E	Yes	Reports can be exported in multiple formats including CSV, XLSX, and PDF.
		Ad Hoc Queries & Reports	ability to generate reports across geographic hierarchy levels			E	Yes	Authorized users can generate reports across hierarchy levels.
		Ad Hoc Queries & Reports	ability to generate data to inform the public via website dashboards or similar means	Particularly relevant for mass vaccination.		E	Yes	Data can be exported and configured to generate data for public dashboards.
		Ad Hoc Queries & Reports	ability to store saved report templates			E	Yes	Authorized users can save an ad hoc query and queries can be configured per jurisdictional policies based on retention policies.
		Ad Hoc Queries & Reports	ability to modify saved report templates			E	Yes	The Solution has the ability to save an ad hoc query and can be configured per jurisdictional policies based on retention policies.
		Ad Hoc Queries & Reports	ability to Inactivate (archive) saved report templates			E	Yes	The Solution has the ability to save an ad hoc query and can be configured per jurisdictional policies based on retention policies.
		Ad Hoc Queries & Reports	ability to modify a query			E	Yes	Authorized users can modify a query.
		Ad Hoc Queries & Reports	ability to delete a query			E	Yes	Authorized users can delete a query.
		Ad Hoc Queries & Reports	ability to save an ad hoc query			E	Yes	The solution can save an ad hoc query and can be configured per jurisdictional policies based on retention policies.

Status	Req. #	Capability	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)
		Ad Hoc Queries & Reports	ability to create a map using geocodes for statistical reporting			O	Yes	The proposed Solution leverages the Federal Information Processing System (FIPS) codes for State and Counties. The FIPS codes are uniquely identified geographic areas. The solution produces a number of graph and map options at the State and County Level. The solution also leverages Smarty to store longitude and latitude which would allow for additional mapping of geographic regions as needed for reporting. The solution has the data visualization capability to produce a geographical map by county/region.
		Print/Export Reports	ability to export IIS data for use in other systems			E	Yes	The Immunization Solution proposed provides a user-friendly interface that assigns end users the appropriate role to export and print designated documents and reports.
		Print/Export Reports	ability to export data in user-defined formats			E	Yes	Data can be exported in formats including CSV, XLSX, and PDF.
		Print/Export Reports	ability to export aggregate level de-identified	Particularly relevant for mass vaccination.		E	Yes	The solution uses Privacy Protecting Record Linkage (PPRL) to share requested aggregate-level data with authorized entities.
		Print/Export Reports	ability to export record level de-identified data	Particularly relevant for mass vaccination.		E	Yes	The solution uses Privacy Protecting Record Linkage (PPRL) to share requested aggregate-level data with authorized entities.
		Print/Export Reports	ability to print reports			E	Yes	The solution can print and export reports.
		Consumer Access	ability for authorized consumers to access personal IIS data per jurisdictional policy			E	Yes	The solution provides a configurable Consumer Access module that enables authorized individuals to securely access their personal immunization information, or information for an associated dependent or guardian relationship, in accordance with jurisdictional policy. The jurisdiction controls whether the module is enabled and the applicable access requirements, allowing jurisdictions to align consumer access with its identity verification, privacy, consent, and data-release policies.
		Consumer Access	ability for authorized consumer to print forecast			O	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
		Consumer Access	ability for authorized consumer to print patient immunization record			E	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
		Consumer Access	ability for authorized consumer to print an official immunization history			E	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
		Consumer Access	ability for authorized consumer to retrieve a verifiable digital vaccine credential without assistance from IIS or immunization program staff	Particularly relevant for mass vaccination.		E	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
Updated		Consumer Access	ability for authorized consumer to view immunization forecast			E	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
Updated		Consumer Access	ability for authorized consumer to view patient information			E	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
Updated		Consumer Access	ability for authorized consumer to view patient immunization record			E	Yes	Authorized consumers can print and export their personal and/or family immunization records and forecasts through Docket.
		Consumer Access	ability for patient/patient representative to opt in for reminder/recall notifications			O	Yes	The solution allows the patient/patient representative, through HL7, to opt in to being included and receiving reminder recalls. The provider can also indicate a reminder/recall within the UI.
		Consumer Access	ability for patient/patient representative to opt out of reminder/recall notifications			O	Yes	The solution allows the patient/patient representative, through HL7, to opt out of being included and receiving reminder recalls. The provider can also indicate a reminder/recall within the UI.

Non-functional

Items in red indicate where a jurisdiction should include a measure/threshold that meets their needs.

[Return to Cover Page](#)

Status	Req. #	Attribute	Sub Characteristic	Requirement: The IIS must/should...	Comments	Reviewer notes	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
		Performance	Time Behavior	support a responsive user interface			E	Yes	Usability, accessibility, and responsiveness are at the forefront of Gainwell's user design. The UI is built for ease of use and responsiveness and is designed around specific user roles and functions. Gainwell's corporate User Interface and User Experience (UI/UX) design team promotes standards for web-based solutions that maximize usability and provide a simple, easy experience. These include providing a modern user interface (UI) that features adaptive web design so users can use different devices to connect with critical immunization information. We also offer a solution design that supports access by common internet browsers including Edge, Chrome, Firefox, and Safari. It also provides responsive web design to allow rendering and user access through mobile devices such as smartphones.
		Performance	Time Behavior	support application launch, i.e. time between user initiation and application start, in less than 10 seconds	Recommendation: 10 seconds		E	Yes	The Immunization Solution proposed is designed to perform in accordance with State and industry performance standards and allow application launch to occur within the mutually agreed performance time period of less than 8 seconds.
		Performance	Time Behavior	support response to a user navigation action (e.g., mouse movement, keypresses, navigation) in less than 1 second	Recommendation: 1 second		E	Yes	The proposed solution is designed to perform in accordance with State and industry performance standards and allow navigation via the user interface within the mutually agreed performance time period.
		Performance	Time Behavior	support response to process submitted information via direct data entry in less than 4 seconds	Recommendation: 4 seconds		E	Yes	The proposed solution is designed to perform in accordance with State and industry performance standards and allow data entry within the mutually agreed performance time period.
		Performance	Time Behavior	support generation of a standard, pre-configured report in less than 30 seconds	Recommendation: 30 seconds		E	Yes	Small reports are generated near-real time in the UI (i.e., cohort) large reports we kick off in the background so the user can use the system and return to the report once complete.
		Performance	Time Behavior	support responsive data exchange system interfaces			E	Yes	The proposed solution is designed to perform in accordance with State and industry performance standards for HL7 messaging. The solution also provides near-real-time dashboards displaying system response times of VXUs and QBP's.
		Performance	Time Behavior	support electronic response to a submitted HL7 message in 5 seconds or less, 95% of the time	Recommendation: 5 seconds or less, 95% of the time (AIRA Measurement and Improvement Initiative)		E	Yes	Gainwell's solution supports mandated throughput, usage, and capacity while maintaining processing speeds in accordance with jurisdiction performance standards.
		Performance	Capacity	support up to 1000 concurrent users of the user interface without performance degradation			E	Yes	The solution is designed to support 1,000 or more concurrent user interface sessions through a scalable cloud architecture that distributes workload and resources to maintain responsive system performance during periods of concurrent use.
		Performance	Capacity	support multiple users viewing the same data at the same time			E	Yes	The solution supports multiple authorized users simultaneously viewing the same patient, provider, inventory, reporting, or other system data without adversely affecting system availability or performance.
		Performance	Capacity	support users using the same function at the same time without degrading IIS performance			E	Yes	The solution supports multiple users performing the same system functions concurrently. The cloud-based architecture is designed to scale application resources based on workload demands to maintain reliable and responsive performance.
		Performance	Resource Utilization	support resource-intensive tasks without degrading IIS performance			E	Yes	The solution is architected to isolate and manage resource-intensive workloads so that activities such as reporting, data processing, interfaces, and scheduled jobs can operate without adversely affecting routine IIS user functions.
		Performance	Resource Utilization	support user queries via the user interface without degrading IIS performance			E	Yes	The solution supports concurrent user searches and queries through the user interface while maintaining responsive application performance. Search and retrieval processes are optimized to efficiently access patient, provider, inventory, and other IIS data.
		Performance	Resource Utilization	support generation of ad hoc reports without degrading IIS performance			E	Yes	The solution supports generation of ad hoc reports while maintaining operational system performance. Reporting workflows are managed to minimize impact to transactional and other user-facing IIS functions.
		Performance	Resource Utilization	support data extracts without degrading IIS performance			E	Yes	The solution supports scheduled and on-demand data extracts using processing methods designed to minimize impacts to interactive application functions and other operational workloads.
		Performance	Capacity	support efficient processing of HL7 messages without performance degradation, as per jurisdictional capacity needs			E	Yes	The solution efficiently processes high-volume HL7 transactions and is designed to scale processing capacity based on jurisdictional exchange volumes. The cloud-based architecture supports both routine transaction volumes and significant increases in inbound and outbound messaging associated with public health events and other surge conditions.
		Performance	Capacity	support processing of up to 200 of HL7 VXU messages per hour without performance degradation			E	Yes	The solution supports processing of at least 200 HL7 VXU immunization update messages per hour and is architected to support substantially higher transaction volumes based on jurisdictional capacity and performance requirements.
		Performance	Capacity	support processing of up to 8000 of HL7 QBP messages per hour without performance degradation			E	Yes	The solution supports processing of at least 8,000 HL7 QBP query messages per hour and is designed to scale to accommodate jurisdictional query volumes while maintaining reliable response and overall IIS performance.
		Performance	Capacity	support permanent storage of records as per jurisdictional policy			E	Yes	Gainwell will comply with State record retention policies.
		Performance	Capacity	support storage of unlimited number of organization records			E	Yes	Yes, this system has no limit on the number of records; additional storage may apply at extra cost if sizes expand beyond the expected amount.
		Performance	Capacity	support storage of unlimited number of user records			E	Yes	Yes, this system has no limit on the number of records; additional storage may apply at extra cost if sizes expand beyond the expected amount.
		Performance	Capacity	support storage of unlimited number of patient records			E	Yes	Yes, this system has no limit on the number of records; additional storage may apply at extra cost if sizes expand beyond the expected amount.
		Performance	Capacity	support storage of unlimited number of patient immunization records			E	Yes	Yes, this system has no limit on the number of records; additional storage may apply at extra cost if sizes expand beyond the expected amount.
		Usability	Accessibility	meet the United States Access Board Section 508 Standards			E	Yes	The Gainwell UI/UX Team's standard and centralized processes that will be applied for Gainwell's Immunization Solution include ADA/508/Web Content Accessibility Guidelines (WCAG) oversight and testing to maximize accessibility as well as mobile compatibility testing.
		Usability	Operability	support best practices for web application session management (e.g., cookies, cache) as recommended by the Open Web Application Security Project (OWASP)			E	Yes	The proposed solution supports best practices per the OWASP Web Security Testing guide.
		Usability	Operability	ability to execute Boolean searches			E	Yes	The search capability considers multiple fields for finding patients (Firstname, Lastname).
		Usability	Operability	ability to execute a wildcard searches			E	Yes	The proposed solution allows for wildcard searches such as partial name search.
		Usability	User error protection	minimize data entry errors			E	Yes	The proposed solution is designed to be easy to use and intuitive. As described previously, Gainwell applies corporate UI/UX best practices to deliver the best possible user experience and minimize abrasion. Data entry through the UI is designed to be quick and easy. To prevent submission of erroneous or incomplete information, we apply standard and configurable rules-based edits. For example, Gainwell will work with the jurisdiction to determine the definition of "completeness" (required data elements) for a given record to configure business rules governing validation. Once these are configured, we employ rules-based validation and accept or reject records accordingly. Error messages are likewise simplified in the new solution. For example, in many legacy solutions, error messages are not table-driven and require a developer to make code changes to update error messages. In the solution, we follow a table-driven and configurable approach, enabling ultimate flexibility in updating message content to meet jurisdiction needs. This is just one example of how we improve the maintainability of Gainwell's Immunization Solution. Error messages are prominently displayed at the top of the screen so users can quickly pinpoint the error and make the necessary correction. Messages displayed to users are configurable.
		Usability	User error protection	assist in entering data correctly via pick-lists, drop-down boxes, or other easy-to-use options such as predictive text			E	Yes	The proposed solution incorporates features designed to make it easier for users to complete their tasks. These include the ability to select dates from calendars, use drop-downs and picklists, and other user-friendly options.
		Usability	User error protection	indicate required fields for data entry			E	Yes	The solution clearly identifies required data-entry fields within the user interface, including visual indicators and validation messaging, to guide users in completing required information before a transaction can be successfully submitted or saved.
		Usability	User error protection	ability to provide alert when required fields are left blank			E	Yes	As described above, if a user attempts to save or submit data without completing required information (denoted via an asterisk next to the field), the solution prominently displays an error message.
		Usability	User error protection	support cross-field checks to ensure accuracy of information where dependencies exist (e.g., warning that a child patient may be receiving an adult vaccine)			E	Yes	To prevent submission of erroneous or incomplete information, we apply standard and configurable rules-based edits. These configurable business rules include, for example, required data, age- or date-constrained data, data format (e.g., text or numeric), and other criteria.
		Usability	User error protection	support spell check functionality with medical terminology for all free text fields			O	Yes	The proposed Solution provides spell check capability incorporating medical terminology for editing of free-text fields. Gainwell has incorporated this functionality into the core Immunization Solution product.
Updated		Usability	User error protection	support differentiation between warning messages (network is recommended prior to entry being continued) and error messages (error must be fixed prior to continuing)			E	Yes	The user interface provides important messages to users to help them perform their tasks. Messages include but are not limited to banner messages, alerts/warnings, and errors. The solution supports Americans with Disabilities Act (ADA)-compliant pop-ups. Pop-ups increase ease of use, as solution users can update data using wizard-like screen pop-ups and menus. For example, when a Provider is adding or updating patient information, a pop-up notifies or warns the user and/or allows the Provider to update specific portions of the information in a quick and easy format. This includes error messaging, described above, as well as warning messages.
		Usability	User interface	support alerts related to user interface response time			O	Yes	The proposed Solution supports monitoring of page response time and provides alerts on responsiveness.

Non-functional

Items in red indicate where a jurisdiction should include a measure/threshold that meets their needs.

[Return to Cover Page](#)

Status	Req. #	Attribute	Sub Characteristic	Requirement: The IIS must/should	Comments	Reviewer notes	Priority: E, O (essential, optional)	Vendor response: "Yes, Yes with customization", No "Comment required"	Vendor comment(s)
		Usability	User interface	support user feedback with a simple indicator for response times between 2-4 seconds	Recommendation: 2-4 seconds		O	Yes	The proposed solution provides a progress indicator if information is not provided back immediately.
		Usability	User interface	support user feedback with expected response time and percent-done indicator for response times greater than 4 seconds	Recommendation: 4 seconds		O	Yes	The proposed solution supports user feedback of anticipated time to completion.
		Usability	User interface	support users in stopping an operation expected to take longer than 10 seconds	Recommendation: 10 seconds		O	Yes	The proposed solution allows for a pause and restart of jobs at the user's discretion.
		Usability	User interface	support users in performing other tasks while waiting for the system to complete tasks expected to take longer than 10 seconds	Recommendation: 10 seconds		O	Yes	The proposed solution allows for report generation to be independent to allow for other tasks to be performed.
		Reliability	Availability	support availability of the system as per jurisdictional needs			E	Yes	The proposed solution infrastructure is designed to conform to jurisdiction and industry performance standards.
		Reliability	Availability	support access to the web application 99.9% of the time	Recommend 99.9%		E	Yes	Gainwell's SaaS solution supports 99.9% availability. The solution crosses two AWS Availability Zones (AZ) for maximum availability.
		Reliability	Availability	support processing of and response to HL7 messages 99.9% of the time	Recommend 99.9%		E	Yes	Gainwell's SaaS solution supports 99.9% availability. The solution crosses two AWS Availability Zones (AZ) for maximum availability.
		Reliability	Recoverability	ability to backup the IIS data as per jurisdictional policy			E	Yes	Gainwell's SaaS solution uses AWS Backup, which adheres to the jurisdiction's backup policy.
		Reliability	Recoverability	support redundancy of the IIS as per jurisdictional recovery plan			E	Yes	Gainwell's SaaS solution supports 99.9% availability. We have configured the solution to cross multiple AZs to provide the required redundancy.
		Reliability	Recoverability	support real-time failover			E	Yes	Gainwell's SaaS solution supports 99.9% availability. We have configured the solution to cross multiple AZs to provide the required redundancy.
		Reliability	Recoverability	support the recovery of backed up data as needed			E	Yes	Backup and redundancy processes and procedures will be coordinated between Gainwell and the jurisdiction.
		Reliability	Recoverability	support the restoration of IIS data after an outage or loss			E	Yes	Gainwell's SaaS solution uses an operations team that restores data as needed from the AWS Backup that is taken on a scheduled basis.
		Reliability	Fault tolerance	support the efficient roll back of software changes as needed			E	Yes	Gainwell's SaaS solution uses an operations team that restores data as needed from the AWS Backup that is taken on a scheduled basis.
		Security	Non-repudiation	support audit logs for security purposes			E	Yes	The proposed solution provides comprehensive audit logging for system events (e.g., data access, data updates). Audit logging also occurs in the solution itself. Gainwell's backup and recovery processes include auditing logging at both the system level and the product level. Log files, audit trails, and logs of system access requests will be maintained in compliance with jurisdiction and CDC IIS Functional Specifications. Gainwell supports comprehensive audit logging in alignment with the Gainwell Access Control Standard (SPS-002), Logging and Monitoring Standard, and the Gainwell Information Security Policy.
		Security	Integrity	ability to electronically notify the system administrator of unauthorized activity			E	Yes	We harness the power of cutting-edge Identity and Access Management (IAM) tools to confirm the solution meets or exceeds the stringent security standards defined. The solution protects sensitive data, prevents unauthorized access, and maintains the system's integrity throughout its life cycle. The IAM tools and security policies work in harmony to enforce appropriate controls across various areas, including applications, networks, physical infrastructure, and end-user security for comprehensive protection. The integrity of the system and program functionality minimizes the risk of unauthorized access or compromise. The solution provides the ability for automatic notifications to the administrator when unauthorized activity is detected.
		Security	Authenticity	ability to track all attempted accesses that fail identification, authentication and authorization requirements			E	Yes	The proposed solution provides the ability to track access attempts, whether failed or successful, at the application level.
		Security	Authenticity	ability to track all accesses that successfully comply with identification, authentication and authorization requirements			E	Yes	The proposed solution provides the ability to track access attempts, whether failed or successful, at the application level.
		Security	Non-repudiation	ability to maintain audit logs for specified time per jurisdictional policy			E	Yes	The proposed solution captures and maintains system audit logs per jurisdictional policy for security analysis. Audit log retention periods are configurable to meet jurisdictional policy requirements and are managed in accordance with documented records retention schedules and security governance controls. Logs are retained for the specified timeframe, protected from unauthorized modification or deletion, and remain accessible for audit, investigation, and compliance purposes consistent with established retention and security standards.
		Security	Non-repudiation	ability for jurisdictional admin to search audit log by function performed			E	Yes	The read-only database will allow for authorized users to search audit log files by function performed.
		Security	Non-repudiation	ability for jurisdictional admin to search audit log by date and time period			E	Yes	The read-only database will allow for authorized users to search audit log files by date and time period.
		Security	Non-repudiation	ability for jurisdictional admin to search audit log by date range			E	Yes	The read-only database will allow for authorized users to search audit log files by date range.
		Security	Non-repudiation	ability for jurisdictional admin to search audit log by user-defined parameters			E	Yes	The read-only database will allow for authorized users to search audit log files by user-defined parameters.
		Security	Non-repudiation	ability for jurisdictional admin to search audit log by patient identifiers			E	Yes	The read-only database will allow for authorized users to search and filter audit log files by patient identifiers.
		Security	Non-repudiation	ability for jurisdictional admin to filter audit log search by user-defined parameters			O	Yes	The read-only database will allow for authorized users to filter audit log files by multiple user-defined parameters.
		Security	Non-repudiation	ability for jurisdictional admin to sort audit log search results			O	Yes	The read-only database will allow for authorized users to sort and filter audit log files.
		Security	Integrity	store audit data related to user access/viewing of patient records in the system			E	Yes	The proposed solution maintains a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an immunization solution record is created, viewed, or modified.
		Security	Integrity	store date of user access to a patient record			E	Yes	The proposed solution maintains a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an immunization solution record is created, viewed, or modified.
		Security	Integrity	store time of user access to a patient record			E	Yes	The proposed solution maintains a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an immunization solution record is created, viewed, or modified.
		Security	Integrity	store user ID of user access to a patient record			E	Yes	The proposed solution maintains a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an immunization solution record is created, viewed, or modified.
		Security	Non-repudiation	store audit data related to data changes in the system			E	Yes	The proposed solution maintains a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an immunization solution record is created, viewed, or modified.
		Security	Non-repudiation	store 'date received' for data modified in the system			E	Yes	The solution captures and retains the date information is received by the IIS, providing traceability of data submitted or modified through supported system processes and interfaces.
		Security	Non-repudiation	store 'time received' for data modified in the system			E	Yes	The solution captures and retains the time information is received by the IIS, supporting detailed transaction tracking, auditing, and troubleshooting.
		Security	Non-repudiation	store 'date updated' for data modified in the system			E	Yes	The solution captures and retains the date system information is updated, providing an auditable record of when changes are applied to data maintained within the IIS.
		Security	Non-repudiation	store 'time updated' for data modified in the system			E	Yes	The solution captures and retains the time system information is updated, providing detailed traceability of system changes and supporting audit and operational review.
		Security	Non-repudiation	store user associated with data modified in the system			E	Yes	The proposed solution maintains a log of changes to the system data, storing data including date, time, and the solution user or site taking the action, when individual-level data in an immunization solution record is created, viewed, or modified.
		Security	Integrity	automatically enforce session timeout for a user when idle period is reached			E	Yes	The proposed solution enforces a session timeout at 30 minutes with a countdown reminder that the session is expiring. This is configurable for the jurisdictional Administrator on what the allowable timeout session is.
		Security	Integrity	ability for automatic session timeout to be customized per jurisdictional policy			O	Yes	The proposed solution has a default 30-minute session timeout but allows for the jurisdiction to configure to meet jurisdictional policies.
		Security	Integrity	ability to notify the user the session will expire			O	Yes	The proposed solution has a default reminder that the user session will expire in 45 seconds and displays the countdown.

Non-functional

Items in red indicate where a jurisdiction should include a measure/threshold that meets their needs.

[Return to Cover Page](#)

Status	Req. #	Attribute	Sub Characteristic	Requirement: The ITS must/should...	Comments	Reviewer notes	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
		Security	Confidentiality	support masking of passwords as they are typed or entered into the user interface			E	Yes	The proposed Solution supports a password eyeglass that masks the password and but also allows for easy view.
		Security	Integrity	ability for system administrator to terminate user connections			E	Yes	The proposed solution allows for authorized users to terminate user connections.
		Security	Confidentiality	Safeguard electronic personally identifiable information by implementing the appropriate technical best practices	NIST Special Publications, Federal Information Processing Standards in the protection of PHI, the HIPAA Security Rule, and AURA's Security Guidance Considerations for IIS		E	Yes	Data is encrypted in transport and at rest.
		Security	Confidentiality	ability to encrypt personally identifiable information at rest			E	Yes	The solution provides encryption in transit with Transport Layer Security (TLS) across services.
		Security	Confidentiality	ability to decrypt personally identifiable information at rest			E	Yes	Gainwell's SaaS solution uses AWS Key Management Service (AWS KMS) to encrypt data at rest. Gainwell creates a unique key so only Gainwell can decrypt the information.
		Security	Confidentiality	ability to encrypt personally identifiable information during transmission			E	Yes	The solution provides automatic encryption of traffic on the AWS global and regional networks between AWS secured facilities.
		Security	Confidentiality	ability to decrypt personally identifiable information during transmission			E	Yes	The proposed solution uses HTTPS to secure PHI during transmission.
		Security	Integrity	ability to maintain firewalls per AURA's Security Guidance Considerations for Immunization Information Systems document			E	Yes	Gainwell maintains network security controls, including firewalls, in alignment with the Gainwell Information Security Policy, Network Security Standards, and applicable public health security guidance such as AURA's Security Guidance Considerations for Immunization Information Systems. Firewalls are implemented at network perimeters and between security zones to restrict inbound and outbound traffic based on defined security rules, least privilege principles, and approved communication pathways. Firewall configurations are documented, subject to formal change management, periodically reviewed for rule optimization, and monitored through centralized logging and intrusion detection processes to confirm compliance with regulatory, contractual, and established security governance standards.
		Security	Integrity	ability to maintain firewalls for protection of the hosting network			E	Yes	Gainwell maintains firewalls to protect the hosting network in alignment with the Gainwell Information Security Policy and Network Security Standards. Network firewalls are deployed at system perimeters and between security zones to control inbound and outbound traffic based on defined security rules, least privilege principles, and approved communication paths. Firewall configurations are documented, managed through formal change control processes, and subject to periodic rule review to confirm appropriate segmentation and traffic restriction. Firewall activity is logged and monitored through centralized security oversight processes to support threat detection, incident response, and compliance with established security governance standards.
		Security	Integrity	ability to maintain firewalls for protection of the hosting environment			E	Yes	Gainwell maintains firewalls for protection of the hosting environment in alignment with the Gainwell Information Security Policy and Network Security Standards. Firewalls and network security controls are implemented at the perimeter and between segmented security zones within the hosting environment to restrict traffic based on approved communication paths and least privilege principles. Firewall configurations are documented, managed through formal change control processes, periodically reviewed, and monitored through centralized logging and intrusion detection mechanisms to protect the confidentiality, integrity, and availability of hosted systems and data in accordance with established security governance standards.
		Security	Integrity	ability to electronically notify the system admin of unauthorized activity			E	Yes	Gainwell supports automated security event monitoring and alerting in alignment with the Gainwell Logging and Monitoring Standard and the Gainwell Information Security Policy. The system generates electronic notifications to designated system administrators when unauthorized or suspicious activity is detected, including failed authentication attempts, privilege escalation attempts, policy violations, or anomalous access behavior. Alerts are configurable based on defined security thresholds, are integrated with centralized monitoring processes, and support timely investigation and response in accordance with established incident response and security governance standards.
		Security	Integrity	ability to support anti-virus protection at current critical patch levels in the hosting environment			E	Yes	Gainwell supports anti-virus and endpoint protection controls within the hosting environment in alignment with the Gainwell Information Security Policy, Endpoint Protection Standards, and Threat and Vulnerability Management standards. Anti-malware solutions are deployed across applicable hosting infrastructure and are maintained at current critical patch and signature levels through automated update mechanisms and centralized management. Security agents and definition files are regularly updated, monitored, and validated to confirm protection against known threats, and related events are logged and reviewed as part of continuous security monitoring and governance processes.
		Maintainability	Analyzability	support event logging			E	Yes	The proposed solution supports application-level event logging.
		Maintainability	Analyzability	ability for system admin to enable event logging on all servers			O	Yes	This is included in the Application-Static Functionality; the system administrator can enable this.
		Maintainability	Analyzability	ability for system admin to enable event logging on all devices			O	Yes	This is included in the Application-Static Functionality; the system administrator can enable this.
		Maintainability	Analyzability	ability for system admin to disable event logging on all devices			O	Yes	This is included in the Application-Static Functionality; the system administrator can enable this.
		Maintainability	Analyzability	ability for system admin to limit access to event logs, including System, Application, Web and Database logs			O	Yes	This is included in the Application-Static Functionality; the system administrator can limit access to event logs, etc.
		Portability	Adaptability	support use of web browsers per jurisdictional policy			E	Yes	The proposed Solution is designed for use in a web browser. In addition, we developed the Solution using Responsive Web Design so that users can access the Solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support use of current version of web browsers			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support use of last prior version of web browsers			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support a responsive design that renders properly on multiple devices			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support web client use on a desktop			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support web client use on a laptop			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support web client use on a tablet			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Adaptability	support web client use on a smartphone			E	Yes	The proposed solution is designed for use in a web browser. In addition, we developed the solution using Responsive Web Design so users can access the solution through a browser-enabled device, including laptops, tablets, and smartphones.
		Portability	Installability	be containerized (e.g., Docker or Kubernetes) to support easy installation and system updates			E	No	The proposed solution supports containerization (e.g., Docker or Kubernetes); however, the Gainwell Immunization Solution is already designed to be easily and rapidly deployed and provide scalability.
		Portability	Installability	be containerized for cloud based environments			O	Yes	The proposed solution supports containerization (e.g., Docker or Kubernetes); however, the Gainwell Immunization Solution is already designed to be easily and rapidly deployed and provide scalability.

Glossary of Terms

[Return to Cover Page](#)

Terms and definitions used within requirements. Note: For definitions of general terms related to immunizations, see the [CDC Vaccines and Immunizations Glossary](#)

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)
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
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.

Glossary of Terms

[Return to Cover Page](#)

Terms and definitions used within requirements. Note: For definitions of general terms related to immunizations, see the [CDC Vaccines and Immunizations Glossary](#)

For definitions of general terms related to IIS, see the [AIRA MIROW Common Vocabulary resources](#).

Term	Definition
Jurisdictional vaccine program admin	Jurisdictional vaccine program staff authorized to enter and modify VFC- and vaccine program-related information in the IIS.
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
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,
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)	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 Children (VFC) program and the adult vaccine program).

Draft IIS Functional Standards, v5.0

			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	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	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.	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	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	
	4.0 The IIS validates patient demographic and vaccination data.	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			X	X	X	X		X							
	B. Continuously improve IIS data quality.	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.													X					
4.5 The IIS meets federal and jurisdictional data quality metrics.						X	X			X								
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	5.1 The IIS exchanges data in accordance with current interoperability standards endorsed by CDC for message content, format, and transport.				X	X				X	X	X	X			
		5.2 The IIS actively recruits, enrolls, and onboards IIS partners and providers for electronic data exchange.				X						X						
		5.3 The IIS actively monitors and evaluates data submitted via electronic data exchange.				X	X				X		X					
		5.4 The IIS investigates and resolves electronic data exchange errors and anomalies with IIS partners and providers.				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	6.1 The IIS establishes and maintains Clinical Decision Support (CDS) functionality consistent with ACIP recommendations.						X									
		6.2 The IIS establishes and maintains Clinical Decision Support functionality in alignment with CDSI resources published on the CDC website.						X										
7.0 The IIS ensures authorized users have access to patient demographic and vaccination data based on		7.1 The IIS implements confidentiality policies that protect the privacy of individuals whose data are contained in the system.	X	X	X				X		X		X		X			
E. Ensure appropriate user access to data.		7.2 The IIS implements comprehensive account management policies consistent with industry security standards.													X			
		7.3 The IIS supports technical attributes for the set up and access of user roles and permissions.	X	X	X													
		7.4 The IIS provides user access in accordance with policies and procedures.			X										X			
		7.5 The IIS supports authorized IIS partners' and providers' appropriate access to data in the IIS for public and population health purposes (e.g. childcare, schools, college, health plans, clinics).	X	X	X						X							
		7.6 The IIS provides training that covers accessing patient demographic and vaccination data.							X				X					
		7.7 The IIS identifies and inactivates user and site accounts when they are no longer active or no longer authorized to access the system.	X	X	X													
	8.0 The IIS supports authorized public access to official immunization records.	8.1 The IIS provides consumers with direct access to immunization records in accordance with policies and procedures.									X				X		X	
	9.0 The IIS supports the reporting needs of federal and jurisdictional immunization programs.	9.1 The IIS provides standard and ad hoc reports to meet federal and jurisdictional reporting requirements.									X							
	10.0 The IIS supports ad-hoc queries of patient demographic and vaccination data.	10.1 The IIS supports direct access for internal authorized users to IIS databases for data extracts and queries in accordance with policies and procedures.									X				X			
		10.2 The IIS supports access to data for data visualization, presentation, and analysis.									X				X			
F. Support the generation and use of IIS data through various channels and formats.	11.0 The IIS supports investigation and reporting of vaccine adverse events.	11.1 The IIS supports vaccine adverse event investigation.							X									
		11.2 The IIS refers users to appropriate resources to support adverse event documentation.							X									
	12.0 The IIS supports the ability to generate coverage reports that users can access without assistance	12.1 The IIS provides access to data to assess vaccination coverage and identify vulnerable populations.						X	X		X							
		12.2 The IIS manages patient status at provider site and jurisdiction levels.							X		X							

Draft IIS Functional Standards, v5.0

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
G. Support federal and jurisdictional vaccine program requirements.	13.0 The IIS supports reminder/recall activities.	12.3 The IIS provides IIS-related training on accessing, generating, and interpreting reports.									X						
		12.4 The IIS supports compliance with immunization requirements in childcare, school, and college settings.						X			X						
		13.1 The IIS supports conducting reminder/recall activities without assistance from IIS staff.						X	X								
	14.0 The IIS supports management and quality assurance functions for federal and jurisdictional vaccine	14.1 The IIS establishes vaccine program procedures in accordance to federal and jurisdictional policies.								X	X	X		X			
		14.2 The IIS supports the tracking of eligibility at the dose level for publicly purchased vaccine.								X							
		14.3 The IIS generates a report listing patients that received a non-viable vaccine.										X					
	15.0 The IIS supports vaccine inventory management and reconciliation according to federal and	14.4 The IIS generates a report listing provider sites that received vaccine lots recalled by the manufacturer.									X	X					
		15.1 The IIS supports vaccine inventory management, tracking, and reconciliation at the IIS jurisdiction and provider site levels.									X	X					
		15.2 The IIS supports creating vaccine orders and monitoring order status.									X	X					
	16.0 The IIS supports data exchange with the national Vaccine Tracking System (VTrckS).	15.3 The IIS supports reporting vaccine returns and wastage.									X	X					
		15.4 The IIS automatically decrements administered doses (not historical doses) from active inventory.									X	X					
		16.1 The IIS establishes data exchange with VTrckS in accordance with ExIS (External Information System) specifications.				X											
	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-	16.2 The IIS completes updates to ExIS functionality following publication of specifications.				X										
			16.3 The IIS establishes automated data exchange with VTrckS.				X										
			17.1 The IIS establishes, coordinates, and executes emergency preparedness plans and procedures in accordance with federal and jurisdictional policies.	X	X	X	X			X		X		X			
17.2 The IIS supports expedited communication and onboarding with partners to capture patient demographic and vaccination data in an emergency.		17.2 The IIS supports expedited communication and onboarding with partners to capture patient demographic and vaccination data in an emergency.	X	X	X									X			
		17.3 The IIS provides training to onboarded partners.		X													
		17.4 The IIS supports vaccine administration functionality to include offline documentation of vaccine administration.								X							X
17.6 The IIS supports public health immunization reporting to federal and jurisdictional authorities.		17.5 The IIS supports integration with tools for vaccination appointment scheduling.				X											
		17.6 The IIS supports public health immunization reporting to federal and jurisdictional authorities.										X					
		18.0 The IIS participates in modernization initiatives and emerging technologies.	18.1 The IIS coordinates modernization efforts.														
18.2 The IIS plans and executes efforts that align IIS initiatives with modernization priorities.																	X
18.3 The IIS participates in initiatives to develop standards and/or capabilities.																X	