Immunization Information System

Technical Proposal Response to CRFP MIS2700000001

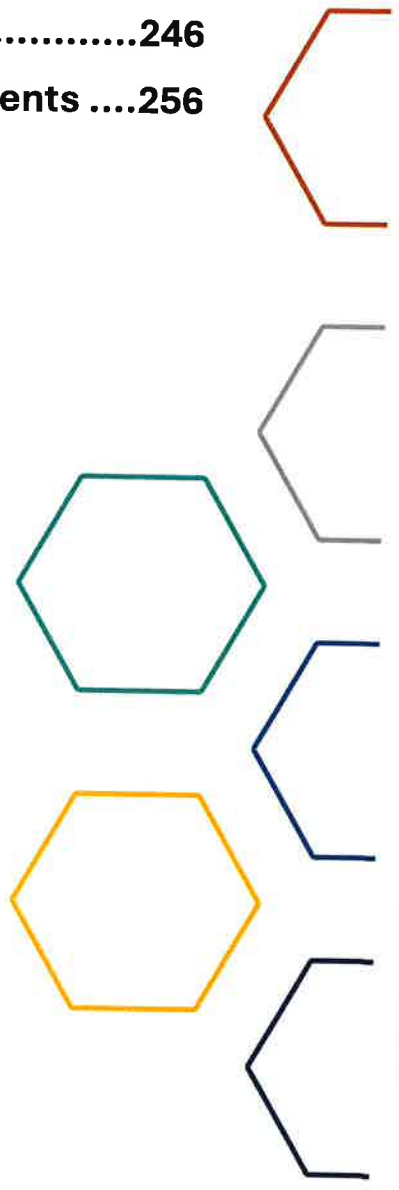
SUBMITTED TO:
Department of Administration,
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Crystal G. Hustead
crystal.g.hustead@wv.gov
(304) 558-2402

SUBMITTED BY:
Strategic Solutions Group, LLC (SSG)
1329 Highland Ave
Needham, MA 02492
www.ssg-llc.com

POINT OF CONTACT:
Ted Hill
VP, Sales and Marketing
thill@ssg-llc.com
(732) 299-7117

T Hill

Table of Contents



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) Ted Hill, VP Sales and Marketing

(Address) 1329 Highland Ave, Needham, MA 02492

(Phone Number) / (Fax Number) 732-299-7117 / 781-644-7460

(email address) thill@ssg-llc.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contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise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.

Strategic Solutions Group LLC
(Company)

Ted Hill
(Signature of Authorized Representative)

Ted Hill, VP Sales and Marketing 7/23/26
(Printed Name and Title of Authorized Representative) (Date)

(732) 299-7117 (781) 644-7460
(Phone Number) (Fax Number)

thill@ssg-llc.com
(Email Address)

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 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = 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.

Strategic Solutions Group LLC
(Company)

Ted Hill, VP Sales and Marketing
(Representative Name, Title)

(732) 299-7117 / (781) 644-7460
(Contact Phone/Fax Number)

7/23/26
(Date)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP 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)

- [x] Addendum No. 1
- [ ] Addendum No. 2
- [ ] Addendum No. 3
- [ ] Addendum No. 4
- [ ] Addendum No. 5
- [ ] Addendum No. 6
- [ ] Addendum No. 7
- [ ] Addendum No. 8
- [ ] Addendum No. 9
- [ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Strategic Solutions Group LLC
Company

Ted Hill
Authorized Signature

8/4/26
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

4.2 – Project Goals & Mandatory Requirements

West Virginia has identified the need for a modern, sustainable, and secure Immunization Information System (IIS) that supports statewide immunization management, aligns with CDC standards, and adapts to West Virginia's unique public health landscape. SSG fully understands these requirements and offers a solution that not only meets them today but positions West Virginia for long-term success.

At the center of our approach is *Casetivity*-IIS, a fully compliant SaaS platform designed specifically for public health immunization programs. Our approach combines proven technology, industry-leading interoperability, strong data stewardship, and a long-term partnership model that reduces implementation risk while providing a foundation for continuous improvement.

Unlike approaches that rely heavily on custom development or fragmented point solutions, SSG delivers an established, production-proven platform that is already supporting statewide immunization programs. This allows West Virginia to benefit from proven functionality, accelerated implementation timelines, more efficient long-term maintenance, and a future-ready solution that can evolve with changing public health needs.

SSG's implementation methodology emphasizes collaboration, transparency, and measurable outcomes. We work closely with agency critical partners, providers, and technical teams to configure *Casetivity*-IIS to support West Virginia's operational requirements, data exchange needs, reporting objectives, and public health goals. Because the platform is highly configurable, West Virginia can adapt workflows, business rules, forms, reports, and user experiences without introducing unnecessary complexity or technical debt.

What differentiates SSG is not only our technology, but our commitment as a long-term partner:

Compliance Guaranteed
Casetivity-IIS meets CDC HL7 v2.5.1 Message Mapping Guides (VXU, QBP, ACK, and ADT), CDC IIS Functional Standards, AIRA certification requirements, IZ Gateway participation requirements, and CDC Data Modernization Initiative objectives. SSG continuously monitors evolving national standards and incorporates required updates into the platform, ensuring West Virginia remains compliant.

Reliability Backed by Warranty

SSG stands behind every solution we deliver. Any defect in software delivered by SSG is corrected under SSG's lifetime warranty for the life of the project. This lifetime warranty demonstrates our confidence in the platform and our commitment to long-term client success.

High Performance Proven in Production

Casetivity-IIS is currently processing up to 5,000 HL7 VXU messages per hour and 25,000 HL7 QBP messages per hour in production statewide IIS environments. The platform's scalable cloud architecture supports high transaction volumes, rapid data exchange, and reliable system performance while maintaining data quality and availability.

Data Stewardship Commitment

West Virginia's data belongs to West Virginia. SSG does not use client IIS data for secondary, commercial, or non-authorized purposes. We view ourselves as stewards of public health information and are committed to ensuring that data remains secure, accessible, and under the control of the agency.

Security by Design

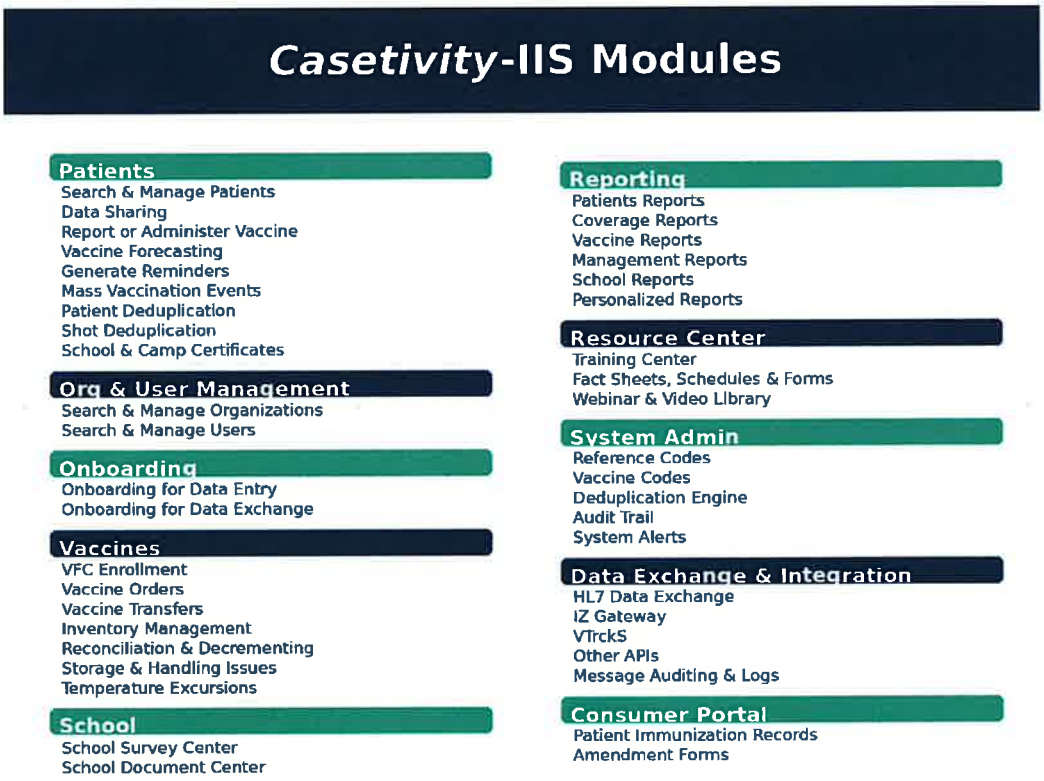
Security is embedded throughout the platform and development lifecycle. *Casetivity*-IIS incorporates secure software development practices, role-based access controls, encryption of data in transit and at rest, continuous monitoring, independent security assessments, and regular penetration testing. These safeguards help protect sensitive immunization information while supporting agency security requirements and operational continuity.

Future-Proof Sustainability

As a cloud-based SaaS solution, *Casetivity*-IIS eliminates the burden of maintaining infrastructure, applying patches, and managing software upgrades. West Virginia will benefit from regular platform enhancements, biannual releases, administrative configuration tools, and emerging capabilities such as *Casetivity* **Compass**, SSG's AI-enabled platform assistant. This approach ensures that the IIS continues to evolve alongside changing program requirements, technology advancements, and public health priorities.

Casetivity-IIS delivers comprehensive registry, inventory, interoperability, provider management, forecasting, analytics, reporting, and consumer engagement capabilities within a single integrated environment. By consolidating these functions into one platform, West Virginia gains a complete and accurate view of immunization activity across the state while reducing administrative burden and improving operational efficiency.

The following figure illustrates the major functional components of *Casetivity*-IIS and how they work together as a unified platform to support immunization program operations, interoperability, inventory management, clinical decision support, reporting, and public access.



A key advantage of SSG's approach is our commitment to standards-based interoperability. *Casetivity*-IIS facilitates seamless exchange of immunization information with healthcare providers, electronic health records, pharmacies, laboratories, public health systems, and federal partners. This improves data completeness, reduces manual data entry, increases provider participation, and enables more timely and informed public health decision-making.

Compared to alternative approaches that depend on extensive customization, legacy technologies, or multiple disconnected systems, SSG's approach provides lower implementation risk, faster time to value, more efficient long-term operations, and greater adaptability to future requirements. West Virginia will receive the benefits of a mature and proven platform while maintaining the flexibility necessary to support evolving immunization program needs.

SSG has successfully delivered every project we have undertaken, maintaining a 100% project success rate through disciplined project management, transparent communication, and a commitment to partnership. By delivering *Casetivity*-IIS, SSG will provide West Virginia with a

secure, reliable, and sustainable Immunization Information System that improves immunization tracking, enhances vaccination coverage, and supports data-driven public health decision-making for years to come.

4.2.1 CDC-Based Goals & Objectives

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.

SSG's *Casetivity*-IIS is physically and digitally secured in accordance with industry standards for protected health information, security, and encryption. The solution operates on a secure cloud-based infrastructure that complies with all relevant federal and state regulations, including HIPAA and CDC guidelines, ensuring the protection of sensitive health information. Security controls are embedded throughout the solution at the physical layer as well as numerous digital safeguards.

Physical Security
Regarding physical security, SSG's hosting environment and operational practices are aligned with industry-recognized security and compliance standards. SSG maintains a SOC 2 Type II audited environment, demonstrating adherence to established controls for security, availability, and confidentiality.

Regarding physical security of the hosting facilities, SSG utilizes industry standard hosting infrastructure for all environments. *Casetivity*-IIS is designed to be run within different hosting providers, but SSG's default provider is Amazon Web Services (AWS) as part of the SaaS offering. Physical access to data centers in AWS (US) is restricted to employees who have been validated as being US citizens. Access to data centers is regularly reviewed. Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Access to any off-site facilities (including storage) used to support the solution is restricted, and the State retains the right to perform physical security audits of both off-site and on-site facilities at the State's discretion.

From a firewall protection perspective, SSG utilizes industry standard measures to protect solutions including physical protection and firewall protection. These safeguards include

network firewalls and web application firewall capabilities used to create private networks, and control access to instances and applications. *Casetivity*-IIS cloud deployment implements many Virtualized Cloud Computing Platform (VCCP) Safeguards including private cloud hosting, data segregation, logical separation of services/hosts, IDS/IPS, firewalls, antivirus and malware protection, and regular security updates and patching of VM images. Within the hosting environment, SSG utilizes secure network protocols such as VPN and SSL/TLS to secure network communications. Furthermore, SSG's cloud hosting is single tenant, so no other customers will have access to the West Virginia environments.

Digital Security
Regarding digital security, *Casetivity*-IIS implements multiple safeguards at different levels of the technology stack.

For application level digital security, *Casetivity*-IIS has robust user authentication and data authorization capabilities consistent with industry security standards, including user account provisioning, single sign-on integration, and session expirations and timeouts. These technical attributes support the setup and access of user roles and permissions, ensuring appropriate access controls are maintained throughout the system.

Regarding the design architecture digital security *Casetivity*-IIS will be hosted in a secure cloud environment with layered controls that support access restriction, encryption, monitoring, logging, and secure administrative practices.

Monitoring
Casetivity-IIS has features to notify administrators of unauthorized activity and to control access. Thresholds can be set for automatic alerts and notifications to administrators based on customizable logic. From a monitoring perspective, the solution logs user views of patient records storing the date, time and user ID.

SSG performs continuous monitoring of *Casetivity*-IIS in accordance with NIST SP 800-137 (Information Security Continuous Monitoring – ISCM) to ensure ongoing visibility into system security posture, timely identification of risks, and effective response to security events. SSG's approach integrates automated monitoring, defined processes, and coordinated reporting to maintain compliance and support the State's risk management objectives.

SSG establishes a continuous monitoring strategy aligned with NIST guidance that defines monitoring objectives, roles and responsibilities, tools, metrics, and reporting processes. This strategy is integrated into system operations and aligned with the system's security categorization and control baseline.

Monitoring activities are designed to provide ongoing awareness of:

- Security control effectiveness
- System vulnerabilities and threats

- Configuration compliance
- User activity and access patterns

Casetivity-IIS leverages automated tools and services to continuously monitor system activity and security controls. This includes:

- Centralized logging of system events, user actions, and security-relevant activities
- Integration with Security Information and Event Management (SIEM) capabilities to support real-time monitoring and analysis
- Alerting mechanisms to notify appropriate personnel of potential security incidents or anomalies

All these safeguards combine to make *Casetivity*-IIS a highly secure solution. SSG built *Casetivity*-IIS from the ground up with public health security requirements in mind. It was built on a modern, inherently more secure, technology stack and done with a superior design that took effort to implement correctly but provides customers with peace of mind that other solutions cannot. *Casetivity*-IIS meets the requirement for physical and digital security in accordance with policies and industry standards for protected health information, security, and encryption, while maintaining documented and updated policies and procedures to manage IIS functions, capabilities, and attributes.

Future Proofing with Security Guarantee
Security protection is an ongoing effort. As part of our solution Guarantee, SSG guarantees that *Casetivity*-IIS will always be in full compliance with all security policies and procedures published by within HIPAA guidelines, CDC guidelines and the state of West Virginia guidelines.

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.

SSG establishes, documents, and updates policies and procedures to manage the collective functions, capabilities, and attributes of the IIS. The organization's breadth of team experience in IIS implementation and capabilities across practice areas support comprehensive policy development and maintenance. SSG provides ongoing training to ensure awareness of and promote adherence to policies and procedures, supporting successful adoption and utilization of the system across all user groups.

In partnership with the West Virginia IIS team will document and maintain policies and procedures for operating the IIS after the initial go-live. This would include:

- User account management policies that are consistent with industry security standards, including:
    - User account provisioning
    - client single sign-on integration

  - Session expirations and timeouts
  - Disabling users if not used within a specified period of days.
  - These technical attributes support the setup and access of user roles and permissions, ensuring appropriate access controls are maintained throughout the system.
- Bug triage and fixes
- Patching and hotfix deployment
- Release management
- Interface monitoring and management
- Identifying and managing change requests
- System performance monitoring and optimization
- Database management and maintenance
- Backup and Recovery Management
- Proactive System Improvement

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.

Casetivity-IIS utilizes a modern technology stack and fully cloud-enabled architecture. This industry standard technical infrastructure establishes and maintains secure technical infrastructure to capture, store, and process patient demographic and vaccination data.

Data Capture

Casetivity-IIS supports multiple pathways for secure data capture. Providers can submit patient demographic and vaccination data through a web-based user interface, automated system-to-system bi-directional HL7 messaging (VXU/QBP and ADT), and UI-based bulk upload via Excel templates. In all situations, regardless of the data capture approach, *Casetivity*-IIS utilizes a common REST API for data capture. This technical approach allows for common data security and easier ongoing maintenance due to code re-use. Other solutions on the market are legacy systems that were added to overtime as opposed to being built from the ground up with more modern technology, so they are a patchwork of historical code that makes ensuring security more difficult. Furthermore, all data capture is done over secured SSL channels, and the payload of the messages are encrypted in transit.

Data Storage

All data resides exclusively in data centers physically located in the continental United States, with no transmission, processing, or storage outside U.S. borders at any time. From a data

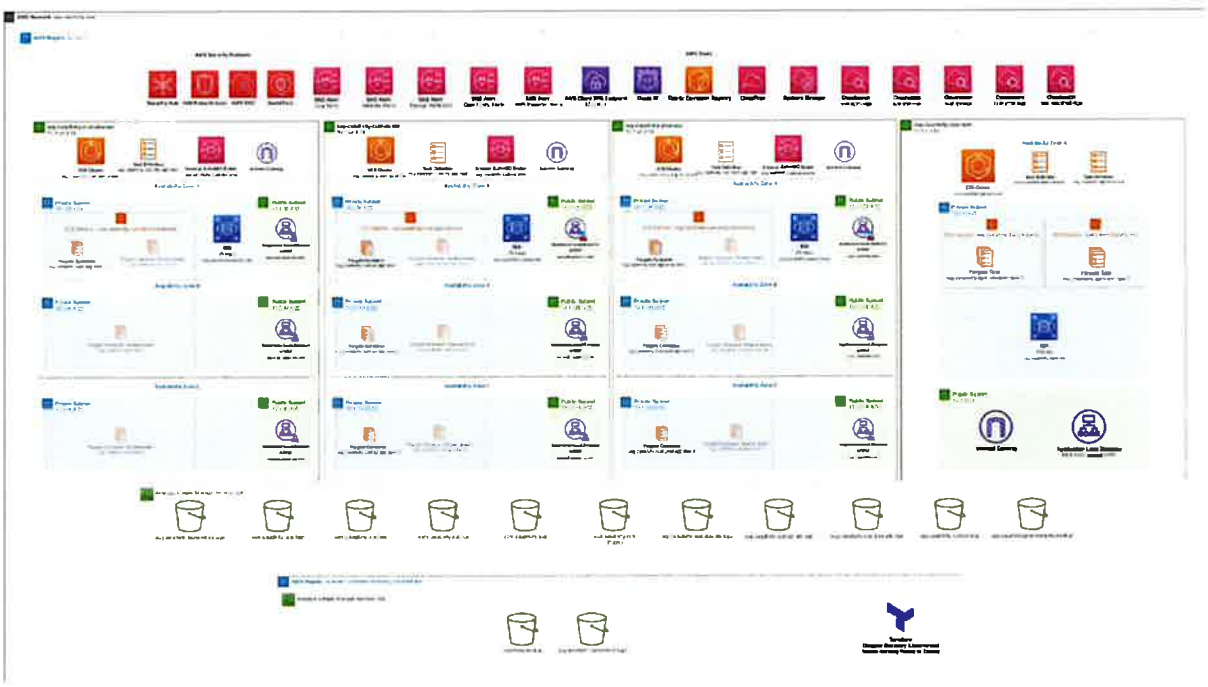
encryption perspective, *Casetivity*-IIS protects sensitive data through robust confidentiality controls, including encryption and decryption of data at rest, using FIPS 140-compliant encryption standards, including AES-256. All data at rest is stored in a database with encrypted disk drives using industry standard encryption services. Typically, Amazon's KMS encryption service is used and encrypted with AES-256 level encryption. Role-based access control (RBAC) ensures that users can only access information appropriate to their role and organizational affiliation. Data access is further restricted through configurable permissions at the module, record, and field levels.

Furthermore, SSG's cloud hosting is single tenant, so no other customers will share West Virginia's infrastructure. SSG feels this is a prudent safeguard to help ensure security of data storage.

Data Processing

To help ensure security of data processing, regardless of the data capture approach, *Casetivity*-IIS utilizes a common REST API and technical infrastructure for data processing. This architecture and infrastructure design allows the SSG DevOps team to closely monitor all processing within the application very easily to ensure proper security. Some legacy systems may have sprawling code that has evolved over time with many bolt-on features so securing data processing routines becomes more complicated. In addition, since *Casetivity*-IIS has all the necessary processing implemented within the solution already, sensitive data is never transmitted to any other environments or services for processing purposes. All processing is done within the secure *Casetivity*-IIS infrastructure.

The following is a typical infrastructure setup for *Casetivity-IIS* which ensures security as well as high performance and availability.



In Summary, *Casetivity*-IIS meets the requirement to establish and maintain technical infrastructure that securely captures, stores, and processes 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.

SSG provides comprehensive, ongoing training to ensure awareness of and promote adherence to policies and procedures through multiple integrated capabilities within *Casetivity*-IIS and direct support services, including ongoing training, help desk support and pro-active notifications.

Ongoing training resources are available for self-help through multiple integrated capabilities within *Casetivity-IIS*. The Resource Center Module serves as a centralized repository for training materials, policy documentation, and procedural guidance. This authorized users to access current training videos, user manuals, security policies, procedures, and training content on demand, supporting continuous awareness and adherence across all user groups.

In addition to these integrated ongoing learning opportunities, SSG makes available professional training team members on an ongoing basis to offer training programs as needed. These programs can be tailored for specific user groups, including internal staff, external partners, and newly onboarded organizations. The training methodology addresses multiple aspects of system established security protocols, generating and interpreting reports while maintaining data

confidentiality, and adhering to role-based access control requirements. SSG provides training provided to onboarded partners to ensure they understand and follow policies from the outset of their engagement with the system.

The platform supports role-based access control with configurable user roles and permissions, which reinforces security policy adherence by technically enforcing access restrictions aligned with organizational policies. This technical control complements training by ensuring users can only perform functions appropriate to their assigned roles, reducing the risk of inadvertent policy violations.

Another aspect of training is the continuous help desk and technical support that SSG provides. SSG team members are available to address security-related questions. This ongoing support model enables users to receive guidance when questions arise during daily operations, reinforcing training and promoting consistent adherence to security requirements.

Finally, SSG provides proactive training through notifications and announcements about evolving security threats and mitigation strategies. *Casetivity-IIS* undergoes regular updates to adapt to evolving security needs and regulatory requirements, including alignment with HIPAA, CDC guidelines, and other applicable federal and state regulations. When updates affect security policies or procedures, SSG ensures critical partners receive appropriate training and documentation to maintain awareness and compliance.

This multi-layered approach to ongoing training — combining accessible training resources, comprehensive training programs, technical enforcement through role-based access controls, continuous support, and regular updates — ensures ongoing awareness and promotes consistent adherence to security policies and procedures across the *Casetivity*-IIS environment.

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

SSG ensures that *Casetivity*-IIS is physically and digitally secured through a comprehensive disaster avoidance, mitigation, and recovery framework built on secure cloud infrastructure, redundant architecture, automated backups, continuous monitoring, and documented business continuity and disaster recovery processes. The solution is hosted within U.S.-based data centers and leverages virtualization, redundancy, and automated recovery capabilities to minimize service disruption and protect critical immunization data. SSG maintains and regularly tests Business Continuity and Disaster Recovery (BCP/DR) plans, conducts annual recovery exercises, validates recovery objectives, and continuously updates recovery procedures based

on testing results, operational experience, and evolving security requirements. This approach supports the high availability, resilience, and recoverability required for a mission-critical Immunization Information System.

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

SSG establishes and maintains disaster avoidance infrastructure through a comprehensive, multi-layered approach that prioritizes system availability, data protection, and operational continuity for the Immunization Information System (IIS).

Hosting Infrastructure and Architecture

SSG delivers *Casetivity*-IIS as a fully managed Software-as-a-Service (SaaS) solution, reducing the burden on jurisdictional IT resources and supporting efficient long-term operations. The hosting infrastructure is designed with disaster avoidance as a foundational principle, incorporating automated backup systems with multiple redundancy layers to ensure data integrity and availability. All IIS data—including backups, logs, and metadata—is stored exclusively within data centers physically located in the continental United States, with no data transmission, processing, or storage outside U.S. borders at any time, including during disaster recovery, failover, or support operations.

Virtualization and Rapid Recovery Capabilities

The infrastructure utilizes virtualization through virtual machines and containers to enable rapid system recovery and migration. This approach ensures the IIS can be quickly restored to a functional state in the event of an outage or disruption. SSG's recovery strategy prioritizes restoration activities based on assessed risks and operational impacts.

SSG's disaster recovery infrastructure utilizes cloud-based hosting in Amazon Web Services (AWS) with multiple redundancy layers and automated backup systems. The recovery strategy prioritizes restoration activities based on assessed risks and operational impacts, using data backups to restore systems while meeting defined Recovery Point Objectives (RPO), typically of one hour, and Recovery Time Objectives (RTO), typically of 24 hours. This approach minimizes data loss and ensures systems are operational as soon as possible but no later than 14 calendar days after a natural disaster. SSG employs virtualization through virtual machines and containers to enable rapid system recovery and migration, ensuring the IIS can be quickly restored to a functional state even in different physical locations.

Ongoing Infrastructure Management and Monitoring

As part of all SaaS projects, SSG provides infrastructure management, application monitoring, incident management, business continuity, and disaster recovery services. The infrastructure is continuously monitored to identify and address potential issues proactively. SSG employs robust data encryption protocols for data at rest and in transit to protect against unauthorized access during backup and recovery processes. Maintenance services include data back-up facilitation and system administration support, with detailed documentation of all disaster recovery activities, including backup schedules, recovery procedures, and test results.

This comprehensive disaster avoidance infrastructure enables SSG to maintain the high availability and reliability required for mission-critical immunization information systems, protecting public health data and ensuring uninterrupted service delivery to jurisdictions and their critical partners.

Casetivity-IIS was built for the cloud from the ground up. Other solutions on the market have been retrofitted and don't take advantage of what the cloud enables, which impacts costs and service levels.

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

SSG establishes and tests recovery plans to mitigate system downtime through a comprehensive Disaster Recovery (DR) and Business Continuity Plan (BCP) aligned with NIST SP 800-34 standards. The plans document specific recovery steps, order of recovery, and verification processes to ensure data integrity, availability, and recoverability in case of system failure or cyber incident.

Business Continuity and Disaster Recovery Planning

SSG maintains documented Business Continuity Plans and Disaster Recovery plans aligned with NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems) throughout the contract term. SSG provides these plans to the Agency within 60 calendar days of contract execution and upon request thereafter. SSG conducts annual BCP/DR testing through tabletop or live failover exercises and provides summary reports of results, corrective actions, and remediation timelines within 30 calendar days of test completion. All BCP/DR activities, including backups, failover, and recovery operations, comply with U.S.-based data residency requirements.

Compliance and Continuous Improvement

SSG updates BCP/DR plans within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment. SSG annually certifies to the Agency that BCP/DR plans remain current, tested, and compliant with federal and state requirements. This commitment to continuous improvement ensures the disaster avoidance infrastructure evolves with emerging threats and operational requirements while maintaining compliance with relevant federal, state, and industry standards for disaster recovery and data protection.

SSG conducts rigorous testing to validate recovery plan effectiveness. The testing program includes one disaster recovery test prior to statewide implementation and annual business continuity and disaster recovery tests thereafter. Testing activities include both tabletop exercises and live failover simulations to ensure ongoing readiness. SSG participates in post-testing activities to certify achievement of RTO and RPO objectives and ensure disaster recovery system readiness. The organization assists with resolving any recovery issues identified during testing and incorporates feedback from tests and real-world incidents to continuously refine disaster recovery strategies.

All disaster recovery activities comply with U.S.-based data residency requirements, with backups, failover operations, and recovery procedures conducted exclusively within data centers physically located in the continental United States. SSG provides copies of BCP and DR plans to the Agency within 60 calendar days of contract execution and upon request thereafter. Plans are updated within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment. SSG provides summary reports of test results, corrective actions, and remediation timelines within 30 calendar days of test completion and annually certifies that plans remain current, tested, and compliant with federal and state requirements.

SSG maintains detailed documentation of all disaster recovery activities, including backup schedules, recovery procedures, and test results, ensuring compliance with relevant federal, state, and industry standards for disaster recovery and data protection. This comprehensive approach ensures the IIS establishes and tests recovery plans that effectively 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.

SSG defines and maintains clear service expectations through formal Service Level Agreements (SLAs) governing system availability, performance, data recovery, maintenance, and support services. These SLAs establish measurable expectations between the IIS program and the entities responsible for hosting, operating, and supporting the solution, helping ensure uninterrupted data exchange and reliable system operations. To fulfill these commitments, *Casetivity*-IIS utilizes a cloud-native, single-tenant architecture with redundant infrastructure, automated failover, proactive monitoring, self-healing capabilities, horizontal scalability, and zero-downtime deployment processes. Combined with SSG's SLA Guarantee and dedicated support services, this approach provides the reliability, availability, and operational continuity required for a mission-critical Immunization Information System.

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

SSG offers an industry leading SLA Guarantee. Having served public health for 23 years and with our dedication to public health, we guarantee that *Casetivity*-IIS will meet all the SLA requirements of West Virginia. SSG implements service-level agreements (SLAs) with immunization programs to ensure Service Levels custom-tailored to meet the needs of West Virginia. This Service Level Guarantee applies to the solution as well as our ancillary services such as Help Desk.

SSG monitors performance against established SLAs and maintains accountability for meeting the applicable service-level requirements. The SSG SLA Guarantee includes the following:

- *Solution Performance SLA.* SSG guarantees that *Casetivity*-IIS will meet all performance requirements of West Virginia, including during spikes in end user activity.
- *Solution Availability SLA.* SSG guarantees that *Casetivity*-IIS will meet all the availability requirements of West Virginia.
- *Solution Data Recovery SLA.* SSG guarantees that *Casetivity*-IIS will meet all the data recovery requirements of West Virginia.
- *Warranty SLA.* SSG will address defects in *Casetivity*-IIS in accordance with the applicable warranty and SLA requirements.
- *Help Desk SLA.* SSG guarantees we will meet the Help Desk SLA requirements pertaining to our SaaS offering.

SSG is dedicated to public health over the long term. This is reflected in our industry leading SSG Guarantee Program.

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

Casetivity-IIS is a modern technology stack that is designed in a cloud enable way which allows us to efficiently fulfill service-level agreements. More specifically, the following are specific infrastructure and design elements that enable our strong SLA's:

1. *Zero-downtime Patches and Upgrades.* West Virginia will not need to worry about coordinating solution downtimes since SSG and the technology of *Casetivity*-IIS supports zero downtime.
2. *Redundant Infrastructure with Automatic Failover.* The solution utilizes redundant infrastructure, load balancing, and automated failover capabilities to minimize downtime and maintain continuous system access.
3. *Cloud enabled Self-healing and Horizontal Scaling. Casetivity*-IIS was built for the cloud from the ground up. Other solutions on the market have been retrofitted and don't take advantage of what the cloud enables, such as auto-healing, auto horizontal scaling for performance and zero downtime deployments. We can provide superior features at less cost since we were engineered for the cloud.
4. *Single Tenant.* utilizing single-tenant cloud architecture that ensures dedicated resources, superior scalability, and reliable performance for the Immunization Information System (IIS). *Casetivity*-IIS operates on a single-tenant hosting topology within a cloud-enabled infrastructure. This architecture provides each jurisdiction with dedicated system resources rather than shared multi-tenant environments. The single-tenant model delivers superior scalability to accommodate usage bursts—particularly critical during mass vaccination campaigns or public health emergencies—while maintaining consistent performance and data isolation. This modern cloud-enabled design ensures the system can scale dynamically to meet demand without resource contention or performance degradation that can occur in shared hosting environments.
5. *Continuous and Proactive Monitoring.* The hosting environment supports system performance monitoring and proactive issue resolution for all managed components

This infrastructure approach fulfills the requirement to implement and maintain hosting infrastructure that supports service-level agreement commitments while providing the scalability, reliability, and performance necessary for mission-critical immunization information management. This combination of cloud scalability, single-tenant infrastructure, formal SLA governance, and comprehensive support services ensures that *Casetivity*-IIS meets the

requirement for implementing and maintaining service-level agreements between the program and IT support entities.

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.

Casetivity-IIS validates patient demographic and vaccination data through a comprehensive data quality framework that combines real-time validation, configurable business rules, duplicate detection and resolution, address standardization, provider feedback mechanisms, and ongoing data quality monitoring. The solution supports jurisdiction-specific policies through configurable validation rules, automated data quality reporting, electronic address verification, and advanced deduplication capabilities while providing training and feedback tools that help providers maintain complete, timely, and accurate immunization records. This integrated approach enables jurisdictions to meet federal and state data quality requirements while ensuring the integrity, accuracy, and usability of IIS 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.

Casetivity-IIS supports the identification, prevention, and resolution of duplicate and fragmented patient demographic and vaccination data through a comprehensive deduplication framework that combines automated detection, configurable business rules, and user-driven review workflows. The approach integrates real-time processing at the point of data submission with systematic deduplication logic in the database to ensure data quality and patient record integrity. These processes apply to both patient data and vaccination data.

Real-Time Deduplication at Submission
Casetivity-IIS prevents duplicate vaccination events at the immunization level through real-time matching logic and background validation. The system evaluates incoming vaccination data against existing records using configurable business rules that jurisdictional administrators can adjust to align with state-specific policies and procedures. This proactive approach stops duplicates before they are committed to the system, reducing the need for retrospective cleanup.

At the time of data submission—via HL7 messages (VXU, ADT), manual entry, or API—*Casetivity*-IIS triggers a real-time deduplication algorithm to assess whether the incoming record matches an existing patient profile. Key Steps include:

- *Data Cleansing and Normalization:* Inputs such as names, birth dates, and addresses are standardized (e.g., via Smarty Streets for address validation).
- *Matching Algorithm Execution:* A combination of rules-based logic and a neural network–based engine evaluates potential matches.
- *Immediate Merging or Flagging:* If a confident match is identified, the solution can automatically merge the records. If the match falls into an indeterminate zone, it is flagged for manual review by authorized users.

Furthermore, the solution automatically identifies potential duplicate vaccination records based on key triggering events, including patient record save or update actions (covering both demographics and vaccination data) and patient deduplication and merge actions. This automated detection process applies consistently across all data input sources—user interface entry, HL7 messaging, and roster uploads—ensuring that potential duplicates are flagged regardless of how data enters the system.

Configurable Matching Logic and Thresholds to Ensure Policy and Procedure Alignment
Jurisdictional administrators configure the deduplication framework to reflect state-specific policies and procedures. Administrators can adjust data quality business rules, set validation levels (Error, Warning, or Informational), and create or update data quality reports that monitor deduplication effectiveness. This configurability ensures that the system operates in accordance with established jurisdictional requirements while maintaining the flexibility to adapt as policies evolve.

More specifically, Administrators can configure the deduplication logic to suit jurisdictional needs, including:

- *Fields Compared:* Name, DOB, SSN, MRN, address, phone number, etc.
- *Match Thresholds:* Define confidence scores for auto-merge, manual review, or no-match.
- *Merge Logic:* Define how each field should be treated during a merge (e.g., which source to prioritize).

Advanced Neural Network Engine: Specifically for person matching, *Casetivity*-IIS includes an advanced proprietary machine learning engine that enhances match accuracy by recognizing phonetic similarities, transpositions, and common data entry errors.

Manual Review and Resolution Interface
When a patient match is uncertain, *Casetivity*-IIS flags the record pair as potential duplicates for review. End users access a dedicated deduplication queue or initiate the resolution process directly from a patient record. The system provides a three-column review interface that

displays the two original records alongside a solution-generated proposed merge. This side-by-side comparison enables users to evaluate potential duplicate vaccination events and make informed decisions about whether records should be merged or flagged as non-matches. The interface supports both patient-level and vaccination event-level deduplication, ensuring consistency across the entire record.

- *Three-Column Review Interface:* The interface shows both original records side-by-side, along with a third column showing the solution's proposed merged record.
- *Editable Merge Suggestion:* Users can override merge field selections before confirming.
- *Post-Decision Outcomes:*
    - Merged records are consolidated using user selections.
    - "Not a match" flags ensure the same pair won't be presented again.
    - Every action is logged in the audit trail, maintaining a full history of decisions.

Access to the deduplication queues is configurable based on user roles and organizational context. Jurisdictions can choose to restrict access to a limited set of authorized users at the state level, or delegate deduplication responsibilities to designated users within provider organizations. In the latter case, organization-level users will only see potential duplicates involving patients that they have access to.

- *Record Splitting:* If a record has been incorrectly merged, the solution provides a tool to split it back into separate profiles and mark them as non-matching to prevent future auto-merges.

Background Deduplication in the Database

Beyond real-time deduplication, the solution runs scheduled or on-demand scans of the database to:

- Identify existing duplicates in the solution.
- Apply updated logic if the configuration has changed.
- Every deduplication action—automatic or manual—is logged in an audit trail including user ID, timestamp, action type, and before/after values, ensuring full transparency and accountability.

Support for Broader Entity Deduplication

Accurate, de-duplicated data is essential to effective public health operations, particularly in environments where information flows in from multiple systems and contributors. *Casetivity*-IIS was designed from the ground up to treat deduplication as a core solution function—not just for patients, but for any entity managed within the registry.

The solution supports configurable deduplication for organizations, facilities, vaccination events, and any custom entities defined by the jurisdiction. Each entity type can have its own matching rules, scoring thresholds, and merge behavior, allowing public health programs to tailor deduplication to their specific data landscape. This flexibility is especially valuable when cleaning up legacy data or managing ongoing data quality across interconnected systems.

Interoperability

Casetivity-IIS is designed with interoperability in mind, allowing jurisdictions to enhance deduplication and data quality efforts by integrating external tools and services where needed. For example, the solution supports real-time address cleansing using third-party services like Smarty to improve match accuracy and standardize incoming data.

In environments where broader identity resolution is required, the solution's architecture allows for integration with external Master Patient Index (MPI) or Master Data Management (MDM) systems. When configured, incoming records can be routed through these external services prior to local processing, and *Casetivity*-IIS can incorporate externally assigned identifiers or confidence scores into its own matching logic. While these integrations are not part of the default deployment, the solution's flexibility makes them feasible where appropriate.

Advanced AI-Driven Insights and Optimization

Casetivity-IIS includes a proprietary neural network–based matching engine designed to enhance accuracy and adaptability in identifying potential duplicates. Unlike static rules-based systems, this AI-driven engine uses a training-based architecture to recognize subtle data entry variations—such as phonetically similar names, transposed fields, or incomplete demographic data—that often cause issues in public health datasets.

SSG has already used this engine to evaluate and improve external deduplication logic, such as the AIRA algorithm currently used by the Commonwealth of Massachusetts, helping identify edge cases and improve overall match quality.

Importantly, *Casetivity*-IIS's comprehensive audit history captures every deduplication decision—manual or automatic—along with associated match scores, field-level changes, and user actions. While this audit trail ensures full transparency and traceability, it also provides a valuable foundation for jurisdictions that wish to further optimize matching performance over time. For those interested, SSG offers the option to collaborate on fine-tuning the neural network based on actual decision patterns and the nuanced data characteristics observed within their jurisdiction, allowing the deduplication engine to adapt to real-world conditions and improve over time.

Casetivity-IIS meets the requirement by delivering a complete deduplication framework that identifies, prevents, and resolves duplicate and fragmented patient demographic and vaccination data through automated processes, configurable rules, and user-driven workflows aligned with jurisdictional policies and procedures.

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

Casetivity-IIS monitors data quality within the system through a comprehensive framework of pre-defined reports, configurable business rules, and validation controls that align with jurisdictional policies and procedures.

The system includes built-in data quality reports that provide jurisdictional administrators with visibility into data completeness, accuracy, and consistency across patient demographic and vaccination records. Administrators can configure which data elements are monitored and set target thresholds at the organization level, enabling tailored quality standards that reflect jurisdictional requirements and program priorities.

Casetivity-IIS provides jurisdictional administrators with the ability to adjust data quality business rules for both HL7 message validation and user interface data entry. Administrators can classify validation rules as Error, Warning, or Informational levels, allowing the jurisdiction to balance data quality enforcement with system usability and external partner adoption. This flexibility ensures that validation rules support data integrity without creating barriers to participation by healthcare providers and other data exchange partners.

Administrators can create new data quality reports or modify existing ones to address evolving monitoring needs. The system's configurable approach allows jurisdictions to fine-tune validation options to satisfy specific requirements as they are confirmed during implementation and ongoing operations.

This approach supports continuous data quality improvement by providing the tools, visibility, and control necessary to monitor compliance with jurisdictional policies and procedures while maintaining practical workflows for end users and data exchange partners.

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

Casetivity-IIS uses electronic tools to standardize and validate addresses through third-party API integrations that support address standardization, verification, and geocoding capabilities. The solution integrates with services such as Smarty (formerly SmartyStreets) to ensure addresses conform to United States Postal Service (USPS) conventions and codes. This integration operates in real-time during data entry and HL7 message processing, enabling immediate address validation and cleansing as information enters the system.

The address validation capability verifies that addresses are valid USPS addresses through electronic means. When users enter or update address information, the system queries the integrated address service to confirm validity, standardize formatting, and correct errors. This

validation occurs automatically during both manual data entry and electronic data exchange, ensuring consistent address quality across all data sources.

The geocoding functionality enriches address records with geolocation data, enabling the system to assign latitude and longitude coordinates to validated addresses. These geocodes support jurisdictional assignment logic, deduplication processes, and statistical reporting. The system can create maps using geocodes for geographic analysis and coverage reporting, allowing public health staff to visualize immunization data by location and identify geographic gaps in service delivery.

The address standardization and validation tools can be configured to cleanse addresses on multiple entity types, including patient records and provider organizations. Jurisdictional administrators control how address validation rules apply across the system, balancing data quality requirements with operational workflow needs. While the system architecture supports integration with Smarty or other address standardization providers, third-party address usage and licensing services are separate from core platform licensing.

These electronic address tools reduce manual data entry errors, improve record matching and deduplication accuracy, support accurate jurisdictional reporting, and enable geographic analysis of immunization coverage. The integration ensures that address data meets federal and jurisdictional data quality standards while minimizing administrative burden on end users.

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.

Casetivity-IIS delivers comprehensive feedback and training to immunization partners and providers through multiple integrated mechanisms that ensure complete, timely, and accurate patient demographic and vaccination records. The solution supports formal training programs, inline user interface resources, customizable error messaging, structured onboarding workflows, and dedicated help desk capabilities—all designed to promote data quality and provider readiness across the immunization ecosystem.

Formal Training and Learning Management: Casetivity-IIS includes a robust training and resource center that houses technical resources, release notes, user guides, provider support materials such as fact sheets and posters, and links to immunization schedules and Vaccine Information Statements (VIS). The training center pages and content are highly customizable to meet jurisdictional branding and content requirements. The solution supports a VFC Training Workflow that includes a task-based process to validate training completion through video modules and testing. Dashboard views and reports monitor training compliance across provider

organizations. The system tracks both in-person training participation and digital module completion, generating reports and certificates of completion to document provider readiness.

Inline UI-Based Training Resources: The solution embeds training resources directly within the user interface, providing contextual guidance where providers need it during their workflow. This inline support reduces the learning curve and reinforces best practices at the point of data entry, helping providers understand requirements as they work within the system.

Customizable Error Messages and Data Quality Feedback: Casetivity-IIS delivers real-time feedback through easily customizable error messages that guide end users toward complete and accurate data submission. The solution employs both hard stops that prevent storage of non-compliant data and soft validations (warnings) that encourage complete, high-quality submissions without blocking workflow. HL7 Response Dashboards allow providers to view a history of validation errors, warnings, and informational messages, enabling them to monitor and improve their submission practices over time. Provider Scorecards and Data Quality Reports provide detailed assessments of each provider's data quality at rest, measuring accuracy, timeliness, and completeness. Invalid Dose and Timeliness Reports help providers identify and address submission anomalies proactively. These transparent feedback mechanisms promote accountability while empowering providers to improve data quality through self-service insight.

Onboarding Support and Tooling: The solution provides structured onboarding support and tooling to ensure new partners and providers are prepared to submit high-quality data from the start. SSG's onboarding workflows guide organizations through enrollment, training completion, and initial data submission, establishing a foundation for ongoing compliance and data quality.

Help Desk Support: SSG provides dedicated help desk support to assist partners and providers with technical questions, data quality issues, and system navigation. This support complements the self-service training and feedback tools, ensuring providers have access to expert assistance when needed.

Through this integrated approach—combining formal training programs, contextual UI resources, real-time validation feedback, structured onboarding, and responsive help desk support—*Casetivity*-IIS ensures immunization partners and providers have the knowledge, tools, and ongoing guidance necessary to maintain complete, timely, and accurate patient demographic and vaccination records throughout the State's immunization ecosystem.

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

Casetivity-IIS meets federal and jurisdictional data quality metrics through a combination of built-in validation tools, configurable business rules, comprehensive reporting, and a

collaborative governance approach that positions SSG as a long-term partner in data quality compliance.

The solution validates patient demographic and vaccination data through multiple mechanisms. Jurisdictional administrators can adjust data quality business rules for validations in HL7 and the user interface, including whether validations are classified as Error, Warning, or Informational levels. Administrators configure which data elements are monitored and set target thresholds for organizations. This flexibility allows jurisdictions to align validation rules with federal requirements and jurisdictional policies while balancing enforcement with external system adoption.

Casetivity-IIS includes pre-defined data quality reports that provide insight into how data quality and deduplication accuracy perform in practice. The Provider Scorecard highlights completeness and validity of key patient and immunization data. The HL7 Data Quality Report flags incomplete or corrected HL7 fields at submission time. The Warnings/Errors Report identifies patterns that may signal deduplication or data quality issues. HL7 message validation and correction summaries provide insights into data quality performance. These reports enable jurisdictions to monitor data at rest and submitted data against federal and jurisdictional metrics, identify areas requiring improvement, and track performance over time.

SSG's approach to partnering with jurisdictions on data quality compliance emphasizes shared accountability and transparency. The solution supports governance structures that fit each jurisdiction's operational model. Jurisdictions may establish internal data quality review groups or integrate deduplication review into broader public health governance efforts. SSG participates in joint working sessions, provides deduplication performance summaries, and assists with interpretation of trends. This collaborative approach ensures jurisdictions can make targeted changes to align with Departmental or CDC guidance without requiring code updates.

Jurisdictions can use nationally recognized test scenarios and tools, such as CDC patient matching test cases and AIRA's Aggregate Analysis Reporting Tool (AART), to validate deduplication logic and confirm that updates align with public health standards. These resources can be incorporated during onboarding, scheduled quality reviews, or in response to Departmental directives. The solution automatically logs all deduplication decisions along with match scores, field-level outcomes, user actions, and timestamps to support comprehensive data quality monitoring and compliance verification.

Configurations can be managed directly by jurisdictional administrators or with support from SSG, providing flexibility based on the jurisdiction's technical capacity and preferences. This partnership model ensures jurisdictions maintain control over data quality standards while

benefiting from SSG's expertise in public health informatics and federal compliance 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.

Casetivity-IIS provides comprehensive interface management capabilities that support the secure exchange and integration of data between the IIS and external systems in accordance with CDC, federal, and jurisdictional standards. The solution supports standards-based interoperability through HL7 messaging, APIs, and other integration methods; provides structured recruitment, enrollment, and onboarding processes for data exchange partners; actively monitors and validates incoming and outgoing transactions; and includes tools to investigate, manage, and resolve interface errors and data quality issues. This integrated approach ensures reliable, standards-compliant interoperability while supporting continuous data quality improvement and uninterrupted data exchange across the immunization ecosystem.

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.

Casetivity-IIS exchanges data in full accordance with current interoperability standards endorsed by the Centers for Disease Control and Prevention (CDC) for message content, format, and transport. The solution supports comprehensive bidirectional data exchange with health information systems, electronic health records (EHRs), the CDC Immunization Gateway (IZ Gateway), and the Vaccine Tracking System (VTrckS) using CDC-endorsed HL7 v2.5.1 messaging standards.

HL7 Messaging via CDC-Endorsed SOAP Interface

Casetivity-IIS implements CDC-endorsed interoperability standards across all data exchange functions. The platform manages interfaces for exchange and integration of data electronically between the IIS and other information systems in accordance with federal and jurisdictional standards. Message content, format, and transport protocols align with CDC specifications to

ensure seamless interoperability with external systems and compliance with federal requirements.

Casetivity-IIS exposes its HL7 interface using the standard CDC SOAP WSDL for IIS messaging. It supports the most common HL7 v2 message types used in immunization systems:

- **VXU** for vaccine record submissions and demographic updates
- **QBP** for patient history and forecast queries (bulk and individual)
- **ADT** for demographic-only updates

These are implemented in alignment with the CDC's HL7 Implementation Guide for Immunization Messaging. The solution includes message validation tools, logging, and configurable error handling to support onboarding and long-term quality monitoring.

CDC VTrckS

The solution provides comprehensive bidirectional integration with CDC VTrckS via the ExIS (External Information System) interface, using standard CDC communication formats and protocols. *Casetivity*-IIS supports both manual file-based import/export and API-based integration with VTrckS. The API integration can be configured to run on a scheduled basis, reducing manual workload and allowing state staff to focus on higher-priority program activities. Key file exchange capabilities include Master Data (outbound), Provider Orders (outbound), Inventory (outbound), Returns (outbound/inbound), and Wastage (outbound). This integration ensures real-time or near-real-time synchronization of vaccine ordering, shipment tracking, and inventory reconciliation.

Support for Integration Beyond HL7

In addition to the CDC-standard SOAP interface for HL7 messaging, *Casetivity* supports a wide range of additional integration methods to meet current and future needs. This includes:

- **RESTful APIs** for real-time, bidirectional communication with external systems
- **Excel-based roster templates** for use cases such as school reporting or mass vaccination clinics
- **Flat file processing** (CSV, TXT, XML, JSON, etc) for file-based integration needs
- **Custom data parsers** for handling unique formats when needed

Casetivity is built as a configurable low-code platform, and integration work is typically handled through configuration rather than custom code deployments. Interface development—whether using HL7, REST, or file-based protocols—is one of the most common areas of customization and is supported by a library of reusable building blocks. This allows the system to adapt quickly and efficiently to new interface requirements without extensive redevelopment.

Cross-Jurisdictional and Gateway Exchange

Casetivity-IIS can connect to the CDC's Immunization Gateway (IZ Gateway), supporting services such as Connect and Share for nationwide interoperability. It also supports direct connections to other jurisdictions using the same standards as needed to meet cross-state data sharing goals.

SSG Standards Compliance Guarantee

As technology evolves, SSG guarantees continued compliance with CDC and state interoperability standards. SSG will maintain applicable interoperability standards throughout the delivery and operation of *Casetivity*-IIS.

Casetivity-IIS meets the requirement by exchanging data with health information systems in accordance with current CDC-endorsed interoperability standards for message content, format, and transport, supporting federal compliance and seamless integration across the immunization ecosystem.

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

Casetivity-IIS actively supports the recruitment, enrollment, and onboarding of IIS partners and providers for electronic data exchange through a comprehensive Resource Center and integrated onboarding capabilities designed to streamline engagement and reduce administrative burden. The following describes the integrated functionality as well as SSG services that support these onboarding activities.

End User and Data Exchange Partner Onboarding

The system enables jurisdictions to configure custom onboarding processes that manage and monitor engagements with external healthcare providers. Self-registration functionality allows providers to initiate enrollment independently, while automated onboarding steps reduce manual work and streamline the process from initial contact through activation. This approach accelerates partner onboarding while maintaining oversight and quality control.

More specifically, the solution translates AIRA's best practices through automated workflows, role-based dashboards, and integrated communications tracking. The system supports a variety of data exchange scenarios—including VXU, QBP/RSP (bidirectional), GUI/direct entry, and legacy transitions.

Provider Registration and Workflow

- Providers initiate onboarding through a dynamic online registration form that captures key details such as organization information, user roles, data exchange intent, and legal agreements.

- The registration process triggers a jurisdictionally governed workflow that includes approval steps, automated account provisioning, and tailored onboarding task assignments.
- Onboarding lifecycle phases—including Discovery & Planning, Development & Testing, Production Approval, and Ongoing Monitoring—are fully supported within the system.

Role-Specific Onboarding

- System supports designation of key contacts:
  - **Access Administrator:** Manages site and users.
  - **Clinical Champion:** Oversees clinical readiness.
  - **Technical Contact:** Leads interface setup and testing.

Workflow, Communication & Monitoring

- *Casetivity*-IIS facilitates structured HL7 onboarding with automated task assignments, milestone tracking, and integrated project communications (e.g., kickoff calls, readiness checklists, vendor coordination).
- The Rollout Team actively supports providers by:
  - Guiding providers through onboarding tasks and HL7 interface setup.
  - Reviewing test messages submitted to the certification environment.
  - Providing feedback on conformance and data quality.
  - Approving providers for production access upon successful completion of readiness criteria.
- Beyond initial onboarding, the team continues to monitor message quality and supports providers when changes occur – whether due to HL7 specification updates, validation rule changes, or EHR system modifications – ensuring ongoing compliance and uninterrupted data exchange.

Training & Reporting Capabilities

  - Optional training series, videos, and email outreach campaigns can be delivered through integrated third-party tools like Constant Contact.
  - Built-in reporting and extracts support queue management, progress tracking, and data quality oversight throughout the onboarding lifecycle.

Data Exchange Certification Testing

Data submitters can test their HL7 messages against the jurisdiction's custom validation rules before going live. This pre-production testing capability ensures that interfaces are configured correctly and data quality standards are met before production data exchange begins, reducing errors and support burden after go-live.

Providers begin the onboarding process by sending HL7 messages to a dedicated Certification Environment. This environment mirrors the production system but is isolated for safe testing and validation. It allows providers to:

- Validate message structure and content.
- Test conformance to HL7 v2.5.1 standards and State-specific requirements.
- Review validation reports that identify any errors, warnings, or missing data.
- Iteratively refine and improve their HL7 messages in collaboration with the Department's Rollout staff.

Review and Approval by Rollout Team
During this phase:

- The Department's Rollout team monitors message submissions, provides feedback, and assists providers with interpreting validation results.
- Providers must successfully demonstrate accurate, complete, and standards-compliant HL7 messaging for various scenarios (e.g., new immunizations, historical records, updates, and deletes).

Certification and Go-Live Authorization
Once a provider's messages meet the required standards:

- They are formally certified to exchange data.
- The provider is approved to go live and begin sending HL7 messages to the production *Casetivity*-IIS system.

Centralized Ticketing System
A centralized ticketing system tracks and manages all open requests throughout the onboarding process. This ensures that all follow-up items are completed in a timely manner and provides visibility into the status of each partner's onboarding progress.

Extensive Data Extracts for Ad-Hoc Analysis
The Resource Center provides extensive data extracts that enable jurisdictions to optimize onboarding processes and provide status updates on current onboarding efforts. This reporting capability supports continuous improvement and accountability in partner recruitment and enrollment activities.

Training and Support Materials
Casetivity-IIS has an integrated Training and Resource Center which supports provider data exchange onboarding through the following.

General Training

- Embedded in the application, the Training Center hosts:
  - Instructional videos
  - Mini-guides and walkthroughs for various modules of the system.
  - Links and resources for recorded webinars, live webinars, in-person and self-hosted trainings
  - Technical resources, release notes, user guides.

  - Materials to support providers like Fact Sheets, Posters, Objection Forms, etc.
  - Links to Immunization schedules, VIS sheets, etc.
- The training and resource center pages and content are highly customizable to meet the look and feel your jurisdiction desires.

VFC Training Workflow

- Includes a task-based process to validate training completion with a video and test.
- Dashboard views and reports to monitor training compliance.

Support for Multiple Learning Formats

- Tracks in-person training participation alongside digital modules.
- Generates reports and certificates of completion.

When major system releases occur, training materials are updated and posted on the resource website. New training sessions can be scheduled with users as needed to ensure partners remain current with system capabilities and best practices.

In summary, all these integrated capabilities and services enable jurisdictions to actively recruit, efficiently enroll, and systematically onboard IIS partners and providers for electronic data exchange while maintaining data quality standards and reducing the administrative burden on both the jurisdiction and participating providers.

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

Casetivity-IIS actively monitors and evaluates data submitted via electronic data exchange through a comprehensive HL7 Administration module and integrated data quality management capabilities. The solution provides jurisdictional administrators with configurable tools to establish validation rules, monitor message quality in real time, and investigate anomalies systematically.

The HL7 Administration module enables administrators to configure rules governing data validation of incoming HL7 messages. Administrators can adjust data quality-related business rules for validations in both HL7 and the user interface, including setting whether validations are classified as Error, Warning, or Informational levels. This flexibility allows jurisdictions to balance data quality enforcement with external system adoption rates. Administrators also can create or update existing data quality reports to align with jurisdictional monitoring requirements.

Casetivity-IIS supports real-time data exchange per the CDC HL7 Implementation Guide, processing the most common HL7 v2 message types used in immunization systems: VXU for vaccine record submissions and demographic updates, QBP for patient history and forecast queries, and ADT for demographic-only updates. The solution includes message validation tools,

logging, and configurable error handling to support both initial onboarding and long-term quality monitoring.

The system provides the ability to view HL7 messages for an organization within a defined date range per jurisdictional policy. This capability is available out-of-the-box as part of the Data Exchange functionality, enabling staff to review message history and identify patterns or issues at the organizational level.

Data quality monitoring extends beyond message-level validation. Pre-defined data quality reports are included in the solution, and jurisdictional administrators can configure which data elements are monitored along with target thresholds for organizations. Data Quality Dashboards compile data quality investigations and issues from multiple modules into a central location, including HL7 message quality, patient completeness, invalid dose summaries, and pending corrections. Users can drill down to view full patient and provider context in one place and manage clinical data issues through task-based workflows that assign follow-ups to appropriate staff.

The solution features real-time anomaly detection, automated alerting, scalable processing architecture to handle surge traffic, and detailed logging and audit trails for rapid issue resolution. A centralized ticketing system tracks and manages all open requests to ensure follow-up items are completed in a timely manner during the onboarding process and ongoing operations.

These capabilities enable jurisdictions to maintain high data quality standards, identify and resolve electronic data exchange errors systematically, and support continuous improvement of interoperability with IIS partners and providers. The combination of configurable validation rules, comprehensive monitoring dashboards, and workflow-driven investigation tools ensures that data submitted via electronic data exchange is actively monitored and evaluated in accordance with jurisdictional policies and CDC standards.

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

Casetivity-IIS provides comprehensive capabilities to investigate and resolve electronic data exchange errors and anomalies with immunization information system (IIS) partners and providers. The solution delivers out-of-the-box monitoring, troubleshooting, and error resolution functionality that supports proactive data quality management and partner collaboration.

Casetivity-IIS monitors all data exchange traffic using AWS CloudWatch, which records response status and response time in ongoing metrics. This continuous monitoring enables SSG to track API response times and employ robust error handling strategies to maintain optimal performance in production environments. The solution's adaptive scaling capabilities ensure compliance with service levels and enhance resilience against disruptions.

The solution provides jurisdictional administrators with the ability to retrieve error messages within a specified date range by organization and filter error messages to identify patterns and prioritize resolution efforts. Administrators can adjust data quality business rules at Error, Warning, or Informational levels in both HL7 interfaces and the user interface, then create and update data quality reports to track resolution progress. This configurability allows jurisdictions to fine-tune validation rules based on their specific requirements while maintaining transparency with partners about data quality expectations.

Casetivity-IIS APIs utilize industry standards and design patterns, including loose coupling and sending acknowledgements for transactional integrity. This architecture leverages workflow and enterprise service bus (ESB) orchestration to make data-related processes more efficient in event-driven environments. The solution actively monitors and evaluates data submitted via electronic data exchange, enabling SSG and jurisdictional staff to investigate and resolve electronic data exchange errors and anomalies with partners and providers through transparent communication throughout the system development lifecycle.

These integrated monitoring, troubleshooting, and resolution capabilities ensure that *Casetivity*-IIS meets the requirement to investigate and resolve electronic data exchange errors and anomalies, supporting sustained data quality and strong partnerships with providers and external systems.

4.2.1.4. Ensure 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.

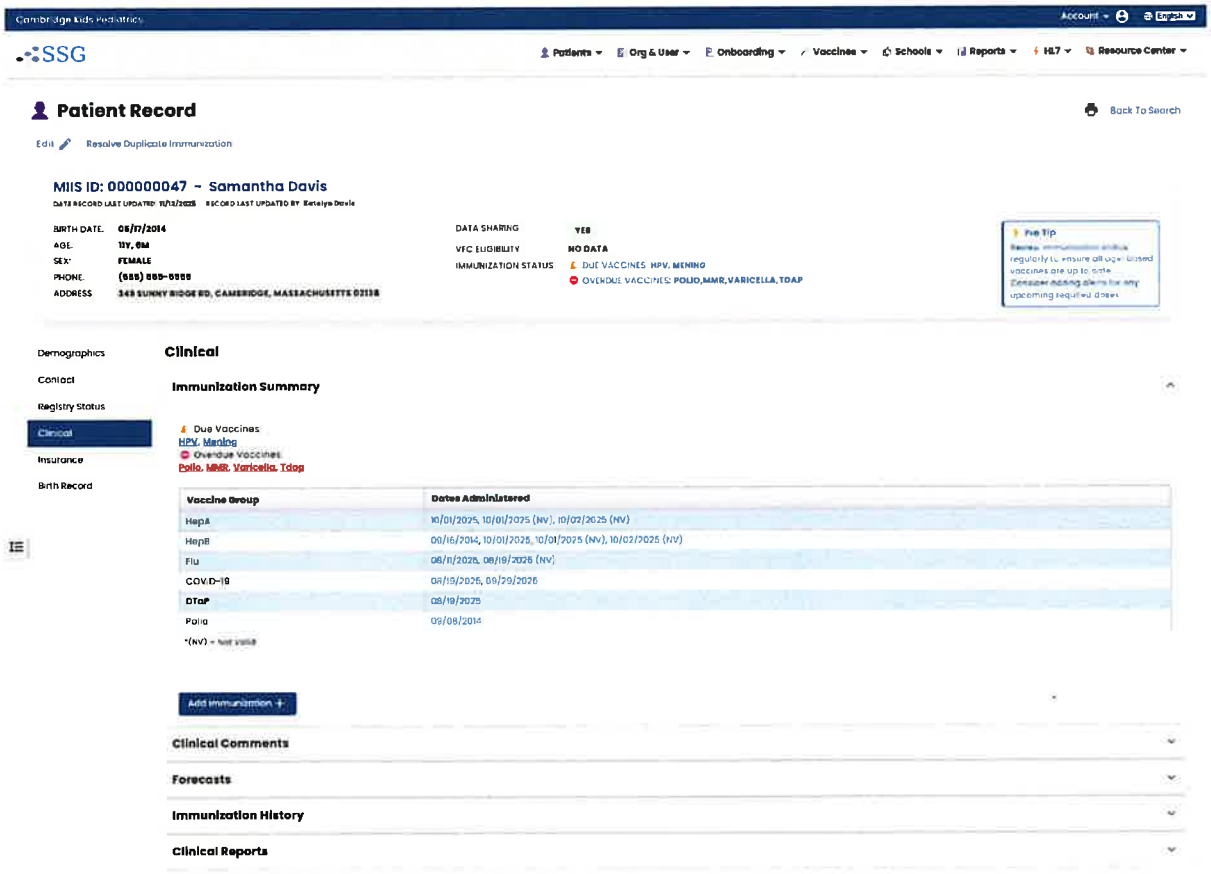
Casetivity-IIS supports pediatric, adolescent, and adult immunization forecasting through standards-based Clinical Decision Support (CDS) functionality aligned with current ACIP recommendations and CDC Clinical Decision Support for Immunization (CDSi) guidance. The

solution evaluates patient immunization histories, validates administered doses, and generates age- and risk-based vaccine forecasts using a forecasting engine that is maintained in alignment with evolving CDC and ACIP recommendations. This approach provides healthcare providers with accurate, up-to-date immunization evaluation and forecasting capabilities while reducing the administrative burden of maintaining forecasting logic and ensuring ongoing compliance with federal immunization standards.

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

SSG establishes and maintains Clinical Decision Support (CDS) functionality in *Casetivity*-IIS. This can be done either through integration with the Immunization Calculation Engine (ICE)—an open-source, standards-based forecasting engine developed and maintained by HLN Consulting and endorsed by the American Immunization Registry Association (AIRA) or a more custom jurisdictional solution. This integration provides out-of-the-box CDS capabilities that align with Advisory Committee on Immunization Practices (ACIP) recommendations for pediatric, adolescent, and adult immunization forecasts.

The ICE Forecaster is a production-grade engine designed to evaluate whether a patient is up-to-date on vaccinations and recommend next-dose scheduling based on current immunization schedules. *Casetivity*-IIS leverages ICE to deliver real-time decision support that includes age-based and risk-based evaluation, dose validity assessment, and forecasting for all age groups. The system evaluates a patient's immunization history against ACIP schedules—including the ACIP Recommended Catch-up Immunization Schedule for Children and Adolescents and the ACIP Child and Adolescent Immunization Schedule—to generate appropriate vaccine recommendations.



The solution is designed to adapt to updates in ACIP recommendations, ensuring healthcare providers receive proactive clinical decision support aligned with the latest guidance. This adaptability supports improved health outcomes by helping providers deliver age- and risk-appropriate immunization services based on each patient's unique immunization history.

Whether utilizing ICE or the SSG custom solution, *Casetivity*-IIS maintains CDS functionality in alignment with Clinical Decision Support for Immunization (CDSi) resources published on the CDC website, ensuring consistency with federal standards and interoperability requirements. This approach provides jurisdictions with a reliable, standards-based forecasting capability that supports compliance with IIS Functional Standards while reducing the administrative burden of maintaining custom forecasting logic.

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.

Casetivity-IIS establishes and maintains Clinical Decision Support (CDS) functionality in full alignment with CDSi resources published on the CDC website through integration with a third-party immunization forecasting engine that adheres to CDC CDSi logic specifications.

Casetivity-IIS utilizes ICE (Immunization Calculation Engine) from HLN Consulting as its vaccine clinical decision support algorithm. This third-party engine is specifically designed to align with CDC CDSi logic specifications, ensuring that immunization forecasts and evaluations reflect current ACIP recommendations and CDSi technical guidance. The integration enables Casetivity-IIS to deliver accurate, standards-based forecasting for pediatric, adolescent, and adult immunizations without requiring custom development or manual updates when CDC publishes new CDSi resources.

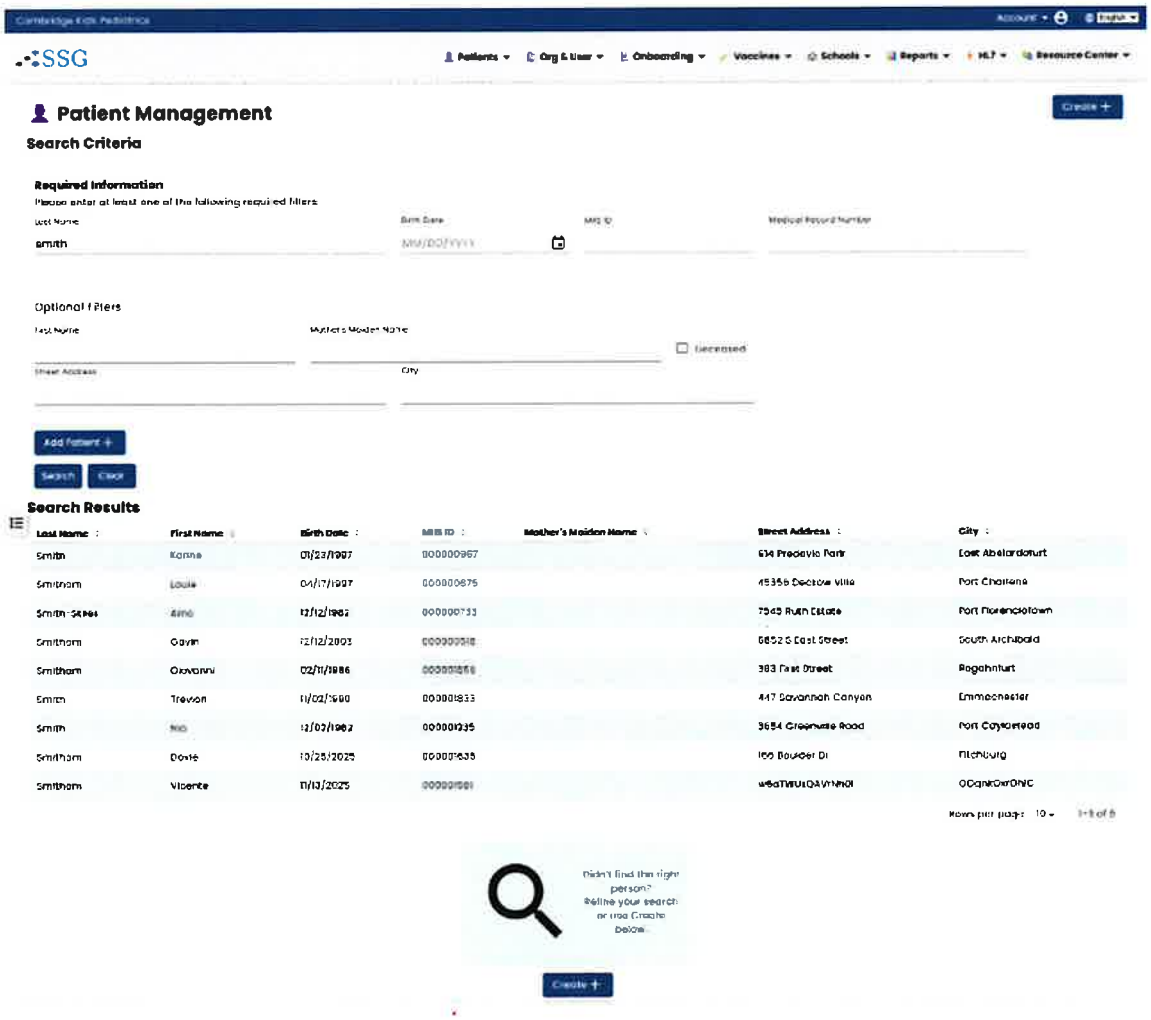
When CDC releases updated CDSi logic specifications or ACIP recommendation changes, the third-party vendor updates the forecasting engine to maintain alignment with the latest published resources. This approach reduces the administrative burden on jurisdictional staff and ensures that clinical decision support remains current with federal standards throughout the system lifecycle. The solution supports automated evaluation of patient immunization histories against ACIP schedules, generation of forecasts for due and overdue vaccines, and identification of valid doses based on CDSi-compliant business rules.

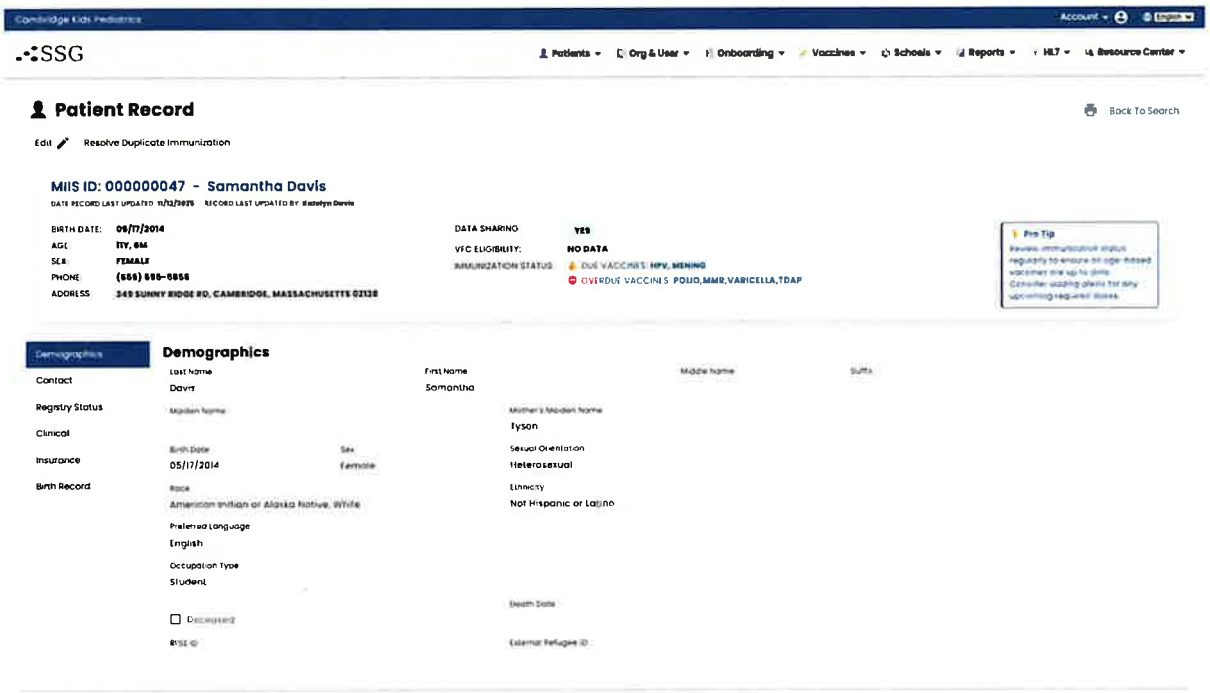
This architecture provides West Virginia with a reliable, maintainable CDS capability that evolves with CDC guidance while minimizing implementation risk and ongoing configuration requirements. SSG's approach ensures that *Casetivity*-IIS meets the requirement to establish and maintain Clinical Decision Support functionality in alignment with CDSi resources published on the CDC website.

4.2.1.5. Ensure 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.

Casetivity-IIS ensures that patient demographic and vaccination data is accessible only to authorized users through a comprehensive security and access management framework. The solution combines role-based access control, configurable permissions, strong authentication, account lifecycle management, audit logging, confidentiality protections, and role-specific training to ensure users have appropriate access based on their responsibilities and organizational affiliations. The following are the Patient Management and Record-related screens.





This approach supports secure access for public health agencies, providers, schools, childcare organizations, health plans, and other authorized partners while maintaining compliance with jurisdictional policies, privacy requirements, and industry security standards.

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

Casetivity-IIS implements comprehensive confidentiality policies that protect the privacy of individuals whose data is contained in the system through multiple integrated technical and administrative safeguards. The solution ensures that authorized users access patient demographic and vaccination data based strictly on user roles and permissions, with all access governed by role-based access control (RBAC) that limits data visibility to legitimate business purposes.

The system encrypts all data at rest using AES-256 encryption implemented with FIPS 140-2 validated modules, ensuring that personally identifiable information remains protected from unauthorized access. Only authorized administrators with appropriate RBAC permissions can decrypt personally identifiable information as needed for legitimate operational requirements. All user access and activity—including logins, data additions, edits, deletions, and exports—is captured in an internal audit log that supports compliance monitoring and investigation of suspected breaches. These audit logs are maintained for six years and provided to the agency at designated timeframes or upon request, with access limited to authorized agency staff.

Casetivity-IIS supports the configuration of authorization agreements and user agreements per jurisdictional policy, allowing agencies to define jurisdiction-specific data elements, address granularity levels, and demographic data collection based on privacy sensitivity requirements. The system's authentication and authorization capabilities validate user identity, entity affiliation, and system permissions before granting access, ensuring that only properly credentialed users can view or modify protected health information.

SSG complies with all relevant state and federal data privacy laws, regulations, and policies, including HIPAA and CDC guidelines. In the event a data breach is discovered or suspected, SSG immediately follows the incident reporting and response procedures outlined in agency policies, ensuring rapid containment and transparent communication. The solution's comprehensive account management policies align with industry security standards, and SSG provides ongoing training to ensure awareness of and adherence to confidentiality policies and procedures.

This multi-layered approach—combining encryption, role-based access control, comprehensive audit logging, configurable privacy policies, and regulatory compliance—ensures that *Casetivity*-IIS fully implements confidentiality policies that protect individual privacy while supporting authorized public health activities.

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

Casetivity-IIS implements comprehensive account management policies consistent with industry security standards through role-based access control, secure authentication mechanisms, and automated session management.

The system supports granular user account provisioning through delegated administration capabilities. Each user of *Casetivity*-IIS receives a unique login identity. The solution prohibits shared credentials and enforces user-specific validation workflows.

- Account Provisioning:
  - Requires a verified email address.
  - Role-dependent verification process (e.g., Access Administrator approval for sensitive roles).
  - Electronic signature and storage of applicable legal or data-use agreements.
- Authentication Options:
  - **Username and Password:** Enforces configurable complexity rules (length, character types, expiration, etc.).
  - **Multi-Factor Authentication (MFA):** Optional or mandatory by role; supports authenticator apps, reCAPTCHA, and email verification.
  - **Single Sign-On (SSO):** Supports SAML-based integration for jurisdictions requiring federated identity or enterprise IAM solutions.

Single Sign-On (SSO) integration is supported within the authentication and authorization framework, enabling the system to validate user identity and entity permissions through enterprise identity management systems. This integration streamlines access while maintaining security controls consistent with industry standards.

Session security is enforced through configurable expirations and timeouts that automatically terminate inactive user sessions. These controls reduce unauthorized access risk and align with federal cybersecurity standards governing protected health information systems.

The account management framework includes automated lifecycle controls that identify and inactivate user and site accounts when they are no longer active or authorized to access the system. This capability ensures access privileges remain current and aligned with organizational policies throughout the user lifecycle—from provisioning through deactivation.

SSG maintains these account management capabilities within a documented Secure Software Development Lifecycle (SSDLC) process aligned with NIST SP 800-218, ensuring security controls are embedded throughout system development, maintenance, and operations. Annual third-party penetration testing validates the effectiveness of access controls and authentication mechanisms in compliance with NIST 800-53 standards.

This comprehensive approach to account management delivers the security, auditability, and access governance required for immunization information systems handling protected health information.

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

Casetivity-IIS supports technical attributes for the setup and access of user roles and permissions through a comprehensive role-based access control (RBAC) that enables jurisdictional administrators to define, manage, and enforce granular access controls across the system.

Robust and Granular Role-Based Access Control
Casetivity-IIS uses function-based, granular RBAC to control visibility and actions across the solution. Permissions are shaped by:

- Role type (e.g., Provider, Jurisdictional Admin, Immunization Coordinator).
- Facility or organization affiliation.
- Geographic or jurisdictional scope (e.g., statewide or county-level access).

The solution provides jurisdictional administrators with out-of-the-box functionality to add user roles with distinct permissions, modify permissions to IIS processes and data for specific user roles, and configure page-level and field-level permissions and restrictions. Administrators can

assign multiple roles to individual users, allowing flexible permission structures that accommodate complex organizational hierarchies and jurisdictional policies.

Support for Multi-Organization Affiliations
Casetivity-IIS recognizes that users may operate across more than one organization (e.g., a nurse working at two clinics). The solution allows:

- Single-user profiles with multiple affiliations.
- A quick-switch interface that enables seamless transitions between organizational contexts without needing separate log-ins.
- Context-aware permissions that change dynamically based on the selected organization.

Role hierarchies automatically update all users assigned to a role based on changes made to the master role attributes, with all updates occurring in real time. This capability ensures consistent access control enforcement as policies evolve. This approach simplifies workflow for users with multiple roles and eliminates the need for redundant accounts.

Easy User Account and Role Maintenance
Role-based authorization can be configured easily by system administrators through explicit associations—such as users to roles and roles to permissions—or through expression-based rules. This flexibility allows access to be granted or restricted based on business rules down to the field level. The system supports the ability to delete roles or remove them from all users as needed, providing administrators with full control over the permission structure.

The Admin Console provides centralized tools for role definition and permission management, supported by audit logging of user activity, configuration changes, and data interactions. Security reports deliver real-time and historical insights into active and inactive accounts, role hierarchies and access mappings, login attempt history, and multi-factor authentication (MFA) status. These reporting capabilities enable administrators to monitor access patterns, identify potential security issues, and maintain compliance with jurisdictional policies.

An Access Administrator role, managed at the organization level, is responsible for user onboarding, role assignments, and coordination with IIS oversight teams. Authorized administrators and support personnel can impersonate users—with full audit tracking—to replicate and troubleshoot user-reported issues, validate role-specific UI elements or workflow steps, and provide direct in-session support without compromising user security. This capability is particularly valuable in environments with complex role hierarchies or nuanced jurisdictional workflows.

The solution's role-based security structure is designed to accommodate regulatory changes in future states, ensuring that jurisdictional administrators can adapt permissions and access controls as requirements evolve. This configurability reduces administrative burden, supports compliance with industry security standards, and ensures that authorized users have

appropriate access to patient demographic and vaccination data based on their assigned roles and permissions.

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

Casetivity-IIS provides user access in accordance with policies and procedures through a comprehensive role-based security framework that governs data authorization at multiple levels. The solution supports technical attributes for the setup and access of user roles and permissions, ensuring authorized users have appropriate access to patient demographic and vaccination data based on their assigned roles.

The solution implements role-based access control with delegated administration capabilities. Jurisdictional administrators can add, modify, and remove user access using role-based security standards. Individual users can have multiple roles assigned to their permissions, providing flexibility to accommodate complex organizational structures and varied responsibilities. The system supports page-level and field-level permissions and restrictions, with configurations designed to adapt to regulatory changes in future states.

The security framework operates through several integrated mechanisms. Users are associated with facilities through role-based access control, and clinicians are similarly linked to their respective facilities. Access is granted based on established confidentiality policies that protect the privacy of individuals whose data is contained in the system, consistent with industry security standards.

Authorization to Data
For data authorization, *Casetivity*-IIS maintains comprehensive account management policies. Jurisdictional administrators can configure authorization agreements and user agreements per jurisdictional policy, including jurisdiction-specific data elements, address granularity, and demographic data based on privacy sensitivity requirements. Access Controls Include:

- **Field-Level Security:** Define what data elements users can view/edit.
- **Task-Specific Menus and Dashboards:** Interfaces are dynamically rendered based on user roles.
- **Data Partitioning:** Users only access data relevant to their assigned entities.

The solution provides authorized IIS partners and providers with appropriate access to data for public and population health purposes, including childcare, schools, colleges, health plans, and clinics.

Hierarchy Configuration
Casetivity-IIS supports a flexible, multi-level organizational hierarchy that can be configured to reflect the State's structure, including state, local health departments, providers, and partner organizations. The solution's data model enables administrators to define and manage hierarchy levels, parent-child relationships, and multi-site organizations without code changes. Hierarchy

configuration drives data access, reporting outputs, and workflow routing. This allows the State to operate within defined boundaries while maintaining appropriate oversight and visibility. Administrative users can update hierarchy structures through intuitive tools, with changes applied dynamically without any downtime.

Monitoring
The solution identifies and inactivates user and site accounts when they are no longer active or no longer authorized to access the system, maintaining security integrity throughout the account lifecycle.

SSG conforms to the State's Information Security Framework and maintains the technical infrastructure to securely capture, store, and process patient demographic and vaccination data consistent with established policies and procedures. This approach ensures that user access remains aligned with jurisdictional policies while protecting individual privacy and maintaining data security throughout all system operations.

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).

Casetivity-IIS supports authorized IIS partners and providers with appropriate access to data for public and population health purposes through a comprehensive role-based access control framework. The system ensures that childcare facilities, schools, colleges, health plans, and clinics can access the immunization data they need to fulfill their public health responsibilities while maintaining strict confidentiality and security protections.

The solution implements technical attributes for user roles and permissions that enable jurisdictional administrators to configure access levels based on organizational type and function. Partners such as school nurses, childcare administrators, and health plan staff receive role-specific permissions that allow them to view and use immunization records for compliance verification, coverage assessment, and population health reporting without accessing data beyond their authorized scope. This granular permission structure ensures that each partner organization can perform its public health functions while protecting individual privacy.

Casetivity-IIS provides direct access to standard and ad-hoc reports that support public health purposes. School and childcare partners can generate compliance reports by grade, school, and district to identify students who need immunizations or exemption documentation. Health plans and clinics can access coverage reports to assess vaccination rates and identify vulnerable populations requiring outreach. The system supports data visualization, presentation, and analysis tools that enable partners to interpret immunization data for program planning and quality improvement without requiring assistance from IIS staff.

Role-Based Access Control (RBAC)

- Hierarchical Role Assignments: Users are assigned one or more roles at account creation or approval, which govern their access to system features, data types, and jurisdictional scopes.
- Roles are function-based and tailored for different user types, such as: Providers and clinical staff (e.g., vaccine data entry, patient lookup), School nurses and local health officials (e.g., certificate printing, compliance tracking), Jurisdictional administrators (e.g., user management, reporting), System administrators (e.g., configuration, security settings).

Customizable Role Definitions

- The Department can define and manage new roles or adjust existing ones.
- Each role can be configured for:
  - Field-level access (view, edit, hide specific fields).
  - Entity-level permissions (e.g., patients, vaccines, inventory).
  - Functional access (e.g., dashboards, reports, data exchange).
  - Group and Organizational Scoping

Organization and Location-Based Segregation

- Users are associated with specific organizations or provider sites, which restricts access to data relevant to their assignments.
- The system can enforce strict data partitioning, preventing users from viewing or editing data outside their designated facility or jurisdiction.

Jurisdictional Configurations

- Supports complex jurisdictional hierarchies such as:
  - Cities spanning multiple counties.
  - Public health regions made up of grouped municipalities.
  - Access to reports, dashboards, and patient data is scoped to the jurisdictional level assigned to the user's group.
  - Role-Specific Dashboards and Views

Personalized User Interfaces

- Upon login, users are presented with dashboards, menus, and tasks relevant to their roles.
- Irrelevant functions or data entities are hidden, reducing confusion and enhancing user experience.

Role Review and Deactivation Tools

- Administrators can review assigned roles and deactivate or adjust them as needed.
- Inactive users can be automatically suspended after a defined period of non-use.

Self-Service and Delegated Administration

- Each provider site designates an Access Administrator who can:
  - Add and deactivate users.
  - Assign roles based on local workflows.
  - Monitor user activity within their facility.
- Department administrators maintain authority over global role definitions, jurisdictional access, and system-wide security settings.

For partners requiring more detailed data access, the system supports direct database access for authorized internal users to perform data extracts and queries in accordance with policies and procedures. This capability enables public health agencies and authorized research partners to conduct population-level analyses while maintaining appropriate security controls and audit trails. All access is governed by comprehensive account management policies consistent with industry security standards, and the system identifies and inactivates user and site accounts when they are no longer active or authorized.

Casetivity-IIS meets the requirement by providing authorized IIS partners and providers with appropriate, secure, role-based access to immunization data that supports public and population health purposes across childcare, school, college, health plan, and clinic settings.

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

SSG provides comprehensive training to support users in accessing patient demographic and vaccination data within *Casetivity*-IIS. The training program addresses both internal authorized users and external IIS partners and providers, ensuring complete, timely, and accurate patient demographic and vaccination records across the system.

SSG delivers role-based training that covers the technical aspects of accessing patient demographic and vaccination data through the system's user interface. This training includes instruction on user roles and permissions, authentication and authorization processes, and the specific workflows for searching, retrieving, and managing patient records. Users learn how to navigate the system's patient search functionality, access immunization histories, and utilize reporting tools to generate coverage reports and ad-hoc queries without requiring assistance from IIS staff.

The training program extends to IIS partners and providers, delivering feedback and instruction to ensure data quality standards are maintained. SSG provides training on proper data entry practices, validation requirements, and the use of electronic tools for address standardization and verification. This approach supports the identification, prevention, and resolution of duplicate and fragmented patient demographic and vaccination data in accordance with established policies and procedures.

SSG's training also covers HS-related topics, including accessing, generating, and interpreting reports for federal and jurisdictional reporting requirements. Users receive instruction on utilizing standard reports, creating ad-hoc queries, and accessing data for visualization, presentation, and analysis purposes. The training ensures that authorized users understand how to access patient demographic and vaccination data appropriately based on their assigned roles and permissions, while maintaining confidentiality policies that protect individual privacy.

To accommodate different learning preferences and operational constraints, SSG employs a variety of training delivery methods. Typically, the training program includes both live sessions and asynchronous content to maximize accessibility. For users unable to attend live sessions, comprehensive digital resources remain available on demand. The following is a list of Training Delivery Methods available:

- Online self-paced training modules that provide foundational system exposure and instruction, accessible anytime for flexible learning
- Live instructor-led training sessions delivered both in-person and via webinar, enabling real-time interaction and immediate question resolution
- Asynchronous training videos available on the website and within the IIS itself, providing just-in-time learning support
- Written manuals and job aids that serve as ongoing reference materials
- Frequently Asked Questions (FAQs) addressing common user challenges
- Hands-on practice sessions in training environments that allow users to apply skills immediately

Based on the target user groups and input from West Virginia about the best delivery methods, SSG will adjust the training delivery approach. SSG will document the specific delivery methods in the Training Plan. Based on the information in the solicitation, SSG proposes the following training sessions, estimated at approximately 300 hours total:

- Three (3) Train-the-Trainer Sessions for Agency Staff Trainers
- Ten (10) End-User Training sessions covering specific user groups, including one session dedicated to UAT Testers
- Participation in 23 training sessions led by the WV team, but attended and supported by SSG.

This comprehensive training approach ensures that all system users, from internal staff to external partners, have the knowledge and skills necessary to access patient demographic and vaccination data effectively, supporting data quality, compliance, and improved immunization service delivery. Additionally, it is done in partnership with WV so that the knowledge and skill for continued training is transferred to provide WV more flexibility and autonomy.

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.

Casetivity-IIS identifies and inactivates user and site accounts through both automated and manual processes that ensure only authorized individuals retain access to the system.

The solution includes a configurable automated process that inactivates user accounts based on inactivity. The system records each user's last login date and evaluates account activity on a regular schedule, such as nightly. If a user has not logged in within a defined period, for example, 90 days—and does not meet any exclusion criteria, their account is flagged and automatically inactivated. The inactivity threshold and exclusion rules can be configured based on user properties such as role, allowing the jurisdiction to tailor the process to its policies.

In addition to automated inactivity-based deactivation, authorized users—including Access Administrators and members of the User Support Team—can manually and immediately inactivate user accounts at any time. This capability is essential when a staff member leaves an organization or transitions into a role that no longer requires system access. Once deactivated, the user's access is immediately revoked. To regain access, the individual must be re-invited by an authorized user and complete all required registration and security verification steps.

The system supports role-based deactivation authority. Administrators can inactivate user accounts across the system, organization administrators can inactivate accounts associated with their organization, and jurisdictional administrators can inactivate user accounts or multiple accounts in one transaction. The system also stores the reason for inactivation, supporting accountability and audit requirements.

Access administrators have dashboard tools to monitor user activity and deactivations. These dashboards display accounts recently deactivated, those approaching inactivity thresholds, and overall counts of active and inactive users. Optionally, tasks can be generated upon deactivation to support follow-up actions with users. This visibility enables proactive account management and helps ensure that only active, authorized users maintain access to the immunization information system.

Casetivity-IIS meets the requirement to identify and inactivate user and site accounts when they are no longer active or authorized, providing both automated enforcement and administrative control to protect system access and data confidentiality.

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

Casetivity-IIS supports authorized public access to official immunization records through a secure, integrated Consumer Access Portal. The portal enables individuals, parents, and legal guardians to directly access, view, and print official immunization records in accordance with jurisdictional policies and procedures. Secure authentication controls, including multi-factor authentication and identity verification mechanisms, protect patient privacy while providing convenient self-service access to immunization histories and forecasting information without requiring assistance from IIS staff.

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

Casetivity-IIS provides consumers with direct access to immunization records through a secure, web-based Consumer Access Portal that aligns with jurisdictional policies and procedures. The portal enables individuals, parents, and legal guardians to retrieve personal and dependent immunization records (such as those for minors) in accordance with consent and authorization policies established by the jurisdiction.

The system implements multi-factor authentication (MFA) to ensure secure access. Authentication combines a user-supplied PIN with a unique, time-limited link sent to the email or phone number on file for the individual. This approach verifies identity while maintaining compliance with privacy regulations. The portal also integrates reCAPTCHA technology to prevent automated misuse and denial-of-service attacks, protecting the integrity of the system and the confidentiality of immunization data.

Once authenticated, authorized consumers can view the appropriate comprehensive immunization records through the portal. This includes the ability to view vaccination history and immunization forecasts with due dates—displaying earliest, recommended, and overdue dates for the next dose. The system also provides valid or invalid indicators with reasoning for previously administered doses, supporting informed decision-making about immunization needs. Consumers can print patient immunization records and generate official immunization histories directly from the portal without requiring assistance from IIS staff.

The Consumer Access Portal is delivered as an out-of-the-box capability within *Casetivity*-IIS. It is part of the single integrated solution, ensuring seamless alignment with the broader IIS infrastructure for demographic and immunization data management. This approach reduces implementation complexity, supports compliance with federal and jurisdictional privacy

requirements, and provides the public with convenient, secure access to official immunization records in accordance with established policies and procedures.

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.

Casetivity-IIS supports the reporting needs of federal and jurisdictional immunization programs through a comprehensive reporting framework that includes pre-configured standard reports, user-defined ad hoc reporting capabilities, and direct access to IIS data for authorized users. The solution enables jurisdictions to meet routine operational, programmatic, regulatory, and public health reporting requirements while maintaining flexibility to respond to emerging information needs, data quality initiatives, and analytical activities without vendor-dependent report development.

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

Casetivity-IIS provides comprehensive standard and ad hoc reporting capabilities that meet federal and jurisdictional reporting requirements through a combination of pre-configured reports, flexible query tools, and direct data access options.

- *Standard Reports: Casetivity*-IIS includes a library of pre-configured standard reports that jurisdictional administrators can generate without vendor assistance. These reports cover organizational and facility enrollment status, immunizing facilities, IIS user information, and other core reporting needs. Jurisdictional administrators control access to standard reports through role-based permissions, ensuring that users see only the reports appropriate to their responsibilities. The solution provides all standard reports currently available in the incumbent vendor's IIS solution, plus custom reports developed specifically to meet jurisdictional needs.
- *Ad Hoc Reporting: Casetivity*-IIS supports ad hoc queries of patient demographic and vaccination data through user-defined report formats. Authorized users can create, customize, and generate reports on demand without requiring IIS staff assistance. The solution allows jurisdictional teams—including immunization program staff and data analytics teams—to access all portions of the system to produce ad hoc reports as

necessary. This capability ensures that reporting can adapt quickly to emerging program needs, policy changes, or outbreak response requirements.

- *Direct Data Access:* SSG provides direct access to raw IIS data for internal authorized users through database extracts and queries in accordance with policies and procedures. This access supports data visualization, presentation, and analysis activities. The solution accommodates direct data connections through APIs or other interfaces, enabling jurisdictional data teams to extract information for custom reporting workflows and analytical tools without vendor-dependent development cycles.
- *Data Quality and Validation:* Jurisdictional administrators can adjust data quality business rules that inform reporting accuracy. The system allows configuration of validation rules at Error, Warning, and Informational levels for both HL7 messages and user interface data entry. Administrators can create and update data quality reports, configure data elements, and set target thresholds per organization to ensure that reporting meets federal and jurisdictional standards.

This reporting architecture ensures that the jurisdiction maintains control over both routine and specialized reporting needs while meeting CDC requirements and supporting public health decision-making at all levels.

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

Casetivity-IIS supports ad hoc queries of patient demographic and vaccination data through a combination of configurable reporting tools, direct database access for authorized users, reusable query templates, and data export capabilities. The solution enables jurisdictions to securely access, analyze, visualize, and present immunization data in accordance with established policies and procedures while supporting operational reporting, coverage assessments, data quality initiatives, public health analysis, and evidence-based decision-making without requiring vendor-developed custom reports.

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.

SSG's *Casetivity*-IIS supports direct access for internal authorized users to IIS databases for data extracts and queries through role-based access control and configurable permissions aligned with jurisdictional policies and procedures. The solution enables authorized internal users to access IIS data securely while maintaining data integrity and system performance.

The solution implements comprehensive user roles and permissions that govern database access based on user authorization levels. Jurisdictional administrators configure access controls to define which internal users can perform data extracts and queries, ensuring compliance with established policies and procedures.

Casetivity-IIS provides secure, efficient querying methods for authorized users through its data access framework. The solution supports standard reports, ad hoc queries and reports, and the ability to create, save, and schedule customized data queries on demand. Internal authorized users can generate data extracts and perform queries in accordance with their assigned permissions, with all access activities traceable to ensure accountability and maintain audit trails.

The single-tenant architecture enhances direct database access by providing dedicated infrastructure for each jurisdiction. This architecture ensures that internal authorized users access only their jurisdiction's data environment, eliminating cross-tenant data exposure risks. The dedicated database instance supports consistent query performance without resource contention from other jurisdictions, enabling reliable data extracts and analytics workflows. Single-tenant deployment also allows jurisdictional administrators to configure database access controls, backup schedules, and maintenance windows according to their specific operational requirements and security policies.

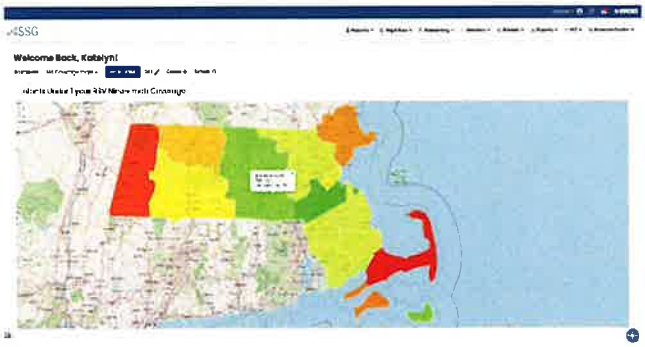
SSG supports jurisdictions in establishing and maintaining appropriate database access protocols through implementation planning, configuration services, and ongoing technical support. The solution includes documentation of access protocols and security frameworks related to data authorization, enabling jurisdictions to align database access practices with their governance requirements. This approach ensures internal authorized users can perform necessary data extracts and queries while maintaining data confidentiality, system security, and compliance with jurisdictional policies and procedures.

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

Casetivity-IIS supports access to data for visualization, presentation, and analysis through multiple integrated capabilities that enable authorized users to generate insights, create custom reports, and export data for use in external analytical tools.

The solution provides direct database access for internal authorized users to perform data extracts and queries in accordance with jurisdictional policies and procedures. This access supports ad-hoc analysis while maintaining appropriate security controls and audit logging. Authorized administrators can define user roles and permissions that govern data access levels, ensuring users interact only with data appropriate to their organizational role and jurisdiction.

For visualization and presentation, *Casetivity*-IIS includes standard reporting capabilities that generate pre-configured reports accessible to users based on their assigned permissions. The system supports the ability to store saved report templates, enabling users to create, save, and reuse custom report configurations tailored to specific analytical needs. Users can generate reports about IIS users, immunization coverage, data quality metrics, and other program-relevant topics without requiring assistance from IIS staff.

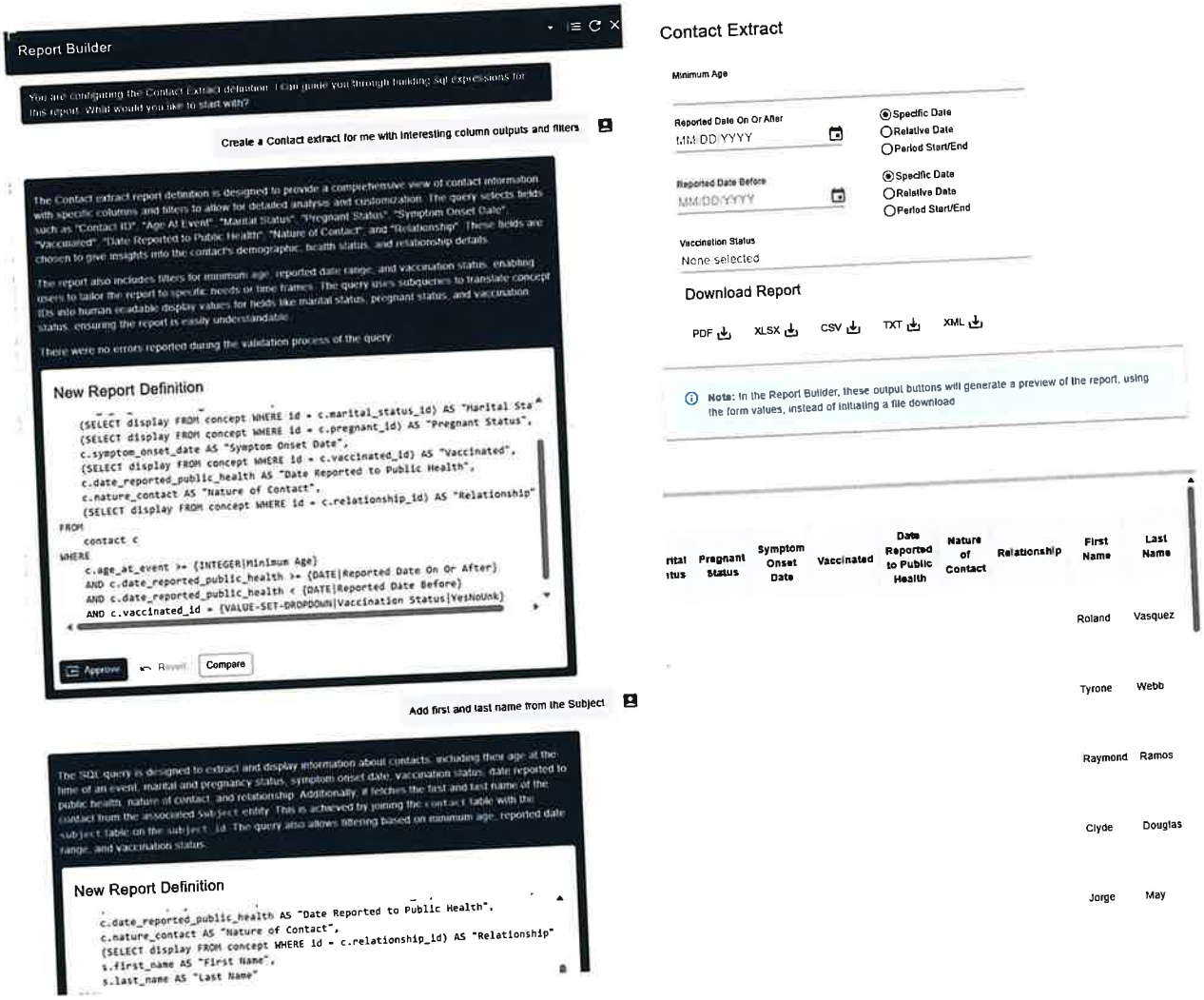


The solution supports data export functionality, allowing authorized users to export IIS data for use in other systems and external analytical tools. This capability facilitates integration with business intelligence platforms, statistical software, and data visualization applications that organizations may use for advanced analysis and presentation.

Casetivity-IIS also incorporates *Casetivity* **Compass**, a suite of AI-enabled capabilities that empowers administrators to configure, maintain, and optimize the IIS environment more effectively. With Compass, system administrators can leverage AI assistance to streamline report generation, tailor dashboards, and make real-time configuration adjustments without writing code. Compass-enabled features provide greater transparency in system behavior by summarizing security roles, data visibility, and workflow configurations in a user-friendly manner, supporting both immediate analytical needs and long-term scalability as public health requirements evolve.

The Admin Console provides role definition and permission management with audit logging of user activity, configuration changes, and data interactions. Security reports deliver real-time and historical insights into active and inactive accounts, role hierarchies, access mappings, and login attempt history. This governance framework ensures that data access for visualization and analysis remains secure, auditable, and aligned with jurisdictional policies.

These capabilities align directly with IIS Functional Standard 10.2, ensuring that authorized users can access, visualize, present, and analyze immunization data to support program reporting, coverage assessment, identification of vulnerable populations, and evidence-based public health decision-making.



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

Casetivity-IIS supports ad hoc queries of patient demographic and vaccination data through a combination of configurable reporting tools, direct data access for authorized users, reusable query and report templates, and data export capabilities. The solution enables jurisdictions to securely access, analyze, visualize, and present immunization data in accordance with established policies and procedures, supporting operational reporting, program evaluation,

public health analysis, and data-driven decision-making without requiring vendor-developed custom reports.

4.2.1.6.3.1. The IIS supports vaccine adverse event investigation.

Casetivity-IIS supports vaccine adverse event investigation by enabling authorized users to access patient demographic and vaccination data necessary to investigate reported adverse events. The system maintains comprehensive immunization records that include vaccine product details, lot numbers, administration dates, and provider information—all critical data elements needed during adverse event investigations.

When an adverse event is reported, authorized users can query the system to retrieve the complete vaccination history for affected patients, identify other individuals who received vaccines from the same lot, and generate reports listing patients who received non-viable vaccines or provider sites that received recalled vaccine lots. This capability allows public health officials to quickly assess the scope of potential adverse events and identify patterns across populations.

The system also refers users to appropriate resources to support adverse event documentation, ensuring that investigation findings are properly recorded and reported through established channels. This integrated approach enables jurisdictions to conduct thorough investigations while maintaining compliance with federal and state reporting requirements for vaccine safety monitoring.

Casetivity-IIS meets the requirement by providing the data access, reporting capabilities, and resource guidance necessary to support comprehensive vaccine adverse event investigation activities.

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

Casetivity-IIS supports vaccine adverse event investigation and refers users to appropriate resources to support adverse event documentation. When users need to document or investigate adverse events, the system provides access to relevant guidance and directs them to the proper reporting channels and resources established by federal and jurisdictional immunization programs.

This functionality ensures that healthcare providers and immunization program staff can quickly access the information and tools they need to properly document adverse events in compliance with federal reporting requirements. By integrating resource referrals directly into the workflow,

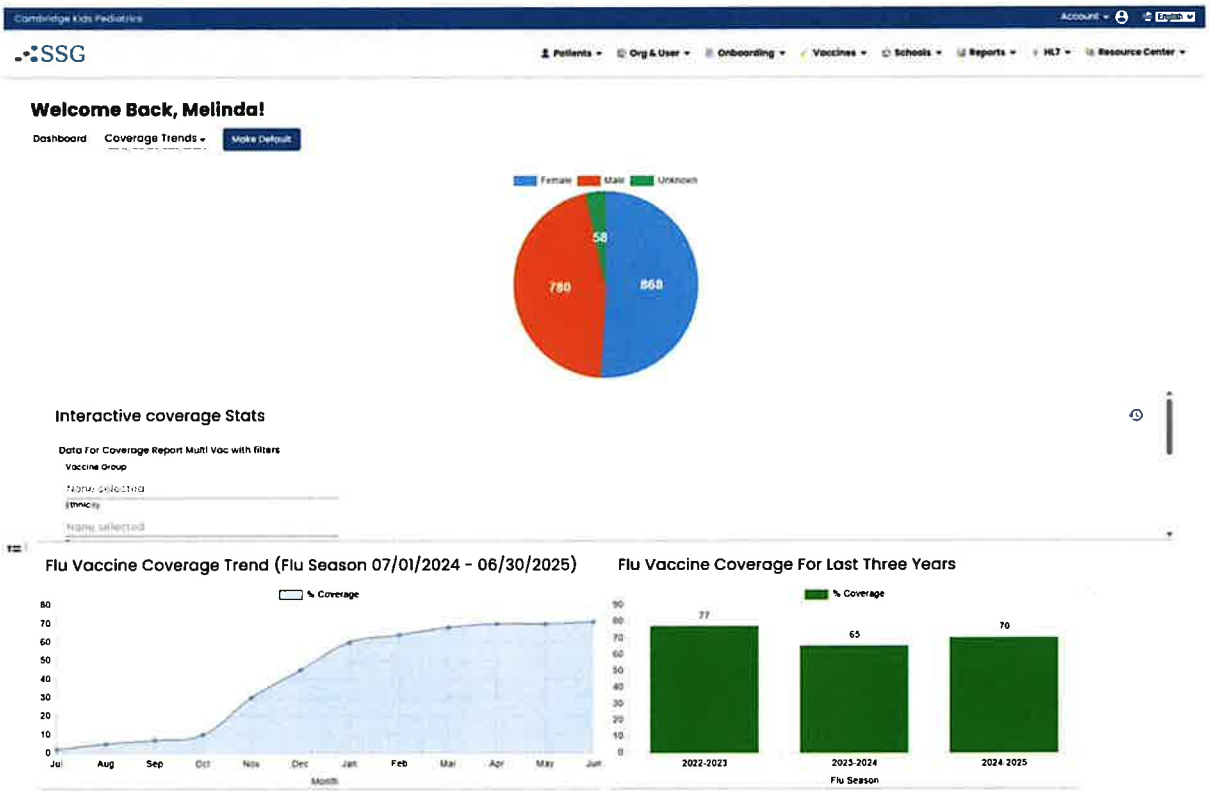
Casetivity-IIS reduces the administrative burden on users while supporting timely and accurate adverse event reporting.

The system's approach to adverse event support aligns with CDC IIS Functional Standards and helps your immunization program maintain compliance with federal and state adverse event investigation and documentation requirements.

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

Casetivity-IIS enables authorized users to independently generate immunization coverage reports without assistance from IIS staff through a combination of standard reports, ad hoc reporting capabilities, and role-based access to immunization data. The solution supports assessment of vaccination coverage, identification of vulnerable populations, patient status management at provider and jurisdiction levels, and compliance monitoring for childcare, school, and college immunization requirements. Comprehensive user training ensures that authorized users can access, generate, and interpret coverage reports to support program operations, public health analysis, and regulatory reporting needs.

In addition to detailed Coverage Reports, Casetivity-IIS also has robust and configurable Dashboards that provide useful information to end users in a secure way. The following is an example of such a Dashboard.



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

Casetivity-IIS provides comprehensive data access capabilities that enable authorized users to assess vaccination coverage and identify vulnerable populations through standard and ad-hoc reporting tools, user-defined parameters, and demographic segmentation.

The system includes predefined standard coverage reports that authorized users can generate on-demand without requiring assistance from SSG staff. These reports support multiple dimensions of analysis, including coverage by ethnicity, age range, patient sex/gender, user-defined geographic areas, vaccine type, and patient cohort. Standard reports available out-of-the-box include the Standard Childhood Coverage Report, Standard Adolescent Coverage Report, Adolescent 13–17-Year-Old Coverage Report, Flu Coverage Report, COVID-19 Coverage Report, Standard Childhood Master Rate Comparison Report, Standard Adolescent Master Rate Comparison Report, and CDC AFIX Report.

Beyond standard reports, *Casetivity*-IIS supports ad-hoc reporting functionality that allows authorized users to generate customized coverage reports using user-defined parameters. This capability enables jurisdictional staff to conduct independent analysis tailored to specific program needs, policy questions, or outbreak response scenarios. Users can define parameters

such as geographic boundaries, age ranges, vaccine series, and demographic characteristics to identify coverage gaps and vulnerable populations requiring targeted outreach.

The system also generates doses administered reports to support accountability for publicly purchased vaccine, ensuring that coverage assessment is linked to vaccine program management and stewardship. All reports respect role-based access controls, ensuring that users only view patient data they are authorized to access in accordance with confidentiality policies and procedures.

Casetivity-IIS supports direct access for internal authorized users to IIS databases for data extracts and queries in accordance with policies and procedures. The solution provides access to data for data visualization, presentation, and analysis, enabling jurisdictional staff to conduct sophisticated population health assessments. SSG provides training that covers accessing, generating, and interpreting reports, ensuring that authorized users can effectively leverage the system's data access capabilities 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.

Casetivity-IIS manages patient status at both the provider organization level and the geographic jurisdiction level through configurable, role-based functionality that supports active and inactive status tracking, reason codes, and status editing capabilities.

At the geographic jurisdiction level, the system stores active patient status, inactive patient status, and the reason for inactive status. Authorized users can edit active patient status and manage inactive patient status based on their assigned roles and permissions. This enables jurisdictional administrators to maintain accurate patient assignment records across counties, regions, or other geographic boundaries defined in the system hierarchy.

At the provider organization and facility level, *Casetivity*-IIS provides the same core functionality to store, edit, and manage both active and inactive patient status. This allows provider sites to track which patients are assigned to their organization for care coordination, reminder/recall activities, and reporting purposes. The system supports the ability to associate patients with specific facilities and organizations within the configurable hierarchy, ensuring that patient status reflects current care relationships.

The patient status management capability integrates with the system's role-based access control framework. Jurisdictional administrators configure user roles and permissions that determine which users can view, edit, or manage patient status at different organizational and

geographic levels. This ensures that status changes are made only by authorized personnel in accordance with program policies and data governance requirements.

These capabilities support accurate patient assignment for coverage reporting, reminder/recall campaigns, vaccine program eligibility tracking, and compliance with immunization requirements. By maintaining patient status at both provider and jurisdiction levels, *Casetivity*-IIS enables the immunization program to track patient movement between providers, identify patients who have moved out of jurisdiction, and ensure that reporting reflects current patient populations.

Casetivity-IIS meets the requirement to manage patient status at provider site and jurisdiction levels through out-of-the-box functionality that requires no customization.

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

SSG provides comprehensive training to support users in accessing, generating, and interpreting immunization coverage reports within *Casetivity*-IIS. The system enables users to generate predefined and ad hoc assessment and coverage reports without assistance from IIS staff, ensuring that authorized users can independently access the data they need to assess vaccination coverage and identify vulnerable populations.

The training program covers accessing patient demographic and vaccination data, with specific instruction on how to navigate the reporting interface, define user-specific parameters for coverage analysis, and interpret the results. Users learn to generate reports displaying immunization coverage by parameters they define, including geographic boundaries, age groups, vaccine series completion status, and other relevant filters. This training ensures that users at both provider site and jurisdiction levels can manage patient status and produce the coverage reports required for federal and jurisdictional reporting requirements.

SSG's training approach includes instruction on both standard reports and ad hoc query capabilities, enabling users to create customized reports on demand for data visualization, presentation, and analysis. The training also addresses how to support compliance with immunization requirements in childcare, school, and college settings, ensuring that users understand how to access and interpret coverage data for these specific populations.

By providing training that enables independent report generation and interpretation, SSG ensures that users can conduct coverage assessments, identify vulnerable populations, and support immunization rate improvement efforts without requiring ongoing assistance from IIS

staff. This approach reduces administrative burden while ensuring that authorized users have the skills and knowledge needed to leverage *Casetivity*-IIS reporting capabilities effectively.

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

Casetivity-IIS supports compliance with immunization requirements in childcare, school, and college settings through integrated roster management, reporting, and clinical decision support capabilities that enable educational institutions and health departments to track, evaluate, and report student immunization status efficiently.

The system evaluates student immunization histories against Advisory Committee on Immunization Practices (ACIP) recommendations using the Immunization Calculation Engine (ICE) – an open-source, standards-based forecasting engine that provides real-time decision support. This evaluation includes age-based and risk-based assessments, dose validity determinations, and forecasting aligned with the ACIP Child and Adolescent Immunization Schedule and the ACIP Recommended Catch-up Immunization Schedule for Children and Adolescents. Schools and childcare facilities can identify which students meet immunization requirements, which students need additional doses, and which students have exemptions on file.

The solution supports immunization-related efforts in both childcare and school settings by enabling authorized users to generate compliance reports without assistance from Immunization Information System (IIS) staff. Educational institutions can access student immunization data based on role-based permissions, filter by school, grade, district, and compliance status, and identify students who require follow-up. This functionality reduces administrative burden on health departments while giving schools the tools they need to maintain compliance with state and local immunization requirements.

For college settings, *Casetivity*-IIS provides the same evaluation and reporting capabilities, supporting institutions in verifying that incoming and enrolled students meet higher education immunization requirements. The system's ability to assess immunization histories according to ACIP schedules ensures that colleges can identify students who need additional vaccines or documentation before enrollment or participation in campus activities.

Casetivity-IIS meets the requirement to support compliance with immunization requirements across childcare, school, and college settings through clinical decision support, roster integration, role-based reporting access, and automated compliance tracking that streamline verification processes for educational institutions and public health programs.

4.2.1.6.5. The IIS supports reminder / recall activities.

Casetivity-IIS supports reminder and recall activities through integrated, self-service tools that enable authorized users to identify patients who are due or overdue for immunizations, generate reminder/recall lists, and conduct outreach activities without assistance from IIS staff. The solution leverages immunization forecasting and configurable business rules to support targeted patient outreach, improve immunization coverage rates, and reduce administrative burden on public health programs and provider organizations.

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

Casetivity-IIS supports conducting reminder/recall activities without requiring assistance from IIS staff through self-service functionality that enables authorized users to independently identify, generate, and manage reminder and recall notices.

The solution provides authorized users with direct access to reminder/recall tools that operate without manual intervention from IIS administrators. Users can configure time intervals between reminder/recall notices—such as 90 days or 60 days—through system settings that apply globally or can be tailored to specific organizational needs. This configuration capability allows immunization programs to establish reminder schedules for patients due for upcoming immunizations and recall schedules for patients who are past due, all without requiring technical support or custom development from IIS staff.

The reminder/recall functionality integrates with *Casetivity*-IIS's clinical decision support engine to automatically identify eligible patients based on immunization forecasting and ACIP recommendations. Authorized users can generate reminder/recall lists, review patient cohorts, and initiate outreach activities directly through the user interface. The system supports standard and ad hoc reporting for reminder/recall campaigns, enabling users to monitor outreach effectiveness and adjust strategies independently.

This self-service approach reduces administrative burden on IIS staff, accelerates time-to-action for immunization programs, and empowers provider organizations and public health users to conduct proactive outreach that improves immunization coverage rates. *Casetivity*-IIS meets the requirement by delivering reminder/recall capabilities that authorized users can access, configure, and execute without assistance from IIS staff.

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.

Casetivity-IIS supports management and quality assurance functions for federal and jurisdictional vaccine programs through configurable program workflows, dose-level vaccine eligibility tracking, inventory management and reconciliation capabilities, and comprehensive reporting tools. The solution enables jurisdictions to administer vaccine programs in accordance with federal and state policies, monitor vaccine accountability, track publicly purchased vaccine eligibility, and rapidly identify affected patients and provider sites in the event of vaccine recalls or non-viable vaccine events.

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

Casetivity-IIS establishes vaccine program procedures in accordance with federal and jurisdictional policies through configurable workflows, role-based access controls, and system-wide configuration tools that enable jurisdictional administrators to define, enforce, and maintain program-specific requirements.

The solution provides jurisdictional administrators with comprehensive configuration capabilities to establish vaccine program procedures aligned with federal and jurisdictional policies. Administrators configure enrollment forms unique to each program—including facility enrollment, vaccine ordering program enrollment, and HL7 data exchange—ensuring that program-specific requirements are captured and enforced from the point of onboarding. These forms can be modified to add or remove fields as jurisdictional policies evolve, and the system supports rules-based approval and rejection logic that automatically evaluates enrollment submissions against organization information, system-wide configurations, and program criteria.

Workflow support for establishing and enforcing procedures is built into the solution's administrative functions. Jurisdictional administrators adjust data quality business rules to set validation levels—Error, Warning, or Informational—for both HL7 message processing and user interface data entry. This ensures that vaccine program procedures are consistently applied across all data capture channels. The system maintains separate inventory tracking for VFC-supplied vaccines, jurisdiction-supplied vaccines, and private stock, enabling administrators to enforce eligibility tracking and program compliance at the dose level as required by federal vaccine program policies.

The solution supports vaccine inventory management, tracking, and reconciliation at both the IIS jurisdiction and provider site levels, with functionality for creating vaccine orders, monitoring order status, and automatically decrementing administered doses from active inventory. These capabilities ensure that vaccine program procedures governing ordering, distribution, and accountability are operationalized within the system workflow. Administrators configure authorization agreements and user agreements per jurisdictional policy, ensuring that all system users operate within established program parameters.

For emergency response scenarios, the solution supports expedited communication and onboarding with partners to capture patient demographic and vaccination data and includes offline documentation functionality for vaccine administration when connectivity is limited. This ensures that vaccine program procedures remain enforceable even during public health emergencies.

Casetivity-IIS provides the technical infrastructure and administrative controls necessary to establish vaccine program procedures in accordance with federal and jurisdictional policies, with workflow support that enables jurisdictional administrators to configure, enforce, and adapt procedures as program requirements evolve.

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

Casetivity-IIS supports the tracking of eligibility at the dose level for publicly purchased vaccines out of the box. The system captures and stores vaccine eligibility information at the individual dose level as part of the patient immunization record management process, enabling jurisdictions to track which doses qualify as publicly purchased vaccine in accordance with federal and jurisdictional vaccine program requirements.

This dose-level eligibility tracking capability integrates directly into the immunization record workflow. When authorized users add or edit patient immunization records, they can designate eligibility status for each vaccine dose administered. The system maintains this eligibility information at the dose level rather than at the patient or visit level, providing the granular tracking required for Vaccines for Children (VFC) program compliance and other publicly funded vaccine programs.

The eligibility tracking functionality supports vaccine inventory management and reconciliation at both the jurisdiction and provider site levels. As doses are administered and recorded, *Casetivity*-IIS automatically matches vaccine doses reported as administered to vaccine doses in inventory to facilitate dose decrementing. This automated matching process ensures that

publicly purchased vaccine inventory is accurately tracked and reconciled based on the eligibility designation captured at the dose level.

Jurisdictional administrators can establish and enforce vaccine program procedures in accordance with federal and jurisdictional policies through the system's workflow configuration capabilities. The dose-level eligibility tracking supports management and quality assurance functions required for federal and jurisdictional vaccine programs, including reporting requirements and inventory oversight.

Casetivity-IIS meets the requirement to support the tracking of eligibility at the dose level for publicly purchased vaccines through standard system functionality available to all authorized users.

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

Casetivity-IIS generates reports that identify patients who received non-viable vaccines through multiple standard reporting capabilities. The system provides out-of-the-box functionality to filter patient lists by immunization status, vaccine type, age range, or location, and can generate reports showing patients who received specific vaccine lots—including recalled or non-viable vaccines.

The system currently provides aggregate data on non-viable vaccines through the Data Quality/Scorecard report. For detailed patient-level reporting, users can leverage the Patients Vaccinated report and select unspecified vaccine types to identify patients who received non-viable vaccines. This approach allows authorized users to generate the necessary reports without requiring IIS staff assistance.

SSG can enhance this capability through customization to provide a dedicated report that lists individual patients who received non-viable vaccines, moving beyond the current aggregate count functionality. This customization would deliver a comprehensive patient-level report that meets the requirement for tracking and managing non-viable vaccine administration.

The system logs all vaccination activities in the patient's history, including vaccine lot information, ensuring complete traceability for vaccine quality management and patient notification purposes. This supports the jurisdiction's ability to quickly identify affected patients, conduct outreach, and maintain compliance with federal and jurisdictional vaccine program requirements.

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

Casetivity-IIS generates a report listing provider sites that received vaccine lots recalled by the manufacturer through its out-of-the-box standard reporting functionality. The system can generate an exportable listing of all providers and facilities, including their contact information, that were affected by a recall based on vaccine name, vaccination date range, and lot number. This capability enables jurisdictional administrators to quickly identify which provider sites received recalled vaccine lots and take appropriate action.

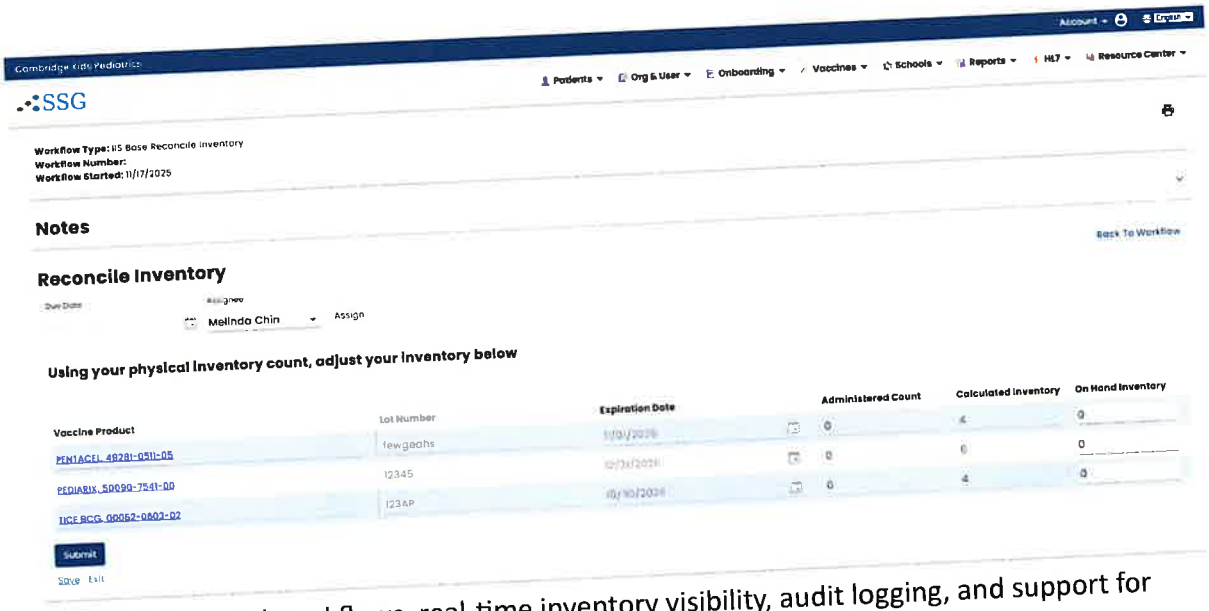
The system supports vaccine product recall activities by filtering and reporting on specific vaccine lots distributed to provider sites. When a manufacturer issues a recall, authorized users can query the system using the recalled lot number, vaccine name, and relevant date range to produce a comprehensive list of affected facilities. This report includes provider and facility contact information, allowing the jurisdiction to efficiently notify impacted sites and coordinate recall response activities.

Casetivity-IIS also provides the capability to generate reports identifying patients who received recalled vaccines, supporting both facility-level and patient-level recall management. The system logs all recall-related activities in the patient's history, ensuring comprehensive tracking and documentation throughout the recall process. These reporting capabilities align with federal and jurisdictional vaccine program requirements for quality assurance and inventory management.

This functionality meets the requirement for generating reports listing provider sites that received recalled vaccine lots, enabling the jurisdiction to respond quickly and effectively to manufacturer recalls while maintaining accurate documentation and supporting public health protection.

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

Casetivity-IIS provides comprehensive vaccine inventory management and reconciliation capabilities that support federal and jurisdictional vaccine program requirements at both the jurisdiction and provider levels. The solution supports vaccine ordering, inventory tracking, automated dose decrementing, reconciliation, wastage and return reporting, recall management, and complete inventory lifecycle accountability.



Through integrated workflows, real-time inventory visibility, audit logging, and support for public vaccine program requirements, *Casetivity*-IIS helps ensure accurate inventory management, regulatory compliance, and effective stewardship of vaccine resources.

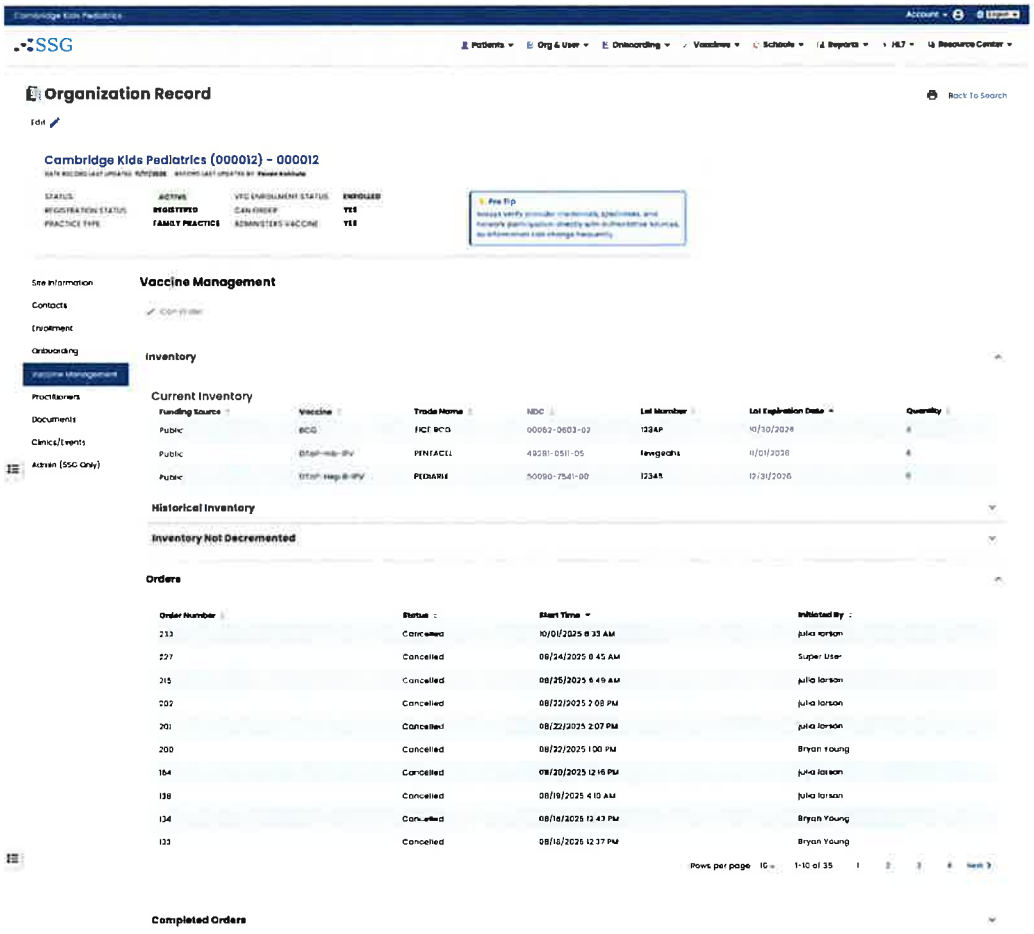
4.2.1.7.2.1. The IIS supports vaccine inventory management, tracking, and reconciliation at the IIS jurisdiction and provider site levels.

Casetivity-IIS provides comprehensive vaccine inventory management, tracking, and reconciliation capabilities at both the jurisdiction and provider site levels. The system supports complete lifecycle tracking of vaccine doses across all statuses—on hand, administered, wasted, expired, ordered, recalled, returned, and transferred—enabling full accountability and compliance with federal and jurisdictional vaccine program requirements.

At the provider site level, *Casetivity*-IIS enables facilities to manage vaccine inventory in real time. Providers track vaccines on hand through active inventory management, record administered doses with automatic inventory deduction, manage wasted doses with full audit logging, and monitor expired vaccines through alerts and dashboards. The system processes vaccine orders through CDC VTrckS integration, removes recalled lots from active inventory, views past vaccine returns within specified time frames, and manages transferred doses between storage units and locations. Providers can reconcile their storage unit quantities with the quantities in the IIS system to ensure accuracy across all dose tracking categories.

At the jurisdiction level, the system aggregates inventory data across user-defined hierarchies, supporting oversight and quality assurance functions for federal and jurisdictional vaccine programs. Jurisdictional administrators maintain separate inventory tracking for VFC-supplied vaccines, jurisdiction-supplied vaccines, and private stock, ensuring proper accountability for

publicly purchased vaccines. The system generates reports listing patients who received non-viable vaccines and provider sites that received recalled vaccine lots, supporting rapid response to quality issues.



The system provides clear visibility into immunizations that were not successfully deducted from inventory, enabling providers to easily identify, review, and resolve discrepancies. All inventory actions—ordering, receipt, reconciliation, and wastage—are fully logged for auditing purposes, and a complete inventory transaction log is available for each inventory line item. Role-specific dashboards highlight pending orders, expiring vaccines, and providers due for enrollment submission, while alerts and task assignments guide providers through necessary compliance actions.

Casetivity-IIS supports monthly and quarterly CDC extracts, including COVID-19, RSV, Flu, and Routine Immunization reports, as well as IISAR and PEAR submissions. Ad hoc exports are available for vaccine inventory reconciliation, accountability, or site visit preparation. This comprehensive approach to vaccine inventory management, tracking, and reconciliation at both

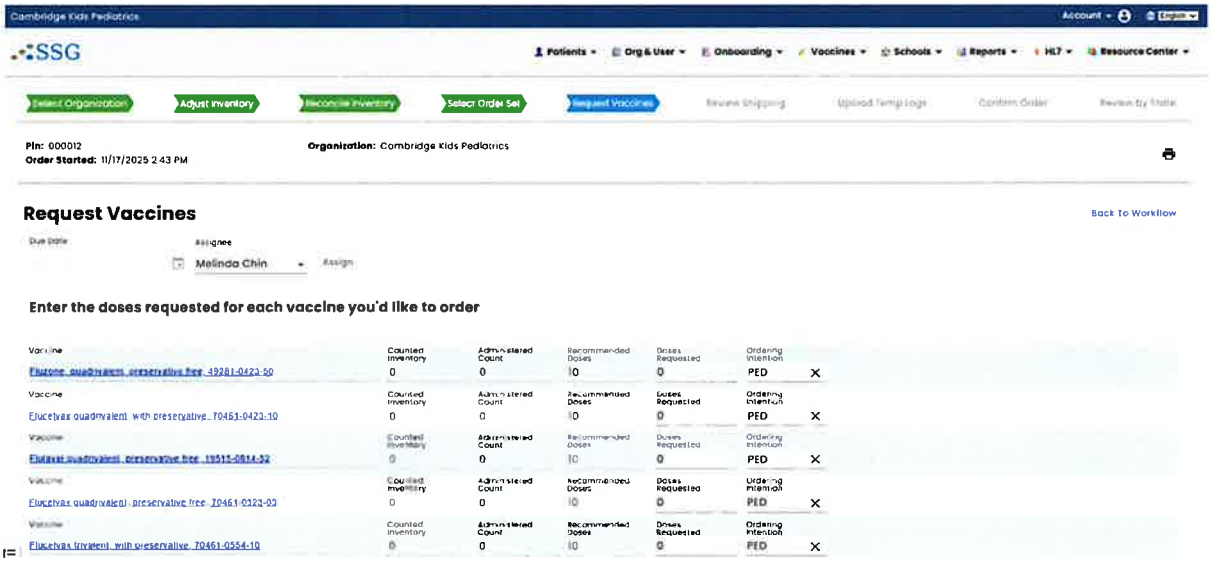
jurisdiction and provider site levels ensures accountability, supports regulatory compliance, and enables effective vaccine program administration.

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

Casetivity-IIS supports comprehensive vaccine ordering and order status monitoring through an integrated workflow that enables providers to place orders, track approvals, and monitor fulfillment directly within the system.

Vaccine Order Creation

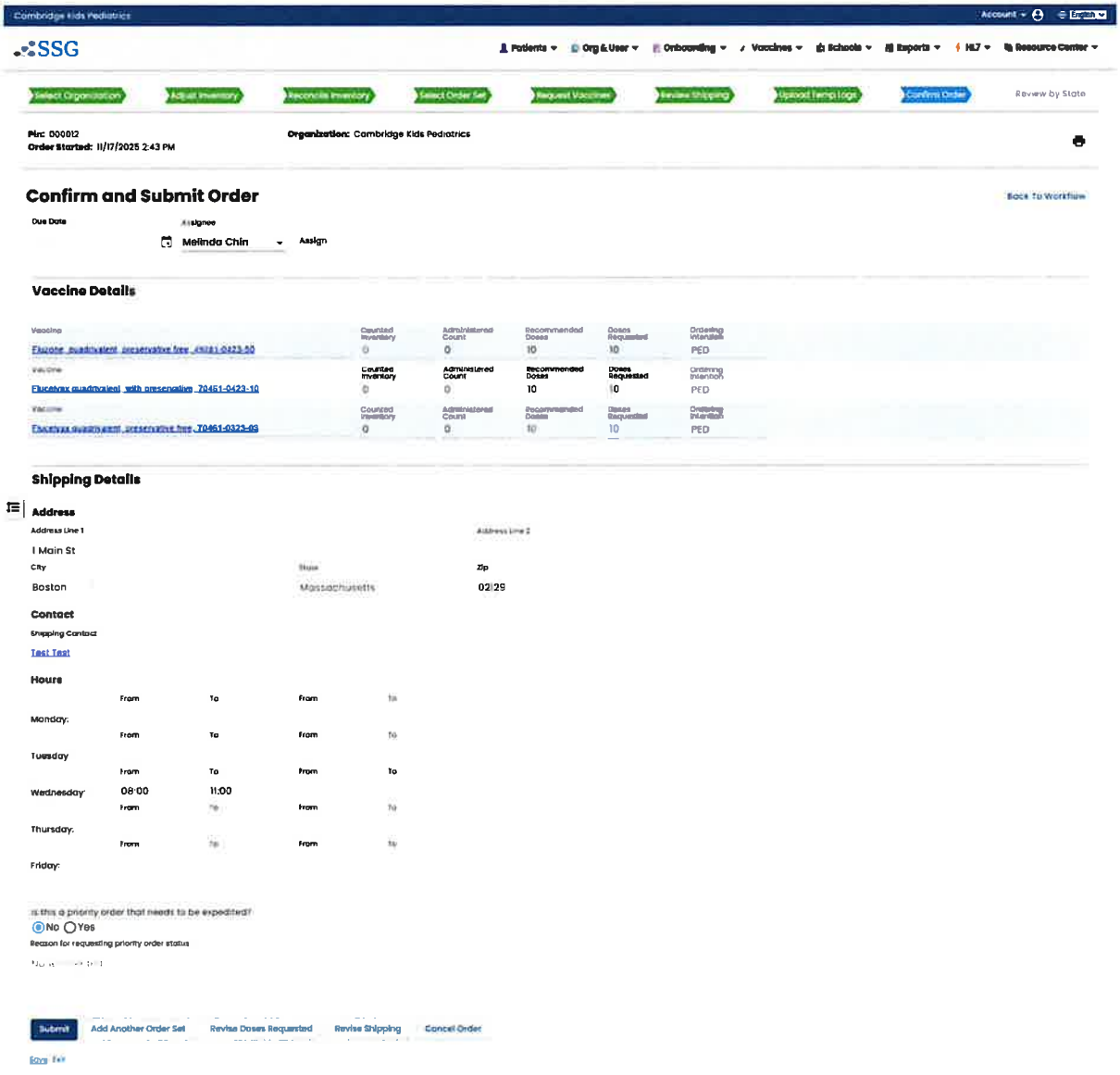
Providers enrolled in Vaccines for Children (VFC) or state vaccine programs place vaccine orders directly through the *Casetivity*-IIS interface. Orders are initiated based on configurable order sets that define allowable products based on the provider's profile. The system supports pre-book vaccines to accommodate seasonal limits and allocation, as well as priority orders when needed. Providers can save unsubmitted orders, edit pre-populated order quantities, and verify contact and order information during the ordering workflow before submission. The system can pre-populate orders with recommended quantities based on current inventory and doses reported as administered to the IIS, helping providers maintain appropriate stock levels.



Order Validation and Compliance

Validations are a core component of Casetivity-IIS workflows. The system allows for configurable requirements and warning rules to ensure that vaccine orders contain complete, accurate, and compliant information before submission. The system can be configured to require inventory

reconciliation as part of the ordering process to ensure providers are maintaining accurate quantities in the IIS. Alert functionality notifies users when reorder recommendation inventory levels are reached.



Order Review and Approval Workflow

Orders undergo a review and approval step managed by designated Department staff. The system supports partial order fulfillment, deferral, and rejection. Department staff can enter funding source for each line item and purchase order numbers. Automatic notifications are sent

to providers notifying them of their order approval status, ensuring transparency throughout the process.

Order Status Monitoring

The system tracks the shipping status of orders and supports the ability to receive vaccine inventory and shipping information. *Casetivity*-IIS can be configured to either automatically receive shipments or require permission-based user action to accept each vaccine product after shipment is received. Role-specific dashboards highlight pending orders and guide providers through necessary compliance actions. The system tracks and manages doses across all lifecycle stages including ordered, on hand, administered, wasted, expired, recalled, returned, and transferred doses.

Integration and Reporting

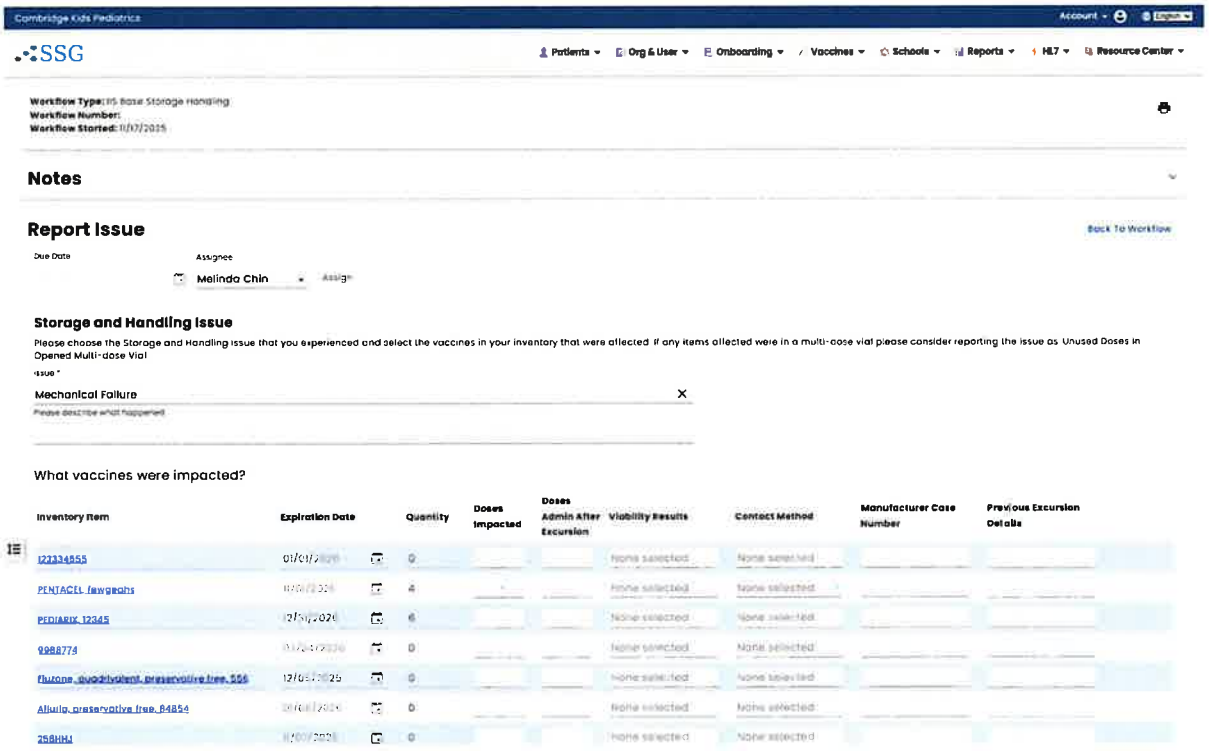
All inventory actions—ordering, receipt, reconciliation, and wastage—are fully logged for auditing purposes. A complete inventory transaction log is available for each inventory line item. The system supports CDC VTrckS integration for vaccine ordering and tracking, and provides ad hoc exports for vaccine inventory reconciliation, accountability, and site visit preparation.

Casetivity-IIS meets the requirement by providing end-to-end vaccine ordering and order status monitoring capabilities that support efficient vaccine program management while maintaining compliance with federal and jurisdictional requirements.

4.2.1.7.2.3. The IIS supports reporting vaccine returns and wastage.

Casetivity-IIS provides comprehensive out-of-the-box functionality to support reporting vaccine returns and wastage. The system enables jurisdictional administrators to modify inventory quantities to reflect wastage and assign reasons for inventory wastage, ensuring accurate tracking and accountability. Providers can electronically document reductions in vaccine inventory due to outgoing vaccine wastage, logging and explaining adjustments including spoilage, breakage, transfer, and returns.

The system generates standard reports that display information about vaccine wastage and returns, supporting federal and jurisdictional vaccine program requirements. All inventory actions—including wastage—are fully logged for auditing purposes, with a complete inventory transaction log available for each inventory line item. This audit trail ensures transparency and supports compliance with CDC reporting requirements and vaccine accountability standards.



Casetivity-IIS also supports comprehensive vaccine inventory reconciliation, enabling providers to track doses across all lifecycle stages including wasted, returned, expired, recalled, and transferred doses. The system provides clear visibility into immunizations that were not successfully deducted from inventory, enabling providers to easily identify, review, and resolve discrepancies. Providers can reconcile their storage unit quantities with the quantities in the IIS system to ensure accuracy across all dose tracking categories.

Casetivity-IIS fully meets the requirement to support reporting vaccine returns and wastage through integrated inventory management, configurable reporting, and complete audit logging capabilities.

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

Casetivity-IIS provides out-of-the-box capability to automatically decrement administered doses from active inventory in real time. The system automatically matches vaccine doses reported as administered to vaccine doses in inventory and decrements them immediately upon administration. This functionality operates through both user interface data entry and HL7 messaging, ensuring that inventory levels remain accurate regardless of how the data enters the system.

When a provider records an administered dose—whether manually through the UI or electronically via HL7 message—*Casetivity*-IIS matches the vaccine information (NDC, lot number, expiration date) to the corresponding inventory line item and automatically reduces the on-hand quantity. Historical doses imported into the system are excluded from automatic decrementing to prevent inaccurate inventory adjustments for vaccines administered before the provider began using the IIS or tracking inventory electronically.

The system provides clear visibility into immunizations that were not successfully deducted from inventory, enabling providers to easily identify, review, and resolve discrepancies within their inventory records. All inventory actions are fully logged for auditing purposes, and a complete inventory transaction log is available for each inventory line item. Providers can reconcile their storage unit quantities with the quantities in the IIS system to ensure accuracy and maintain accountability across all dose tracking categories.

This automated decrementing capability supports accurate vaccine inventory management and reconciliation at both the jurisdictional and provider site levels, reducing administrative burden while maintaining the data integrity required for federal and state vaccine program compliance.

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

Casetivity-IIS supports data exchange with the CDC Vaccine Tracking System (VTrckS) through standards-based, automated integration that complies with current ExIS specifications. The solution supports bidirectional exchange of vaccine ordering, inventory, returns, and wastage data, enabling efficient vaccine program management and inventory accountability. SSG maintains ongoing compliance with evolving CDC requirements by monitoring ExIS specification updates and implementing enhancements necessary to support continued interoperability with VTrckS throughout the system lifecycle.

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/exisfunctionality.html#cdcgenericsection1-exis-functionality.

Casetivity-IIS establishes data exchange with the CDC's Vaccine Tracking System (VTrckS) in full accordance with ExIS (External Information System) specifications published by CDC. The system provides comprehensive bidirectional integration with VTrckS using standard CDC

communication formats and protocols, ensuring compliance with federal standards for vaccine ordering, shipment tracking, and inventory reconciliation.

The solution supports both manual file-based exchange and API-based integration with VTrckS. Manual file exchange capabilities include outbound transmission of Master Data, Provider Orders, Inventory, and Wastage files, as well as bidirectional exchange of Returns data. The API integration can be configured to run on a scheduled basis, enabling real-time or near-real-time synchronization while reducing manual workload and allowing state staff to focus on higher-priority program activities.

Casetivity-IIS maintains alignment with the most current CDC ExIS Specifications and completes updates to ExIS functionality following publication of specification changes. This ensures ongoing compliance as CDC standards evolve and supports seamless vaccine management for public health programs such as Vaccines for Children (VFC).

The automated data exchange capability establishes scheduled, recurring file transmission between the IIS and VTrckS based on CDC requirements and API file specifications. This automation reduces administrative burden, improves data accuracy, and ensures timely synchronization of vaccine ordering and inventory data across systems. The integration comes configured out-of-the-box, supporting rapid implementation and reducing technical risk during system deployment.

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

SSG maintains a structured process for implementing updates to External Information System (ExIS) functionality following the publication of new specifications by the Centers for Disease Control and Prevention (CDC). This process ensures that *Casetivity*-IIS remains compliant with federal vaccine tracking requirements and supports seamless data exchange with the Vaccine Tracking System (VTrckS).

When CDC publishes updated ExIS specifications, SSG evaluates the changes and develops an implementation plan that includes scoping, estimating, and scheduling the required updates. The system's architecture supports configuration-based updates where possible, reducing development time and implementation risk. SSG coordinates with jurisdictional critical partners to understand specific requirements and ensures that updates align with both federal standards and state-specific workflows.

Casetivity-IIS includes interface management tools that support ongoing maintenance and monitoring of data exchange connections. The solution provides administrative controls for

managing interface configurations, monitoring data transmission status, and troubleshooting connectivity issues. These tools enable jurisdictional administrators to oversee ExIS functionality and ensure continuous compliance with VTrckS specifications.

SSG anticipates and supports annual updates aligned with CDC IIS Functional Standards releases. Updates outside the CDC's 90-day IZ Gateway implementation window are evaluated and authorized through the State's standard contract governance and change-order process. SSG accounts for these updates in ongoing maintenance planning and provides a clear approach for scoping, estimating, and implementing future CDC-driven changes.

The configuration benefits of this approach include reduced disruption to daily operations, minimized customization requirements, and faster deployment of federally mandated updates. SSG's maintenance and support services include version upgrades and compatibility assurance for all vendor-supplied components, ensuring continued compliance with CDC and state interoperability standards throughout the contract term.

4.2.1.7.3.3. The IIS establishes automated data exchange with VTrckS.

Casetivity-IIS establishes automated data exchange with the CDC's Vaccine Tracking System (VTrckS) through comprehensive bidirectional integration via the ExIS (External Information System) interface. The system uses standard CDC communication formats and protocols to ensure compliance with federal specifications and enable seamless vaccine management for public health programs.

The solution supports both manual file-based exchange and API-based integration with VTrckS. The API integration can be configured to run on a scheduled basis, automating the exchange process and reducing manual workload for state staff. This automation allows program personnel to focus on higher-priority activities while maintaining real-time or near-real-time synchronization of vaccine ordering, shipment tracking, and inventory reconciliation.

Casetivity-IIS exchanges the following file types with VTrckS in accordance with ExIS specifications:

- Master Data (outbound)
- Provider Orders (outbound)
- Inventory (outbound)
- Returns (outbound and inbound)
- Wastage (outbound)

The system comes configured out-of-the-box to connect with VTrckS and supports the most current CDC ExIS Specifications. SSG completes updates to ExIS functionality following

publication of new specifications, ensuring ongoing compliance with federal standards. This automated integration approach reduces administrative burden, improves data accuracy, and supports efficient vaccine program management across ordering, tracking, and reconciliation workflows.

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.

Casetivity-IIS supports partner and provider onboarding and vaccine management during vaccine-preventable disease outbreaks and public health emergencies through capabilities designed for rapid response, mass vaccination operations, and real-time data exchange. The solution supports expedited partner onboarding, emergency-specific training, mass vaccination event management, offline and field-based vaccination workflows, integration with appointment scheduling tools, and timely reporting to federal and jurisdictional authorities. Combined with resilient infrastructure, emergency preparedness planning, and interoperable data exchange capabilities, *Casetivity*-IIS enables jurisdictions to efficiently manage immunization activities and maintain situational awareness during 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.

Casetivity-IIS supports emergency preparedness and response through a combination of system capabilities, operational flexibility, and partnership with jurisdictional immunization programs to establish and execute emergency plans aligned with federal and state policies.

- *Emergency Preparedness Planning and Coordination:* SSG works in partnership with clients to establish emergency preparedness plans and procedures. The system's technical infrastructure is designed to support rapid response during vaccine-preventable disease outbreaks and public health emergencies, ensuring continuity of immunization data capture, storage, and reporting even under surge conditions. SSG has collaborated with customers to develop and implement disaster recovery and business

continuity plans that align with federal standards, including NIST SP 800-34 guidelines for contingency planning.

- *Rapid Response Capabilities: Casetivity*-IIS enables expedited partner and provider onboarding during emergencies through streamlined communication and data exchange processes. The system supports real-time patient lookup using flexible identifiers such as name, date of birth, address, or phone number, with partial and phonetic matching optimized for field conditions where patient information may be incomplete. Full support for bi-directional HL7 messaging (VXU/QBP) and ADT enables real-time submission and retrieval of immunization data, ensuring continuity of public health reporting to federal and jurisdictional authorities.
- *Mass Vaccination Event Management:* The system includes Mass Vaccination Roster functionality that allows bulk upload of patient lists using Excel templates. Each event can be pre-configured with vaccine types, locations, and staff roles, minimizing administrative overhead and enabling rapid deployment during emergency vaccination campaigns. This capability supports the capture of patient demographic and vaccination data at scale while maintaining data quality and security standards.
- *Infrastructure and Business Continuity:* SSG maintains documented Business Continuity and Disaster Recovery plans that are tested annually and updated based on lessons learned. All backup, failover, and recovery activities comply with U.S.-based data residency requirements, ensuring that emergency response operations maintain the same security and compliance standards as routine operations. The cloud-based architecture provides resilience and availability during critical events, with infrastructure designed for disaster avoidance and rapid recovery.
- *Training and Support:* SSG provides training to onboarded partners during emergency response efforts, ensuring that new users can quickly access and utilize the system's emergency response capabilities. Help desk support with documented escalation procedures ensures that technical issues are resolved promptly, even during high-volume emergency operations.

Through these capabilities and partnership approach, *Casetivity*-IIS establishes, coordinates, and executes emergency preparedness plans and procedures in accordance with federal and jurisdictional policies, supporting effective public health response during vaccine-preventable disease outbreaks and other emergencies.

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.

Casetivity-IIS supports expedited communication and onboarding with partners to capture patient demographic and vaccination data during public health emergencies through built-in capabilities designed for rapid response, secure data capture, and real-time integration.

- *Rapid Patient Lookup and Data Entry:* Providers can conduct real-time searches using flexible identifiers such as name, date of birth, address, or phone number within the user interface. The system supports partial and phonetic matching, optimized for field conditions where patient information may be incomplete or imprecise. This capability enables providers to quickly locate existing records or create new patient entries during high-volume emergency events. Full support for bi-directional HL7 messaging (VXU/QBP) and ADT enables real-time submission and retrieval of immunization data, ensuring that newly onboarded partners can immediately begin capturing and exchanging vaccination information.
- *Mass Vaccination Event Management:* The system supports Mass Vaccination Rosters, allowing bulk upload of patient lists using Excel templates. Each event can be pre-configured with vaccine types, locations, and staff roles, minimizing administrative overhead during emergency response. This roster-based data entry approach enables partners to rapidly document vaccinations for large populations without manual entry for each individual record.
- *Flexible Provider Onboarding and Emergency Program Enrollment:* In response to rapidly changing emergency needs, *Casetivity*-IIS supports fast configuration of new provider types and enrollment workflows for participation in emergency immunization programs. The system enables assignment of appropriate roles, access, and reporting capabilities through role-based access control. Jurisdictional administrators can flag and indicate organization or facility participation in mass vaccination events. Configurable prioritization tiers for provider sites help public health officials categorize providers by priority during vaccine shortages or emergencies.
- *Emergency-Specific Reporting and Surveillance:* The system enables rapid development and distribution of custom reports and dashboards. Role-based dashboards provide visibility into doses administered by date, location, and product; demographics of recipients and patient coverage; and inventory levels and expiration tracking. This real-time reporting capability supports coordination and decision-making during emergency response efforts.

Casetivity-IIS provides a fully integrated, real-time solution to support public health emergency responses. With capabilities for rapid patient lookup, event-based data capture, tracking of

specialized vaccines, and real-time integration, the system ensures that West Virginia can manage immunization campaigns efficiently, accurately, and securely during urgent situations while maintaining compliance with public health reporting standards.

4.2.1.8.1.3. The IIS provides training to onboarded partners.

SSG provides comprehensive training to onboarded partners during emergency response situations through multiple coordinated mechanisms that ensure rapid knowledge transfer and operational readiness. The *Casetivity*-IIS solution supports expedited communication and onboarding with partners to capture patient demographic and vaccination data in an emergency, and training is integrated throughout this accelerated process.

During emergency response situations, SSG delivers training that addresses the specific needs of newly onboarded partners. This training covers accessing the system, generating reports, and interpreting data—capabilities that are essential when partners need to quickly contribute to outbreak response efforts. The training approach ensures that partners understand how to document patient demographic and vaccination data accurately and completely, even under time-sensitive conditions.

SSG's training methodology supports both the technical aspects of system use and adherence to policies and procedures. The solution provides ongoing training to ensure awareness of and promote adherence to established protocols, which is particularly important when new partners are brought online during public health emergencies. Training materials address system administration, forms mapping, and scenario documentation to help partners navigate emergency workflows effectively.

SSG also delivers feedback and training to IIS partners and providers to ensure complete, timely, and accurate patient demographic and vaccination records. This feedback loop is particularly valuable during emergency response situations, as it allows SSG to identify and address knowledge gaps in real time, improving data quality and partner confidence as the response unfolds.

Through these coordinated training and support mechanisms, SSG ensures that partners onboarded during vaccine-preventable disease outbreaks and public health emergencies can contribute effectively to response efforts while maintaining data quality and system security standards.

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

Casetivity-IIS supports vaccine administration functionality during emergencies through rapid patient lookup, mass vaccination event management, and offline documentation capabilities designed for field conditions and high-volume scenarios.

The system enables real-time patient searches using flexible identifiers including name, date of birth, address, or phone number. Partial and phonetic matching capabilities are optimized for field conditions where patient information may be incomplete or imprecise. Providers can conduct searches and create patient records quickly within the user interface, ensuring minimal delays during emergency response operations.

For mass vaccination events, *Casetivity*-IIS supports roster-based data entry through Mass Vaccination Rosters. Authorized users can bulk upload patient lists using Excel templates, with each event pre-configured for vaccine types, locations, and staff roles. This approach minimizes administrative overhead and accelerates data capture during large-scale emergency vaccination campaigns.

The system maintains full support for bi-directional HL7 messaging (VXU/QBP) and ADT for real-time submission and retrieval of immunization data. This interoperability ensures that vaccination records captured during emergencies integrate seamlessly with existing health information systems and public health reporting workflows.

Casetivity-IIS tracks vaccines administered during emergencies, including specialized products such as adjuvanted vaccines, while maintaining compliance with public health reporting standards. The system provides robust tracking capabilities that support accurate inventory management and dose-level accountability even during high-volume emergency operations

These capabilities enable jurisdictions to respond rapidly to public health emergencies, capture accurate immunization data under field conditions, and maintain data quality and reporting compliance throughout emergency response efforts. *Casetivity*-IIS meets the requirement for vaccine administration functionality including offline documentation during emergencies.

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

Casetivity-IIS supports integration with vaccination appointment scheduling tools through single sign-on (SSO) integration and custom interface development. The system can interface with third-party appointment scheduling applications by means of an SSO integration, enabling IIS users to automatically log in to the third-party appointment system without requiring separate

credentials. This streamlined access reduces administrative friction and supports efficient workflow during routine operations and public health emergencies.

For jurisdictions requiring deeper integration or a full scheduling system within the IIS, SSG can develop custom solutions tailored to specific requirements. Development options include viewing and scheduling appointments for patient immunizations within the IIS or within an interfacing application.

This approach provides flexibility to meet jurisdictional needs, whether through lightweight SSO integration for immediate interoperability with existing scheduling tools or through comprehensive custom development for jurisdictions seeking native scheduling capabilities. The solution supports expedited communication and onboarding with partners during vaccine-preventable disease response and public health emergencies, consistent with CDC IIS Functional Standards for emergency preparedness and response.

Casetivity-IIS meets the requirement to support integration with tools for vaccination appointment scheduling through both out-of-the-box SSO capabilities and configurable custom development options.

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

Casetivity-IIS supports public health immunization reporting to federal and jurisdictional authorities during emergencies through real-time data capture, comprehensive reporting capabilities, and bi-directional data exchange. The system ensures rapid, secure, and accurate immunization data flows during critical public health events while maintaining compliance with reporting standards.

The solution enables real-time access to patient records and expedited data entry during emergencies, with robust tracking of vaccines administered—including specialized products such as adjuvanted vaccines. Full support for bi-directional HL7 messaging (VXU/QBP) and ADT facilitates real-time submission and retrieval of immunization data to federal and jurisdictional authorities.

Casetivity-IIS provides emergency-specific dashboards that deliver visibility into doses administered by date, location, and product, along with demographics of recipients and patient coverage. The system supports data extracts required for CDC emergency response monitoring, including COVID-19, RSV, and flu reports. Ad hoc and delivered reports can be generated in multiple formats including PDF, CSV, XLSX, XML, or via direct reporting databases to meet various federal and jurisdictional reporting needs during public health emergencies.

The solution supports Mass Vaccination Rosters for bulk upload of patient lists using Excel templates, with each event pre-configured with vaccine types, locations, and staff roles. This capability minimizes administrative overhead while ensuring accurate data capture for reporting purposes. Rapid patient lookup functionality allows providers to conduct real-time searches using flexible identifiers, with support for partial and phonetic matching optimized for field conditions where patient information may be incomplete.

Casetivity-IIS enables jurisdictions to generate doses administered reports for priority groups during public health emergencies, supporting accountability for publicly purchased vaccine and CDC reporting requirements. The system's configurable prioritization tiers help public health officials categorize providers by priority during vaccine shortages or emergencies, ensuring appropriate resource allocation and reporting visibility.

These capabilities ensure that federal and jurisdictional authorities receive timely, accurate immunization data during emergencies, supporting coordinated response efforts and informed decision-making across the public health ecosystem.

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 IIS participates in modernization initiatives and emerging technologies.

Casetivity-IIS supports and participates in modernization initiatives through a flexible, standards-based architecture, ongoing alignment with CDC IIS Functional Standards, adoption of emerging interoperability technologies, and active engagement in the public health informatics community. SSG coordinates modernization efforts across jurisdictions, incorporates evolving standards such as HL7 FHIR, and leverages lessons learned from multiple public health programs to continuously enhance the platform. This approach ensures that *Casetivity*-IIS remains aligned with current public health priorities while providing a sustainable foundation for future innovation and technology advancement.

4.2.1.9.1.1. The IIS coordinates modernization efforts.

SSG coordinates modernization efforts through a structured approach that aligns *Casetivity*-IIS development with public health modernization priorities and emerging technology standards. The solution's modular, modern architecture enables SSG to participate actively in

modernization initiatives across public health programs while maintaining the flexibility to adapt to evolving requirements and standards.

SSG coordinates modernization by maintaining deep engagement with public health modernization initiatives across multiple program areas. This cross-program understanding informs how SSG plans and executes efforts that align Immunization Information System (IIS) initiatives with broader modernization priorities. The company's work across different public health domains—including disease surveillance, lead poisoning prevention, and early intervention—provides insight into emerging technology patterns and interoperability requirements that extend beyond immunization programs. This perspective enables SSG to design solutions that support not only current IIS functional standards but also future integration requirements as public health systems modernize.

The *Casetivity* platform's low-code architecture supports this coordination by enabling rapid, adaptable delivery of new capabilities as modernization priorities evolve. SSG participates in initiatives to develop standards and capabilities by implementing standards-based functionality while preserving the flexibility to support jurisdiction-specific requirements and enhanced workflows. This approach ensures that modernization efforts remain grounded in proven interoperability standards while accommodating the unique needs of each public health jurisdiction.

SSG's modernization coordination includes anticipating and supporting annual updates aligned with Centers for Disease Control and Prevention (CDC) IIS Functional Standards releases. The company accounts for these updates in ongoing maintenance planning and proposes clear approaches for scoping, estimating, and implementing future CDC-driven changes. This proactive stance ensures that modernization efforts remain synchronized with federal standards while supporting jurisdictional innovation.

Through this coordinated approach, SSG ensures that *Casetivity*-IIS remains adaptable to future requirements and technological advancements, delivering a robust system that supports both current operational needs and long-term modernization goals across public health programs.

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

SSG plans and executes modernization efforts through a structured approach that aligns *Casetivity*-IIS initiatives with evolving public health priorities and emerging technology standards. This approach balances standards-based functionality with the flexibility to support jurisdiction-specific requirements and enhanced capabilities.

SSG organizes modernization planning into four major categories that guide both initial implementation and ongoing evolution: Core IIS Capabilities as defined by the Centers for Disease Control and Prevention (CDC) and articulated in the IIS Baseline Requirements Traceability Matrix (RTM), configurable enhancements to support advanced workflows and tools, data migration to ensure high-quality continuity, and infrastructure setup aligned with cloud and containerization standards. Each category is grounded in domain expertise and a modern low-code architecture that enables rapid, adaptable delivery while preserving long-term value.

The foundation of SSG's modernization execution implements Core IIS Capabilities as outlined in the IIS Functional Model and corresponding IIS Baseline Requirements Traceability Matrix. These core capabilities represent the essential baseline system functionality that all IIS platforms should support. SSG's approach ensures that *Casetivity*-IIS meets federal standards while maintaining the configurability needed to address jurisdiction-specific modernization priorities as they emerge.

SSG coordinates modernization efforts across its client base through consortium engagement. The consortium provides methods for engaging with clients through activities such as monthly consortium calls, enabling jurisdictions to share beneficial system improvements and enhancements. When SSG develops customizations or optimizations through work with one jurisdiction that may be broadly beneficial, those enhancements are evaluated and released to the broader customer base. This collaborative model ensures that modernization investments benefit multiple jurisdictions and that *Casetivity*-IIS evolves in alignment with emerging public health needs.

SSG's modernization execution also incorporates participation in standards development initiatives. The solution is designed to support evolving interoperability standards, including adoption of HL7 Fast Healthcare Interoperability Resources (FHIR) while maintaining HL7 v2.5.1 as the mandatory baseline. This dual-standards approach provides increased flexibility, transparency, and scalability for standards-based immunization data exchange, with a clear methodology and roadmap for FHIR adoption that ensures evolution with federal and jurisdictional priorities.

This structured approach to planning and executing modernization efforts ensures that *Casetivity*-IIS initiatives remain aligned with CDC standards, emerging technologies, and jurisdiction-specific priorities throughout the system lifecycle.

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

SSG actively participates in national and state-level initiatives to develop and advance immunization information system standards and capabilities. This participation ensures that *Casetivity*-IIS remains aligned with evolving public health priorities and federal modernization efforts.

SSG engages directly with the Centers for Disease Control and Prevention (CDC), the American Immunization Registry Association (AIRA), and the Public Health Informatics Institute (PHII) in collaborative efforts to shape IIS functional standards and technical specifications. *Casetivity*-IIS is designed from the ground up to align with the IIS Functional Model developed collaboratively by these organizations, ensuring that the solution reflects current national standards and anticipates emerging public health needs. This alignment enables SSG to contribute informed feedback during standards development cycles and to implement new capabilities rapidly as specifications are finalized.

SSG's approach to standards participation is grounded in operational experience across multiple jurisdictions. By working with diverse state and local immunization programs, SSG gains practical insight into how standards perform in real-world environments. This experience informs SSG's contributions to standards development initiatives, ensuring that proposed standards are implementable, scalable, and responsive to the operational realities of public health agencies. SSG shares lessons learned from implementation and configuration work back to standards bodies, helping to refine specifications and improve interoperability across the national IIS ecosystem.

SSG also participates in modernization initiatives focused on emerging technologies and interoperability standards. The solution's modern low-code architecture enables SSG to evaluate and adopt new technical capabilities as they mature, including support for HL7 Fast Healthcare Interoperability Resources (FHIR) standards alongside the mandatory HL7 v2.5.1 baseline. This dual-standards approach positions *Casetivity*-IIS to evolve with federal and jurisdictional priorities while maintaining backward compatibility and operational stability.

Through this active participation in standards development and modernization initiatives, SSG ensures that *Casetivity*-IIS remains a forward-looking solution that supports both current requirements and emerging capabilities, meeting the requirement for participation in initiatives to develop standards and capabilities related to emerging technologies.

4.2.2 West Virginia Specific Goals & Objectives

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.

SSG evaluates whether a customization or optimization developed for one jurisdiction may be broadly beneficial through a structured, data-informed approach that balances jurisdictional specificity with platform-wide value. This evaluation process ensures that enhancements developed through work with individual clients can be identified, refined, and offered to the broader customer base at no additional cost when they support common public health needs.

SSG's evaluation begins with monitoring how customizations perform in operational use. The solution automatically logs configuration changes, user actions, and system outcomes—including match scores, validation results, and data quality metrics. This data collection provides visibility into how specific customizations address real-world challenges and whether they improve data quality, workflow efficiency, or reporting accuracy. When a customization demonstrates measurable improvement in one jurisdiction, SSG reviews whether the underlying need exists across other jurisdictions.

The evaluation considers several factors: whether the customization addresses a requirement common to multiple jurisdictions, whether it aligns with CDC guidance or national standards, whether it improves core solution capabilities such as deduplication or data validation, and whether it can be implemented through configuration rather than custom code. Customizations that meet these criteria—such as enhanced data quality business rules, configurable match expressions, or improved reporting filters—are strong candidates for platform-wide adoption.

SSG's Software as a Service (SaaS) model supports this approach by enabling broadly beneficial enhancements to be incorporated into the core platform and made available to the broader customer base at no additional cost. When a beneficial customization is identified, SSG incorporates it into the core platform and makes it available to all jurisdictions through annual updates. This ensures that improvements developed through work with one jurisdiction benefit the entire customer base, reducing duplication of effort and promoting consistency across implementations.

The configuration-driven architecture of *Casetivity*-IIS supports this evaluation process. Because deduplication logic, validation rules, and reporting parameters are fully configurable at runtime, jurisdictional administrators can adjust settings based on evolving data patterns or policy changes without requiring code updates. This configurability allows SSG to observe how different configurations perform across jurisdictions and identify which approaches deliver the strongest outcomes. Configurations that prove effective can then be offered as standard options or recommended practices for other clients.

This evaluation methodology ensures that SSG's platform evolves based on real-world operational experience while maintaining the flexibility jurisdictions need to address their specific requirements. By systematically identifying and sharing beneficial enhancements across the customer base, SSG reduces duplication of effort, accelerates time to value, and ensures that all jurisdictions benefit from collective learning and continuous improvement.

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

SSG maintains a collaborative, client-centered approach to releasing system enhancements developed for one jurisdiction to the broader customer base at no additional cost. All clients have full access to enhancements included in applicable releases, ensuring that improvements developed through work with individual jurisdictions can benefit the broader user community.

SSG evaluates whether a customization or optimization may be broadly beneficial by engaging clients directly in the decision-making process. Rather than treating critical partner input as advisory only, SSG reverses the typical decision-making structure used by proprietary systems—clients have not only input but also a stake in determining the functionality of new releases. This collaborative governance model ensures that enhancements align with real-world operational needs across multiple jurisdictions before being incorporated into the platform.

The release process follows a flexible, client-driven cadence. Major upgrades occur twice per year, while minor updates are incorporated into a release schedule determined in partnership with the client. Because *Casetivity*-IIS is built on a low-code platform, the release cycle is driven by the client's product roadmap rather than an artificial calendar. This approach allows

jurisdictions to realize change in a timely manner without dependency on rigid vendor timelines. SSG optimizes release software code packaging to meet the custom needs of each deployment and provides rigorous documentation, making it straightforward for technical team members to conduct installations.

SSG distinguishes between two general types of releases: those that add new functionality to the system and Maintenance Releases used to change configurations within the system. The platform is designed to support zero-downtime deployment for most updates—whether platform-level, solution-level, or configuration—allowing changes to be deployed without taking the system offline. Because customer configurations are separated from base code, base solution updates can be applied without overwriting or undoing local setup. If urgent issues arise, SSG deploys hotfixes in a targeted manner, affecting only the necessary parts of the system.

This release model ensures that all jurisdictions benefit from continuous improvement without incurring additional costs, while maintaining the flexibility and control that public health programs require to meet evolving operational and regulatory requirements.

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

SSG maintains structured governance, release management, and communication procedures to ensure jurisdictions remain informed of available system improvements and enhancements throughout the lifecycle of *Casetivity*-IIS.

SSG communicates release content through a formal, multi-stage documentation process. Immediately after release scope is determined, SSG publishes a Scope Document to inform critical partners of planned improvements. As requirements are defined, SSG publishes a Requirements Document detailing the functional specifications for the release. Once development is complete, SSG creates and publishes Release Notes that summarize functional changes for key critical partners. These Release Notes can also be distributed to end users as part of the rollout, based on jurisdictional preference. SSG also maintains a Known Issues list to communicate any items within the release that are not functioning as originally planned. Together, these four documents—combined with continuous status updates and ongoing communication—ensure that every jurisdiction has timely and accurate information about release content.

Jurisdictional administrators also have direct system-level tools to manage internal communication about system changes. *Casetivity*-IIS provides administrators with the ability to add, edit, and inactivate global messages that are displayed to users upon login. System alerts

can be configured to appear as messages at the top of the screen, on a dashboard, or as email notifications. This capability allows jurisdictions to communicate system updates, new features, or operational changes directly to their user base in a controlled and consistent manner.

This combination of vendor-led release communication and jurisdiction-controlled system messaging ensures that both program leadership and end users remain informed of available improvements, supporting smooth adoption and effective use of new capabilities.

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

SSG provides all clients with full access to all enhancements included in all releases at no additional cost. The company does not require clients to implement every enhancement—if clients prefer alternative approaches or wish to implement particular enhancements independently, SSG supports that flexibility.

The company's approach to enhancements emphasizes client input and shared decision-making. SSG ensures that clients not only provide input but also have a stake in decisions about new release functionality. This reverses the typical decision-making structure used by companies offering proprietary systems, where critical partner input serves only as a mechanism to gather ideas and advice. SSG's model gives clients meaningful influence over the direction of system enhancements.

Recent examples of enhancements shared across all *Casetivity*-IIS clients at no additional cost include:

- Full outbound VTrckS API (Phase 3) integration for real-time inventory and ordering exchange; an automated Temperature Excursion management workflow
- Secure in-system Message Center for jurisdiction-to-provider communications
- Expanded coverage reporting with granular population segmentation.

West Virginia would participate in the same cross-jurisdiction product governance from day one. Another example, for our *Casetivity*-DSS solution, is our enhancement-sharing between Iowa and New Hampshire. Features built for either are shared at no cost to the other.

This approach supports long-term stewardship by ensuring that enhancements align with actual client needs and operational priorities. Clients benefit from continuous system improvements and they retain the flexibility to adopt enhancements on their own timeline or implement custom solutions when preferred.

The SSG Multi-Solution Approach

SSG offers the following solutions on the *Casetivity* platform, enabling reuse across the organization:

- *Casetivity*-EI: Early Intervention Part C Data System
- *Casetivity*-DSS: Electronic Disease Surveillance System
- *Casetivity*-CLPPP: Childhood Lead Poisoning Prevention System
- *Casetivity* LCAP Solutions: Solutions built on the *Casetivity* platform for other public health use cases such as Family Health, Data Cleansing, etc.

Should another program within West Virginia elect to utilize one of these solutions, the State can benefit from the shared *Casetivity* platform architecture and opportunities for reuse across programs.

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.

SSG's approach to HL7 message error management in *Casetivity*-IIS provides jurisdictional administrators with configurable validation rules, real-time error notification, and administrative tools to identify and resolve rejected messages efficiently.

Jurisdictional administrators configure data quality business rules governing incoming HL7 message validation directly within the system. Administrators set validation levels—Error, Warning, or Informational—for data quality checks applied to both HL7 messages and user interface data entry. This configurability allows jurisdictions to align validation strictness with their data quality standards and external system adoption goals. Administrators also create and update data quality reports to monitor validation outcomes over time.

When HL7 messages fail validation, the system returns errors through the acknowledgment (ACK) message to the sending system, providing immediate notification of the issue. Administrators can review HL7 messages within the application, where each validation result—whether Error, Warning, or Informational—is available for review with descriptive detail. This administrative review capability supports troubleshooting and quality monitoring without requiring external tools for routine error identification.

The system includes message validation tools, logging, and configurable error handling to support both initial onboarding of HL7 connections and long-term quality monitoring. SSG collaborates with the Association of Immunization Managers (AIRA) on HL7 requirement alignment and provides HL7 onboarding and troubleshooting support for provider and vendor integrations. This combination of configurable validation rules, real-time error feedback, administrative review tools, and implementation support enables jurisdictions to identify, sort, and resolve rejected HL7 messages efficiently while maintaining data quality standards.

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.

SSG automates the synchronization of CVX (vaccine administered), MVX (vaccine manufacturer), and NDC (National Drug Code) code sets within *Casetivity*-IIS to ensure jurisdictions maintain current, accurate vaccine coding without manual intervention. The solution provides jurisdictional administrators with out-of-the-box functionality to update CVX, MVX, and NDC codes as needed, supporting compliance with CDC standards and enabling seamless interoperability with external systems.

The solution's automated approach reduces administrative burden by eliminating the need for manual code table maintenance while ensuring that vaccine inventory management, clinical decision support, and HL7 message processing rely on the most current coding standards. Jurisdictional administrators retain the ability to review, validate, and apply code set updates through the system's configuration interface, maintaining local control over when changes take effect in the production environment.

This automation supports accurate vaccine tracking, proper dose decrementing from inventory, and reliable data exchange with partners including the IZ Gateway, VTrckS (Vaccine Tracking System), and electronic health record systems. By keeping code sets synchronized with national standards, *Casetivity*-IIS helps jurisdictions maintain data quality, support accurate immunization forecasting per ACIP (Advisory Committee on Immunization Practices) recommendations, and meet federal reporting requirements without ongoing manual code table management.

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

SSG supports efficient bulk management of providers, facilities, and users through a combination of delegated administration, role-based access control, and streamlined enrollment workflows that reduce administrative burden while maintaining data integrity and security.

Bulk Loading and Activation

Casetivity-IIS includes guided workflows for provider enrollment and re-enrollment that enable administrators to manage participation at scale. Vaccine Unit staff or designated state users can open or close enrollment windows, assign or update enrollment statuses in bulk, and guide providers through structured workflows directly within the user interface. The system captures essential provider information including population types, vaccine coordinator and staff training records, storage unit and cold chain details, operational procedures, digital signatures, and contact information. Configurable automated email notifications prompt provider contacts to log in and complete pending enrollment tasks, supporting timely participation across large provider networks.

Delegated Administration Model

Each provider site designates an Access Administrator who can add and deactivate users, assign roles based on local workflows, and monitor user activity within their facility. This delegated model distributes the administrative workload while maintaining centralized oversight. State-level administrators retain authority over global role definitions, jurisdictional access, and system-wide security settings, ensuring secure and structured access across the system.

Deactivation and User Management

The delegated administration framework enables Access Administrators to deactivate users at the facility level as staff roles change or employment ends. State administrators maintain system-wide control to ensure compliance with security standards and public health data privacy requirements. The role-based architecture supports safe delegation of duties across providers, schools, health departments, and system administrators while adapting to dynamic program needs.

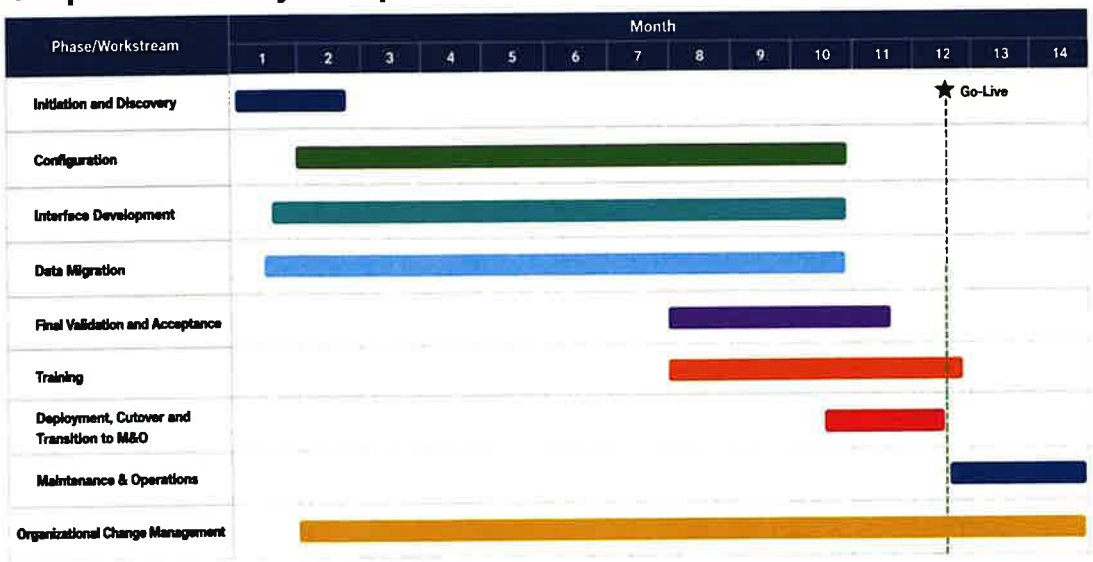
This approach enables jurisdictions to efficiently manage large-scale provider, facility, and user operations through a combination of bulk enrollment management, delegated administration, and automated notifications—reducing manual effort while maintaining data quality and security controls throughout the user lifecycle.

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:

4.2.2.2.1. Overall project management strategy and implementation timeline.

SSG employs a structured, phased project management strategy designed to ensure a seamless transition from the existing IIS to *Casetivity*-IIS while minimizing risk and maintaining operational continuity throughout implementation. The approach balances thorough planning with iterative execution, enabling the State to validate progress at each milestone before advancing to the next phase.

Sample WV *Casetivity*-IIS Implementation Timeline



Project Management Framework

SSG's implementation methodology centers on collaborative governance and milestone-based delivery. Within 30 days of project start, SSG hosts initial planning sessions with the Agency to finalize the project plan and schedule. This collaborative kickoff establishes clear roles and responsibilities for both vendor and client teams, defines communication protocols, and aligns expectations for deliverables and timelines. The finalized Project Plan adheres to the proposed Implementation Plan and requires Agency review and approval before execution begins. Any deviations from the proposed plan are documented, justified, and submitted for Agency approval, ensuring transparency and accountability throughout the project lifecycle.

Phased Implementation Timeline

The implementation unfolds across distinct phases, each with defined objectives and deliverables:

- *Discovery Phase (Months 1-2):* SSG requests a copy of legacy data sources within the first month of project kickoff to initiate gap analysis. This phase includes requirements validation, workflow documentation, and initial system configuration planning. Working sessions during these months establish the foundation for data migration strategy and interface requirements.
- *Environment Setup and Configuration (Months 2-4):* SSG establishes Production, Test, and Development server environments to support parallel workstreams. System configuration and workflow customization proceed based on Discovery phase findings, with jurisdictional administrators able to modify forms, adjust validation rules, and configure business logic to meet State requirements.
- *Data Migration Execution (Months 4-8):* Gap analysis findings are presented beginning four to five months into the project, with working sessions continuing throughout this period. The State reviews two complete rounds of data migration prior to User Acceptance Testing (UAT), enabling validation of data accuracy, completeness, and integrity before production deployment. This iterative approach allows for refinement of migration scripts and resolution of data quality issues in a controlled environment.
- *Interface Migration and Testing (Months 6-9):* Existing interfaces are migrated and tested in parallel with data migration activities. SSG coordinates with external systems to ensure continuity of electronic data exchange with EHRs, VTrckS, vital records systems, and the IZ Gateway.
- *User Acceptance Testing (Months 9-10):* Following successful data migration rounds, the State conducts comprehensive UAT to validate system functionality, workflow alignment, and data accuracy in real-world scenarios.

- *Training, Go-Live and Monitoring (Months 11-13):* The updated system is deployed with continuous performance monitoring to ensure ongoing compliance and operational stability. SSG provides training through train-the-trainer sessions, supports readiness and training efforts during this period. For a period of time after go-live, we provide dedicated resources to address issues and optimize system performance.

West Virginia pays nothing in recurring or subscription fees until the Agency formally accepts the fully implemented system.

Financial and Milestone Governance

SSG does not assess, invoice, or charge the Agency for annual licensing, subscription, hosting, maintenance, or support fees during the Implementation Period. Payment for implementation services is tied exclusively to successful completion of mutually agreed-upon milestones established during initial planning sessions and incorporated into the approved Project Plan. No milestone payment becomes due until the Agency verifies and approves completion of the corresponding milestone. Final implementation payment is made only upon the Agency's formal written Acceptance of the fully implemented IIS solution, and no recurring or annual fees begin or accrue until the system has been accepted.

Risk Mitigation and Contingency Planning

SSG's phased approach incorporates multiple validation checkpoints, enabling early identification and resolution of issues before they impact downstream activities. The two-round data migration strategy prior to UAT provides built-in contingency for data quality remediation. Change request management processes ensure that scope modifications are evaluated, documented, and approved before implementation, protecting timeline integrity and budget predictability.

This comprehensive project management strategy delivers a controlled, transparent implementation that meets the State's requirement for a seamless transition while maintaining accountability at every phase.

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

SSG establishes a multi-environment infrastructure to support secure, controlled implementation and ongoing system operations. The environment setup includes Production, Test, and Development servers configured to enable parallel workstreams, minimize disruption to programmatic activities, and ensure thorough validation before deployment.

- *Development Environment:* SSG provides a dedicated Development environment throughout the contract duration to customize and maintain the solution with minimal disruption to agency operations. This environment includes all necessary components—hardware, software, interfaces, and network specifications—identified and supplied by SSG. The Development environment supports system analysis, design updates, and configuration changes as requirements evolve during implementation.
- *Immediate Sandbox Access:* Within three weeks of contract execution, SSG will have a fully installed version of *Casetivity*-IIS available in a Sandbox environment for Agency staff to access. This early availability allows WVSIIS critical partners to begin exploring the platform's interface, functionality, and configuration capabilities from the outset of the project — reinforcing SSG's commitment to transparency and an implementation approach that is easy for critical partners demonstrating that *Casetivity*-IIS is a production-ready platform, not a system requiring build-out before it can be shown.
- *Testing Environments:* SSG utilizes a Quality Assurance (QA) or Test environment with no real data for functional testing and validation.
- *Configuration and Deployment:* SSG installs and configures software in each environment to meet the specific needs of the jurisdiction. The solution supports efficient rollback of software changes through deployment packages with rollback options, and the zero-downtime deployment model allows most updates—whether platform-level, solution-level, or configuration—to be deployed and rolled back without taking the system offline. Automated testing is integrated into the deployment process using Playwright to ensure application stability when new builds are pushed, with comprehensive regression testing covering major functional aspects of the application.

This multi-environment approach ensures controlled progression from development through testing to production, supports thorough validation at each stage, reduces implementation risk, and maintains system stability throughout the project lifecycle and ongoing operations.

4.2.2.2.3. System configuration and workflow customization.

SSG's approach to system configuration and workflow customization during implementation is designed to deliver a solution that aligns with the Agency's specific workflows, business rules, and data requirements while minimizing disruption and ensuring long-term sustainability.

Hybrid Development and Configuration Model

SSG utilizes a hybrid model that integrates traditional waterfall techniques for discovery phase confirmations and interface design documentation with iterative Agile practices for configuration, development, and quality assurance. This approach provides structure and predictability while maintaining flexibility to adapt to emerging needs. SSG follows waterfall techniques for gathering requirements and creating design documents, then employs an iterative Scrum methodology for configuration, development, and QA activities.

Configuration-First Philosophy

Using *Casetivity* as the base platform, SSG prioritizes configuration over custom development wherever possible. The platform supports extensive configuration capabilities without requiring software development, including workflow configuration for processes such as enrollment, inventory approval, and survey review. Jurisdictional administrators can configure workflows, business logic, field visibility, labels, default values, validation rules, and screen layouts using drag-and-drop editors and intuitive administrative interfaces. This configuration-first approach reduces implementation risk, accelerates delivery timelines, and ensures the Agency retains control over future adjustments.

Phased Implementation Approach

SSG initiates each project with a Project Kick-Off Meeting to introduce project team members and roles, validate the project management approach, and review high-level scope. The implementation follows structured phases including planning and discovery, requirements validation, system analysis and design, environment setup (Production, Test, and Development servers), software installation and configuration, data migration and validation, testing through User Acceptance Testing, and go-live. For each milestone, system components are tested and released only after passing all testing phases.

Comprehensive Configuration Capabilities

Casetivity-IIS provides extensive out-of-the-box configuration options that support jurisdictional customization without custom coding. Administrators can configure interface and layout elements including field visibility, labels, default values, and validation rules. The platform supports dynamic interfaces that respond in real time to context such as user role, enrollment status, or provider type. Dashboard and report customization allows role-based or program-based configurations using drag-and-drop interfaces, with options to configure widgets, charts, filters, and data tiles. Workflow and business logic management supports both structured task flows and ad-hoc overrides to handle exceptions or emergency scenarios, with configurable business logic for processes like order sets, data entry flows, and HL7 validation and translation.

Requirements Management and Validation

SSG employs formal requirements management processes to capture, track, and validate requirements throughout implementation. The team conducts system analysis and design activities to update implementation and integration plans as needed to reflect additional issues and risks that emerge during development. SSG factors user interface and user experience considerations into implementation work to ensure the configured solution supports efficient, intuitive workflows for end users.

Testing and Quality Assurance

SSG's testing approach includes multiple testing phases before application functionality is implemented, with both automated and manual testing conducted throughout the implementation lifecycle. The team follows documented defect management processes and works collaboratively with Agency testing teams to ensure all configured workflows meet requirements and perform as expected in the Agency's operational environment.

Governance and Change Management

SSG assumes that configuration of the existing system to meet the Agency's workflows, business rules, and data requirements is expected and acceptable. The proposal is based on stable scope as defined in the RFQ and referenced documents, with major scope changes addressed through formal change control processes. SSG provides ongoing configuration support through the enhancement configuration pool included in post-go-live years, enabling the Agency to request workflow adjustments and system refinements as operational needs evolve.

This comprehensive approach to system configuration and workflow customization ensures *Casetivity*-IIS is tailored to the Agency's specific operational requirements while maintaining platform stability, supportability, and alignment with industry standards and CDC functional requirements.

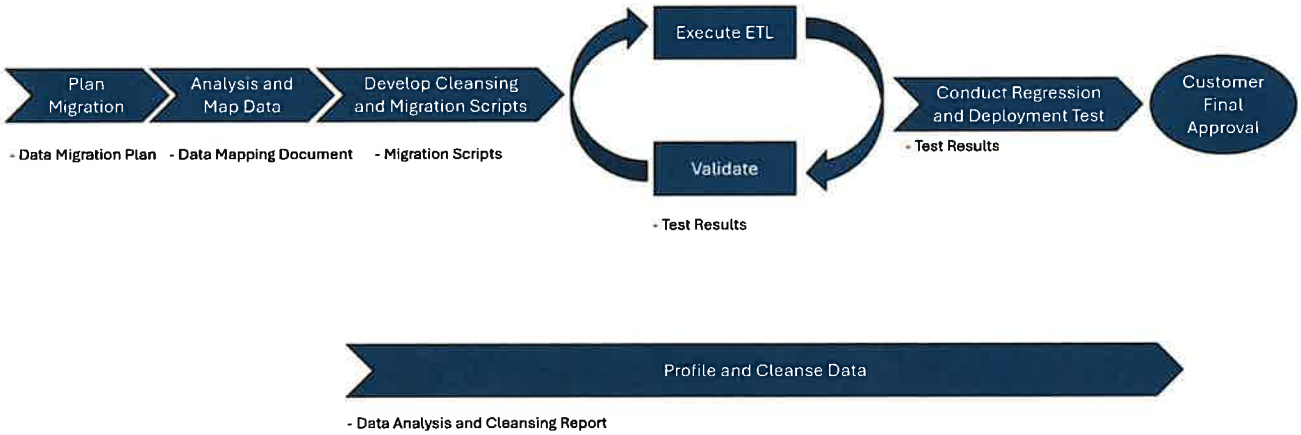
4.2.2.2.4. Data migration strategy, including:

SSG employs a structured, phased data migration strategy that treats migration as a core component of the implementation process. The approach includes data assessment, mapping, transformation, validation, testing, cutover planning, and post-migration verification to ensure the accurate and secure migration of existing IIS data, users and roles, provider and facility records, program enrollments, and interface configurations. Multiple migration test cycles, comprehensive validation activities, and close collaboration with the State help ensure data integrity, continuity of operations, and production readiness while minimizing implementation risk and system downtime.

4.2.2.2.4.1. Existing IIS data migration.

SSG uses a structured, phased approach to data migration that ensures continuity, accuracy, and minimal disruption during the transition to *Casetivity*-IIS. The migration strategy is designed to preserve critical public health data integrity while enabling a seamless cutover from the existing IIS.

The data migration methodology includes initial planning and assessment work, followed by iterative development and testing before a final regression test prior to go-live. The following illustrates this approach followed by information about each phase. Throughout this whole process, WV will have transparent and complete access to all tools, code, configuration, documentation, and data products used during the ETL processes, ensuring full visibility into intermediate and final results.



- **Phase 1: Plan Migration.** Data migration begins with comprehensive planning that establishes the foundation for all subsequent migration activities. During this phase, SSG collaborates with project critical partners to establish the details of the data migration approach, including the work breakdown structure, and clear roles and responsibilities. This effort results in a Data Migration Plan document for review and approval by WV.

  To reduce the burden on our customers, during this phase SSG requests copies of any information readily available that would support the data migration effort. For example, items such as legacy system Data Dictionaries or Database Schemas.

- **Phase 2: Analyze and Map Data.** Using the information gathered during the planning phase, SSG conducts a thorough analysis of legacy data structures and schemas to understand the data architecture. From this, SSG produces a detailed Data Mapping Document that defines the transformation logic for converting legacy data structures to the target system format. The Data Mapping Document will specify mappings such as those for the following: data fields, answer selection values, and user roles.

- **Phase 3: Profile and Cleanse Data.** Data profiling and cleansing activities assess data quality, completeness, and consistency across source systems. SSG understands that data cleansing will be conducted by West Virginia as the owner of the data. If desired, SSG can provide additional data cleansing support, with the scope of such support determined in collaboration with the Agency. This collaborative approach ensures that data transformation aligns with both technical requirements and the State's operational standards.

- **Phase 4: Develop Cleansing and Migration Scripts.** SSG will develop data cleansing and migration scripts based on the documented requirements in the Data Mapping Document and the Data Analysis and Cleansing Report. These scripts will convert legacy data into the target solution format. This includes establishing data migration logic that will be executed through automated ETL tools, ensuring consistency and integrity. The scripts will be delivered to WV and made available at any time for review and use.

SSG uses AI and automation tools to significantly streamline the creation of migration scripts. That efficiency is passed on to customers.
This work does not use any records from data, so maintains confidentiality.

- **Phase 5a: Execute Extraction, Transform, Load (ETL).** During ETL execution, data is extracted from legacy systems, transformed, cleansed, and loaded into the target system using automated methods.

- **Phase 5b: Validate (with de-identified data).** SSG employs a comprehensive, multi-phase testing and validation strategy designed to ensure data integrity, traceability, and full WV visibility throughout the data conversion process. This approach combines structured validation protocols, iterative testing cycles, and transparent reporting mechanisms to deliver measurable confidence in migration outcomes.

  SSG performs rigorous testing through multiple migration test cycles with comprehensive validation to confirm accuracy and completeness of migrated records. During each test cycle, SSG confirms mapping accuracy, transformation logic, and script development. Lessons learned from each test cycle will be incorporated into subsequent runs to improve quality and reduce implementation risk.

  The State plays a critical role in testing and quality assurance to confirm that migrated data meets established standards. SSG validates data accuracy through structured testing protocols and works with State critical partners to verify that all records and data elements have been successfully migrated. This includes confirming completeness, accuracy, and proper mapping of all data elements within patient, provider, facility, organization, user, and program enrollment records.

- **Phase 6: Conduct Regression and Deployment Test (with Production Data).** Upon successful functional and integration tests, a dataset that mimics the size and content of Production data will then be migrated to a secure Certification Environment.

  From a functional perspective, this final test represents a regression test of the data migration and cleansing scripts. After the data is loaded into the Certification Environment, SSG and WV can conduct final testing and UAT.

  During this test, from a data migration script performance perspective, SSG will also capture and monitor the time taken per import batch, general system performance, load metrics, and overall data migration time. This testing cycle will establish the baseline performance results so expectations can be set for the necessary period of time to migrate data to Production. For performance test process, the Certification environment must be set up such that it mirrors the setup of the production environment completely.

- **Phase 7: Customer Final Approval.** SSG will support WV as necessary to provide the final approval on the data migration scripts. Throughout the data migration process, WV will have appropriate end user accounts in the Conversion and Certification environments which will provide transparency and enable User Acceptance Testing (UAT) of the data migration scripts. WV will be able to conduct data validation by exercising the typical business process workflows. SSG will obtain sign-off from the critical partners at this point. After sign-off, a Production import schedule will be developed.

Downtime and Cutover

SSG's migration scripts are structured to run within 24 hours, enabling production cutover to occur over a weekend and avoiding disruption to standard provider workflows. By the time of cutover, scripts have already been validated across multiple test rounds in the Certification environment, so the production window is a controlled execution of a proven process — not a live test.

Roles and Responsibilities

SSG and the State share clearly defined responsibilities throughout the migration process. The State provides legacy data in the agreed-upon format and participates in data cleansing, testing, and quality assurance activities. SSG manages the mapping, conversion, additional cleansing, and technical execution of the migration. Both parties collaborate to ensure data integrity and alignment with operational requirements.

Lessons Learned and Formal Closure

Upon completion of the migration phase, SSG obtains formal approval from critical partners to close the migration and documents lessons learned. This ensures continuous improvement and knowledge transfer for future system enhancements or updates.

SSG's data migration strategy delivers a secure, audited transition that preserves the integrity of immunization records and ensures production readiness from day one. Based on the specification of one legacy data source, SSG estimated the data migration effort to be around 500 hours.

4.2.2.2.4.2. User and roles migration.

SSG's data migration strategy for users and roles is designed to preserve access control integrity, minimize disruption, and ensure continuity of operations during the transition from the existing IIS to *Casetivity*-IIS. The approach leverages SSG's prior experience with secure, audited data migrations and familiarity with legacy system structures to reduce risk and maintain high fidelity throughout the process.

- *User and Role Migration: Casetivity*-IIS supports role-based security standards that align with the existing IIS structure. The system enables jurisdictional administrators to add, modify, and remove access controls based on user roles, and supports assignment of multiple roles to individual users with page-level and field-level permissions. Role hierarchies are preserved during migration, allowing automatic updates to all users

assigned to a role based on changes made to master role attributes. This ensures that existing access patterns, permissions, and organizational hierarchies transfer intact to the new system.

- *Administrative Tooling: Casetivity*-IIS includes robust administrative capabilities to support the migration and ongoing management of users and roles. The Admin Console provides role definition and permission management, audit logging of user activity and configuration changes, and security reports with real-time and historical insights into active and inactive accounts, role hierarchies, access mappings, and login attempt history. Access Administrator roles, managed at the organization level, coordinate user onboarding and role assignments with IIS oversight teams.
- *Testing and Validation:* SSG's methodology includes structured testing to confirm all user and role data has migrated accurately. The two pre-UAT migration rounds allow the jurisdiction to validate that user accounts, role assignments, permissions, and organizational associations are correctly established in *Casetivity*-IIS. Audit logging and security reporting capabilities enable administrators to verify that access controls function as intended and that no users or roles are missing or misconfigured.
- *Timeline and Coordination:* Data migration activities begin within one month of project kickoff and continue through working sessions over the following months. The phased approach ensures that user and role migration is completed, tested, and validated well before go-live, reducing the risk of access-related issues during production deployment.

This strategy ensures that users retain appropriate access to *Casetivity*-IIS from day one, that role-based security controls remain intact, and that jurisdictional administrators have the tools and visibility needed to manage access effectively in the new system.

4.2.2.2.4.3. Provider, Facility, and Organization migration.

SSG's data migration strategy for providers, facilities, and organizations is designed to ensure a complete, accurate, and auditable transition from the existing IIS to *Casetivity*-IIS. The approach leverages SSG's prior experience collaborating with state agencies to perform secure, audited data migrations, reducing risk and shortening timelines while preserving critical public health data integrity throughout the transition.

The migration strategy follows a phased methodology that integrates data migration as a core capability of the implementation process rather than treating it as a separate function. SSG utilizes Extract, Transform, and Load (ETL) tools to execute the migration using established data migration logic. The process includes automated methods for migrating data from source to target systems, ensuring efficiency and consistency across all provider, facility, and organization records.

The migration process includes comprehensive validation to confirm all data has been migrated and to assure the accuracy of records and data elements within those records. SSG's familiarity with operational protocols reduces the risk of data loss or corruption and ensures high fidelity during the transition. The approach addresses data cleansing, mapping, and conversion through clearly defined roles and responsibilities between SSG and the State, with migration timing integrated into the overall project timeline to minimize disruption to ongoing operations.

SSG assumes limited onboarding of new providers during the implementation phase so estimates any support from SSG for this at 150 hours. This activity would support any setup, configuration, and initial operational support for providers not previously enrolled in the IIS. SSG will manage ongoing new provider enrollment post-go-live through standard M&O support.

This strategy ensures that provider, facility, and organization data is migrated completely and accurately, supporting continuity of operations and enabling the State to maintain uninterrupted service delivery throughout the transition to *Casetivity*-IIS.

4.2.2.2.4.4. Program enrollment migration.

SSG's data migration strategy for program enrollments ensures continuity of vaccine program participation records during the transition from the existing IIS to *Casetivity*-IIS. The approach preserves enrollment status, program associations, and historical enrollment data to maintain uninterrupted vaccine program operations.

The program enrollment migration process begins during the Discovery phase, when SSG requests a copy of the legacy data sources to initiate gap analysis. This occurs within one month of project kickoff. Over the following four to five months, SSG conducts detailed analysis and presents findings through working sessions with the State. This structured timeline allows the State to review two complete rounds of data migration before User Acceptance Testing (UAT) begins, typically around the 12-month mark.

SSG brings significant public health data migration and IIS implementation experience to this effort. The SSG team has extensive experience working with complex public health data models, immunization workflows, and large-scale healthcare integrations. *Casetivity*-IIS is designed to align with AIRA and CDC standards, enabling efficient mapping, transformation, and validation of program enrollment data from legacy systems into the new solution. SSG's migration approach emphasizes secure, auditable, and repeatable processes that preserve data integrity, maintain referential relationships, and support continuity of vaccine program operations throughout the transition to *Casetivity*-IIS.

The migration strategy treats data migration not as a separate function, but as a core, integrated capability of *Casetivity*-IIS essential to delivering a complete, production-ready solution. This approach reduces risk, shortens timelines, and ensures high fidelity and accuracy during migration, preserving critical public health data integrity throughout the transition. Program enrollment data is migrated alongside related organizational, facility, and user records to maintain referential integrity and ensure that vaccine program associations remain intact in the new system.

SSG's phased approach includes assessment, planning, implementation, validation, and go-live monitoring phases that span the implementation timeline. Rigorous testing during the validation phase confirms that all program enrollment records have been accurately migrated and that enrollment workflows function correctly in *Casetivity*-IIS. This comprehensive strategy ensures that vaccine program operations continue without disruption and that all enrollment data remains accessible to authorized users in the new system.

4.2.2.2.4.5. Existing Interface migration and testing.

SSG employs a structured, phased approach to migrating and testing existing interfaces from the current IIS to *Casetivity*-IIS. The strategy prioritizes continuity of critical data flows while minimizing disruption to West Virginia's immunization program operations.

Interface Migration Methodology

SSG re-establishes incumbent interfaces and priority connections during the Develop Interfaces phase of implementation. The team focuses first on mission-critical connections including IZ Gateway, Smarty Address Validation, and the ICE forecaster. Additional VXU/QBP connections are implemented as scoped in the project plan. For each interface, SSG delivers interface specifications, test plans, and onboarding playbooks for external partners to ensure clear documentation and smooth transitions.

Testing and Validation Approach

SSG conducts conformance testing using standardized harnesses to ensure compliance with CDC and AIRA standards. The team validates system connectivity prior to the submission of test data and confirms that the transport layer between test sites and the IIS is functional. Interface testing occurs in dedicated environments that mirror production configurations, allowing the team to identify and resolve issues before go-live.

Iterative Data Migration and Interface Coordination

Interface migration is coordinated with the broader data migration strategy. SSG profiles legacy data sources within one month of project kickoff and conducts gap analysis over the following months. The team performs iterative extract-transform-load (ETL) cycles, with each cycle producing reconciliation reports to highlight data quality variances. West Virginia will see two rounds of data migration prior to User Acceptance Testing (UAT), allowing the state to validate both data accuracy and interface functionality in realistic conditions. SSG conducts a cutover rehearsal to ensure readiness before final production deployment.

Deliverables and Documentation

SSG provides Interface Design Documents as formal deliverables. Interface-specific documentation includes specifications, test plans, and onboarding playbooks that support both immediate implementation needs and long-term maintenance. This documentation ensures West Virginia retains full operational knowledge of interface configurations and testing protocols.

This comprehensive approach ensures existing interfaces are migrated systematically, tested thoroughly, and validated against industry standards before production deployment, supporting seamless continuity of West Virginia's immunization data exchange operations.

4.2.2.2.5. Change request management process.

SSG utilizes a structured and systematic change request management process designed to maintain project control while remaining responsive to evolving client needs throughout implementation and post-go-live operations. This process ensures that all critical partners understand proposed changes and their impacts before decisions are made, protecting schedule integrity and budget predictability while supporting necessary adaptations.

Change Control Process During Implementation

SSG establishes a standard Change Control Document at project initiation that defines the complete change management workflow. When a change request is submitted—whether from the State, SSG team members, or other critical partners—the request is documented using a standardized template that captures the nature of the change, the business justification, and

the requestor information. SSG then conducts a thorough impact analysis that evaluates effects on system functionality, project timeline, resource allocation, budget, and interdependencies with other project components. This analysis is documented and presented to the appropriate decision-making authority, typically defined in the Project Management Plan. The State reviews the analysis and makes an informed decision to approve, defer, or reject the change request. Once approved, SSG updates the project plan, schedule, and scope documentation accordingly, and communicates the change and its implications to all affected critical partners.

Governance and Decision Authority

SSG's approach recognizes that clients retain ultimate authority over scope decisions. The change control process is not designed to prevent changes, but rather to ensure changes are made deliberately with full understanding of their consequences. The Project Management Plan establishes clear escalation paths and approval thresholds, ensuring that minor configuration adjustments can be handled efficiently while significant scope changes receive appropriate executive review and sign-off.

Post-Implementation Change Management

After go-live, the change request process continues through SSG's standard maintenance and support framework. Configuration changes, enhancements, and system updates follow the same disciplined approach established during implementation. SSG maintains version control for all system components through the Configuration Management Plan, ensuring that changes are tracked, tested, and deployed in a controlled manner that protects system stability and data integrity.

This structured change management approach balances flexibility with control, enabling the State to adapt the solution to evolving program needs while maintaining project accountability, minimizing risk, and ensuring that all decisions are made with complete transparency regarding their impact on timelines, costs, and system functionality.

4.2.2.2.6. Roles and responsibilities of vendor and client teams.

SSG structures implementation teams with clearly defined roles and mutual accountability to ensure seamless transition from the existing IIS to *Casetivity*-IIS. Both vendor and client teams work collaboratively throughout the project lifecycle, with responsibilities distributed to

leverage each party's expertise while maintaining clear ownership and communication channels.

SSG Vendor Team Roles and Responsibilities

SSG assigns a dedicated project team led by a Project Manager who serves as the single point of contact for all project communications and deliverables. This role ensures on-time completion of all phases and milestones, maintains compliance with contractual requirements and reporting obligations, leads status and quality-review meetings, manages risk and issue resolution processes, and oversees SSG functional leads while coordinating with client program and technical teams.

The vendor team includes specialized roles across implementation, technical, and support functions. The Implementation Lead and Release Manager coordinates system configuration, customization, testing, training, and go-live support tasks. The Data Migration Lead manages the transfer of existing IIS data, users and roles, and provider, facility, and organization records. The Lead Architect and Database Administrator establish and maintain the Production, Test, and Development server environments. The OCM Lead and Training Lead develop and deliver comprehensive role-specific training programs. The Testing Lead and QA Analyst ensure quality assurance throughout configuration and deployment. Functional System Analysts and Business Analysts translate client workflows and business rules into system configuration. Security Advisors ensure compliance with industry standards and jurisdictional requirements. Developers and Low Code Engineers execute system customization and workflow configuration as needed.

SSG also provides executive oversight through an Executive Lead, ongoing relationship management through an Account Manager, and operational continuity through a Maintenance and Operations Manager. A Public Health Subject Matter Advisor brings domain expertise to align the solution with immunization program requirements and CDC standards. The Project Coordinator maintains documentation, tracks deliverables, and supports cross-team coordination.

Client Team Roles and Responsibilities

The client engages a project manager during the system implementation phase who serves as the primary liaison with SSG's Project Manager. This role coordinates internal critical partners, facilitates decision-making, reviews and approves deliverables, and ensures alignment between the implementation and the agency's workflows, business rules, and data requirements.

Client programmatic and technical teams participate actively throughout implementation. Program staff validate requirements, review system configuration to confirm it meets operational needs, participate in user acceptance testing, and provide feedback on training materials. Technical teams coordinate on environment setup, interface development and testing, security reviews, and infrastructure integration. Subject matter experts from the immunization program provide domain guidance on policies, procedures, and CDC compliance requirements.

Collaborative Approach

SSG and the client maintain regular communication through status meetings, quality-review sessions, and acceptance checkpoints. SSG leads the technical implementation while the client provides domain expertise, policy guidance, and operational validation. This partnership model ensures the configured system reflects the agency's specific workflows and meets all functional and regulatory requirements. SSG manages the change-control process with client input and approval, maintaining a deliverable acceptance log to track progress and ensure mutual accountability.

This clearly defined division of responsibilities, combined with structured collaboration and communication protocols, supports successful implementation and positions both teams for effective long-term partnership during the maintenance and operations phase.

4.2.2.2.7. Risk mitigation strategies and contingency planning.

SSG's risk mitigation and contingency planning approach for IIS implementation is structured around proactive identification, transparent communication, and proven response strategies developed through large-scale public health deployments.

SSG recognizes that large-scale public health implementations inevitably encounter unexpected challenges and plans for this reality rather than minimizing it. The approach centers on partnering with clients to resolve issues quickly and transparently, whether challenges involve data quality, interface dependencies, or evolving federal requirements. SSG brings the experience and flexibility to respond effectively to implementation risks.

A key area of potential risk involves managing dependencies with external partners, such as Electronic Health Record (EHR) vendors, Health Information Exchanges (HIEs), and CDC services like IZ Gateway. These connections often involve varying standards, uneven data quality, and external schedules. SSG mitigates this risk through proven strategies including conformance

validation tools, interface playbooks, phased onboarding, and strong critical partner communication.

SSG's implementation approach is structured around risk mitigation and phased implementation, organized into two high-level configuration phases and a parallel data migration track. This phased structure allows for controlled deployment, early identification of issues, and iterative refinement before full production deployment.

For legacy data quality and reconciliation complexity—a common risk that can cause delays and incorrect records—SSG employs early profiling, iterative conversions, automated reconciliation, and targeted data cleanup sprints. The Data Migration Lead owns this risk area and applies these mitigation strategies throughout the implementation period.

SSG's Pre-Implementation Setup phase establishes the foundational project framework, confirms shared understanding of scope and priorities, and prepares the technical and organizational environment necessary for successful implementation. This stage includes formal governance alignment and discovery workshops to validate scope and high-level requirements, reducing the risk of misalignment or scope gaps.

The approach balances standards-based functionality with the flexibility to support unique public health priorities and enhanced functionality requirements. SSG organizes implementation into clearly defined categories—Core IIS Capabilities, configurable enhancements, data migration, and infrastructure setup—each grounded in domain expertise and modern architecture that enables rapid, adaptable delivery while preserving long-term value.

This comprehensive risk mitigation and contingency planning approach ensures that potential implementation challenges are anticipated, managed proactively, and resolved through structured processes and clear accountability, supporting a seamless transition to the new IIS.

4.2.2.2.8. Training, support, and knowledge transfer during implementation.

SSG's comprehensive training approach is designed to ensure that all user groups—from Agency staff and trainers to clinical providers, schools, childcare facilities, and members of the general public—achieve full proficiency with the IIS solution and maintain that proficiency. This approach combines proven instructional methodologies, role-specific learning journeys, and ongoing knowledge transfer to drive sustained adoption and operational continuity.

Training Philosophy and Design Principles

SSG's training program is built on a user-centered foundation that accommodates diverse learning styles and preferences. SSG recognizes that some users learn best through reading

materials, others through listening to presentations, and still others through hands-on practice that allows immediate application of new skills. All training materials and delivery methods are designed to be accessible and compliant with WCAG 2.2 standards, ensuring that every user can effectively engage with the content regardless of ability.

Trainers actively solicit and incorporate user feedback throughout the training process, creating an interactive learning environment that responds to real-world needs and challenges. This approach ensures that training remains relevant, practical, and directly applicable to users' daily responsibilities.

SSG will provide a dedicated training environment during the initial implementation and during all the Maintenance and Operations phase.

Training Approach During Implementation

SSG develops tailored learning journeys for key program areas, working collaboratively with WV to define the specific competencies required for each role. Representative training groups include:

- Agency Staff Trainers—equipped to train external interested parties including clinical, school, and childcare users
- Help Desk personnel—prepared to provide technical assistance and troubleshooting support
- Data Exchange specialists—trained on interface management and data quality assurance
- School Law administrators—focused on school immunization reporting and compliance
- Immunization Quality Improvement Program (IQIP) staff—trained on assessment and evaluation capabilities
- IIS Technical staff—provided with advanced system administration and configuration knowledge
- System Administrators—equipped with operational and maintenance expertise
- General Agency Staff—trained on core system functionality relevant to their roles
- Consumer/General Public—enabled to effectively utilize the Public Portal

Each learning journey is customized based on the audience type (casual users, power users, or specialty users) and their specific interaction model with the system. For example, clinical users who enter data directly into the system receive more extensive hands-on training, while data exchange users who primarily query information receive focused instruction on search and reporting capabilities.

SSG develops comprehensive training materials including on-demand video instructions and demonstrations for each user role, as well as digital user guides and manuals for both functional and technical reference. These materials are designed to support both initial learning and ongoing reference needs.

The training program addresses all core system functions including patient and immunization record management, vaccine inventory operations, data quality monitoring, reporting and analytics, interoperability workflows, and role-based access controls. SSG also provides specialized training for emergency preparedness scenarios, supporting expedited onboarding of partners during vaccine-preventable disease outbreaks or public health emergencies. This ensures the jurisdiction can rapidly scale operations when needed while maintaining data quality and security standards.

Post-Implementation Support

Following go-live, SSG provides a defined period of enhanced dedicated support to resolve user adoption issues and ensure smooth transition to full operational use. This elevated support level addresses the natural learning curve as users begin working with the system in production environments. Help desk support is available Monday through Friday, 8:00 AM to 5:00 PM local time, with documented escalation procedures to ensure timely resolution of issues. SSG maintains system performance monitoring and proactive issue resolution for the hosted environment, addressing potential problems before they impact users.

Knowledge Transfer and Sustainability

SSG's knowledge transfer approach ensures West Virginia develops internal expertise to manage and optimize the system over time. This includes training jurisdictional administrators on system configuration, user and organization management, data quality rule adjustment, and report customization. SSG provides annual or on-demand refresher training modules and updated documentation to cover new system features, version upgrades, and changes to federal or jurisdictional standards. This ongoing education ensures the jurisdiction remains current with evolving immunization program requirements, including updates aligned with CDC IIS Functional Standards releases and Advisory Committee on Immunization Practices (ACIP) recommendations.

Training materials are updated to reflect system changes, ensuring documentation remains accurate and relevant throughout the contract term. SSG's approach emphasizes building sustainable operational capacity within the jurisdiction, reducing long-term dependence on vendor support while maintaining access to expert assistance when needed.

This comprehensive training, support, and knowledge transfer strategy ensures West Virginia achieves successful implementation, smooth operational transition, and sustained system optimization throughout the contract lifecycle.

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.

Casetivity-IIS supports the ability to record vaccine exemptions by vaccine or disease category out of the box. The system can be configured to make exemptions disease-specific, allowing jurisdictions to align exemption tracking with their specific public health and school-entry compliance requirements.

The system captures exemption information at the patient level and links it to specific vaccines or disease categories based on jurisdictional configuration. This capability supports accurate tracking of which vaccines a patient is exempt from receiving, whether the exemption applies to a single vaccine (such as MMR) or to a broader disease category (such as all measles-containing vaccines). Authorized users can record exemptions during patient record management workflows, ensuring exemption status is documented alongside demographic and immunization data.

Casetivity-IIS generates standard reports displaying vaccine exemption rates, enabling public health staff to monitor exemption trends by vaccine type, disease category, and other demographic or geographic factors. The system also produces exclusion letters that identify which vaccines a student needs to come into compliance with school-entry requirements, supporting enforcement of immunization policies while respecting documented exemptions. Additionally, the system generates reports of patients declining or refusing vaccinations, providing visibility into exemption patterns and supporting targeted outreach and education efforts.

This functionality enables jurisdictions to maintain accurate exemption records, support school and childcare compliance reporting, and assess exemption rates across populations—meeting both operational and regulatory requirements for vaccine exemption management.

4.2.2.3.2. Support for exemption types: permanent, temporary (with expiration date), and provisional (with review date).

Casetivity-IIS supports all three exemption types required for comprehensive vaccine exemption management: permanent, temporary with expiration date, and provisional with review date. This functionality enables jurisdictions to accurately track and manage exemptions in accordance with state policy and school-entry compliance requirements.

The system allows authorized users to record permanent exemptions for individuals who have ongoing medical or other qualifying conditions that preclude vaccination. For temporary exemptions, *Casetivity*-IIS supports the entry of expiration dates, enabling the system to track when an exemption period ends and the individual may need to resume vaccination or renew their exemption status. Provisional exemptions can be recorded with review dates, allowing jurisdictions to flag records that require periodic reassessment or follow-up action.

This capability integrates with the system's broader exemption tracking functionality, which links exemption records to patient demographics and supports reporting by exemption type. The expiration date and review date fields enable automated tracking and reporting workflows, helping immunization programs and school health officials identify students whose exemption status requires attention. Jurisdictional administrators can configure exemption workflows to align with state-specific policies and review processes.

Casetivity-IIS meets the requirement for supporting permanent, temporary, and provisional exemption types, providing the flexibility and data integrity needed for effective exemption management and compliance reporting.

4.2.2.3.3. Support for exemption reasons: medical, religious, philosophical.

Casetivity-IIS supports the full range of exemption reasons required for comprehensive vaccine exemption tracking and reporting, including medical, religious, and philosophical exemptions. This capability enables jurisdictions to accurately document and report exemption data in alignment with state policies and school-entry compliance requirements.

The system provides out-of-the-box functionality to generate reports of student exemptions by type, including medical and religious exemptions. This reporting capability is available as standard functionality within *Casetivity*-IIS. Authorized users can generate exemption reports that support school compliance monitoring, public health surveillance, and jurisdictional reporting requirements.

Casetivity-IIS also supports the generation of exclusion letters that identify which vaccines a student needs to come into compliance with requirements and be permitted to attend school. This functionality streamlines communication between schools, parents, and healthcare providers while supporting enforcement of immunization requirements.

The exemption tracking and reporting capabilities integrate with the system's broader school roster functionality, enabling jurisdictions to monitor exemption patterns by school, grade, and district. This integration supports longitudinal tracking of exemption trends and helps identify populations that may be vulnerable during disease outbreaks.

SSG's approach ensures that exemption data is linked to patient demographics and can be configured to meet jurisdiction-specific workflows and review processes. This flexibility allows the system to adapt to evolving state policies while maintaining consistent, accurate exemption records that support both compliance monitoring and public health decision-making.

4.2.2.3.4. Linkage of exemption records to patient demographics (e.g., age, race/ethnicity, geography).

Casetivity-IIS links exemption records to patient demographics through its integrated patient record management system, which stores comprehensive demographic information including age, race/ethnicity, and geographic location as part of each patient's core record. When an exemption is recorded in the system, it is associated directly with the patient's demographic profile, enabling jurisdictional administrators and authorized users to analyze exemption patterns across demographic dimensions.

The system captures country of birth, address information with geocoding support, and configurable demographic data elements that can be tailored to meet jurisdictional requirements and privacy policies. Geographic linkage is supported through address standardization per US Postal Service conventions and geocoding functionality, which enables mapping and statistical reporting by location. This geographic association allows exemption data to be analyzed by county, district, school, or other jurisdictional boundaries defined in the system's configurable geographic hierarchy.

Report parameters such as age and geographic location enable identification and filtering of patient populations, including those with exemptions. Administrators can define additional parameters to support exemption reporting by school, grade, district, exemption type, and compliance status. The system's role-based access control ensures that only authorized users

can access linked demographic and exemption data, maintaining confidentiality while supporting public health reporting and school-entry compliance tracking.

This linkage supports longitudinal tracking of exemption trends across demographic groups and enables jurisdictional programs to identify vulnerable populations, assess coverage gaps, and generate reports that inform targeted outreach and policy decisions. *Casetivity*-IIS meets the requirement to link exemption records to patient demographics including age, race/ethnicity, and geography.

4.2.2.3.5. Reporting capabilities by school, grade, district, exemption type, and compliance status.

Casetivity-IIS provides comprehensive reporting capabilities for vaccine exemptions that support school compliance monitoring, public health analysis, and jurisdictional oversight. The system generates exemption reports by type—including medical and religious exemptions—and supports filtering and analysis across multiple dimensions to meet federal and jurisdictional reporting requirements.

The system provides out-of-the-box functionality to generate reports displaying vaccine exemption rates. These reports provide visibility into exemption patterns and support compliance tracking for childcare, school, and college settings. *Casetivity*-IIS captures exemptions at the patient or student level, with the ability to associate exemptions with specific vaccines when relevant. This granular data capture enables detailed analysis of exemption trends by vaccine series, exemption type, and student population.

For school-specific reporting, *Casetivity*-IIS supports uploading lists of patients or students and returns School Compliance reports when patient matches are found in the system. These reports display a count of students who have met each vaccine series, have exemptions, or have no records on file. The School Compliance report provides a summary of student immunization data with all vaccine series listed, enabling school administrators and public health officials to quickly assess compliance status at the individual school level. The system also generates exclusion letters stating which vaccines a student needs to come into compliance with requirements and be permitted to attend school.

The system provides access to data for assessing vaccination coverage and identifying vulnerable populations. Jurisdictional administrators can generate reports that provide information about students and their immunization histories for school compliance purposes.

These reporting capabilities enable users to access coverage reports without assistance from IIS staff, supporting efficient compliance monitoring and public health surveillance.

Casetivity-IIS meets the requirement for reporting vaccine exemptions by exemption type and compliance status, with school-level reporting available out of the box and additional customization options available to support jurisdiction-specific reporting needs across grade levels and districts.

4.2.2.3.6. Integration with school roster functionality and support for longitudinal tracking.

Casetivity-IIS integrates vaccine exemption tracking with school roster functionality and supports longitudinal tracking through a roster-based approach that links students to schools and enables compliance monitoring over time.

The system supports uploading student lists via Excel templates, which are then matched against patient records in the IIS. When matches are found, the system generates School Compliance reports that display exemption status alongside immunization records at the individual school level. These reports include counts of students who have met each vaccine series, have exemptions on file, or have no records. The School Compliance report displays a summary of student immunization data with all vaccine series and exemption information listed together, enabling school administrators to assess compliance status across their student population.

Roster integration allows exemption records to be linked to patient demographics and school enrollment information, supporting targeted reporting by school, grade, and county. This linkage enables the jurisdiction to identify geographic and demographic gaps in immunization coverage and track exemption patterns across different student populations. The system supports registration of public and private schools, non-registered facilities, and school districts, and can initiate scheduled school immunization surveys for preschool, kindergarten, grades seven and 12, and college populations.

For longitudinal tracking, the system maintains exemption records as part of the patient's immunization history, allowing authorized users to monitor exemption status over time as students progress through grade levels. The Mass Vaccination Roster functionality supports bulk upload and roster-based data entry, which can be extended to track exemption status during school enrollment periods or compliance review cycles. Dashboards track survey responses,

compliance status, and coverage metrics, providing visibility into exemption trends across schools and over time.

This integrated approach reduces administrative burden for school nurses and health officials while supporting compliance with immunization requirements in childcare, school, and college settings. The system's ability to link exemption data to school rosters and generate compliance reports without IIS staff assistance enables the jurisdiction to monitor exemption patterns, assess compliance rates, and identify students requiring follow-up for school entry requirements.

4.2.2.3.7. Configuration options for jurisdiction-specific exemption workflows and review processes. Allowing administrators to review, approve, or reject submitted exemption requests for all exemption types supported by the system.

Casetivity-IIS provides jurisdictional administrators with comprehensive configuration capabilities to tailor exemption workflows and review processes to meet jurisdiction-specific policies and operational requirements. These configuration options enable administrators to align the system with local laws, public health priorities, and school-entry compliance procedures without requiring custom development.

Jurisdictional administrators can configure authorization agreements and user agreements to reflect jurisdictional policy. The system supports configuration of data elements included for each jurisdiction, including address granularity, demographic data based on privacy sensitivity, and other jurisdiction-specific settings. This flexibility extends to exemption management, allowing administrators to define how exemption data is captured, validated, and reviewed according to local requirements.

In addition to configurable exemption workflows, *Casetivity*-IIS supports an administrative review process for exemption requests. Authorized users can review submitted exemption requests for all exemption types supported by the system and take appropriate action based on jurisdictional policy. Administrators can approve or reject exemption requests, and the system records the outcome as part of the exemption record. All review activities are captured in the audit log, including the reviewing user, action taken, date and time, and any associated comments, providing a complete history of the exemption review process.

Administrators can adjust data quality business rules for exemption-related data validations in both HL7 messaging and the user interface. This includes setting validation levels as Error, Warning, or Informational, ensuring that exemption data meets jurisdictional standards for

completeness and accuracy. Administrators also can create or update data quality reports specific to exemption tracking and compliance monitoring.

The system supports configurable match and merge logic based on source trust levels, which applies to exemption records linked to patient demographics. This ensures that exemption data remains accurately associated with individual patient records even when demographic information is updated or records are merged. Role-based access controls can be configured to restrict exemption data access to authorized personnel based on user roles, organization jurisdiction, and data sensitivity.

For school-entry compliance workflows, administrators can configure business rules that govern how exemptions are processed, reviewed, and reported. The system's audit logging capabilities track all actions related to exemption records, including data views, edits, and report generation, with user ID, role, and timestamp information. This supports accountability and enables administrators to monitor compliance with jurisdictional review processes.

These configuration capabilities enable jurisdictions to implement exemption workflows that align with local policies while maintaining data quality, security, and reporting requirements for public health analysis and school compliance tracking.

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).

Casetivity-IIS supports the definition and documentation of demographic populations used for immunization rate calculations through comprehensive coverage reporting capabilities that

enable jurisdictions to establish both numerators and denominators for rate analysis. The system provides predefined and ad hoc assessment and coverage reports that authorized users can generate independently without requiring assistance from SSG staff, ensuring timely access to population-level immunization data.

The solution enables jurisdictions to define demographic populations using multiple configurable parameters. Users can establish population cohorts by user-defined geographic areas, age range, vaccine type, and patient cohort. The system supports jurisdictional filtering by state, county, and other geographic boundaries, allowing public health programs to align population definitions with their specific reporting requirements and public health priorities. Coverage reporting supports analysis by multiple demographic dimensions, including ethnicity and age range, enabling comprehensive assessment of immunization coverage across different population segments.

Casetivity-IIS generates reports that reflect complete vaccine series, initiation of series (one or more doses), and final dose needed to complete a series. This functionality supports accurate numerator calculation by identifying individuals who meet specific immunization milestones within defined populations. The system includes standard predefined coverage reports available out-of-the-box, including Standard Childhood Coverage Report, Standard Adolescent Coverage Report, Adolescent 13–17-Year-Old Coverage Report, Flu Coverage Report, COVID-19 Coverage Report, Standard Childhood Master Rate Comparison Report, Standard Adolescent Master Rate Comparison Report, and CDC AFIX Report. All reports can be run on-demand by authorized users and include only patient data the user has permission to view, ensuring appropriate data governance.

The solution provides access to data to assess vaccination coverage and identify vulnerable populations, supporting denominator definition through comprehensive demographic data capture. The system contains complete and timely demographic and immunization data for children, adolescents, and adults residing or immunized within the jurisdiction. The technical infrastructure securely captures, stores, and processes patient demographic and vaccination data consistent with established policies and procedures, ensuring data quality and completeness for accurate rate calculations.

Casetivity-IIS supports the identification, prevention, and resolution of duplicate and fragmented patient demographic and vaccination data in accordance with policies and procedures. This data quality functionality ensures that both numerator and denominator calculations reflect accurate, deduplicated patient counts, improving the reliability of coverage rate reporting. The system's configuration options allow jurisdictions to customize report

parameters and align with CDC and state-defined coverage metrics, ensuring that population definitions and rate calculations meet federal and jurisdictional reporting requirements.

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

Casetivity-IIS provides comprehensive jurisdictional filtering capabilities that enable users to generate coverage reports by state, county, and other geographic boundaries. The system supports the establishment of a geographic jurisdictional hierarchy that allows users to define and organize geographic areas according to their operational structure. Once configured, users can generate coverage reports across these hierarchical levels without requiring assistance from SSG staff.

County organizations with user-level based access can independently generate reports for user-defined geographical areas. The system assigns different roles to users and provides access through those assigned roles to various reports with county filters that can be utilized to restrict data to particular geographic areas. This role-based approach ensures that users see only the patient data they have permission to view while maintaining the flexibility to analyze coverage within their jurisdictional boundaries.

The solution includes both predefined standard coverage reports and ad-hoc reporting functionality. Standard reports available out-of-the-box include Standard Childhood Coverage Report, Standard Adolescent Coverage Report, Adolescent 13–17-Year-Old Coverage Report, Flu Coverage Report, COVID-19 Coverage Report, Standard Childhood Master Rate Comparison Report, Standard Adolescent Master Rate Comparison Report, and CDC AFIX Report. All reports support filtering by user-defined geographic areas, enabling public health officials to analyze immunization coverage at the state, county, or other geographic levels relevant to their program needs.

For users requiring more specialized analysis, *Casetivity*-IIS offers a personalized report option where SSG provides various filter options for each report. Users can save their own filter choices, eliminating the need to re-enter parameters each time they run a report. This capability streamlines routine reporting workflows while maintaining the geographic specificity required for jurisdictional public health analysis.

Casetivity-IIS meets the requirement for jurisdictional filtering by state, county, and other geographic boundaries through its hierarchical geographic configuration, role-based access controls, and flexible reporting tools that support both standard and customized coverage

analysis.

4.2.2.4.3. Ability to generate reports reflecting:

4.2.2.4.3.1. Complete vaccine series.

Casetivity-IIS generates coverage reports that reflect complete vaccine series completion through both predefined standard reports and configurable ad-hoc reporting capabilities. The system includes a Standard Childhood Coverage Report and a Standard Adolescent Coverage Report, both of which assess whether patients have completed full vaccine series according to Advisory Committee on Immunization Practices (ACIP) recommendations. These reports evaluate immunization coverage by vaccine type and series completion status, allowing authorized users to identify populations that have finished recommended vaccination schedules.

The solution also provides Custom Coverage reports that enable users to define their own coverage criteria for vaccine series completion. Users can specify the doses needed for each vaccine group of interest and configure report parameters to align with Centers for Disease Control and Prevention (CDC) and state-defined coverage metrics. All coverage reports include filter options by geographic area, race, ethnicity, and Vaccines for Children (VFC) eligibility, supporting targeted analysis of series completion rates across different population segments.

Authorized users generate these reports on-demand through the system's no-code/low-code reporting interface without requiring technical intervention from SSG staff. This self-service capability ensures that immunization program staff can access timely data to assess vaccination coverage, identify vulnerable populations with incomplete series, and support quality improvement initiatives. The reporting functionality operates out-of-the-box and supports the jurisdiction's ability to monitor complete vaccine series completion in accordance with federal and jurisdictional reporting requirements.

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

Casetivity-IIS provides comprehensive coverage reporting capabilities that include the ability to generate reports reflecting initiation of a vaccine series, defined as one or more doses administered. This functionality supports public health programs in identifying populations that have begun but have not yet completed recommended immunization schedules, enabling targeted outreach and intervention strategies.

The system includes predefined Standard Coverage Reports that assess series initiation across key age groups and vaccine types. Authorized users can generate Standard Childhood Coverage

Reports, Standard Adolescent Coverage Reports, and Adolescent 13–17-Year-Old Coverage Reports on demand without requiring assistance from SSG staff. These reports are designed to align with public health program requirements and can be filtered by user-defined parameters including geographic area, age range, race, ethnicity, and Vaccines for Children (VFC) eligibility status.

In addition to predefined reports, *Casetivity*-IIS offers ad-hoc Custom Coverage reporting capabilities that allow authorized users to define their own coverage criteria for various vaccine groups. Users can specify the doses needed for each vaccine group of interest and generate reports that reflect series initiation based on their program-specific definitions. This flexibility ensures that jurisdictional programs can assess coverage according to both federal standards and state-defined metrics.

All coverage reports are accessible through the system's no-code/low-code reporting interface, enabling authorized users to independently generate, filter, and export reports for program decision-making and population health planning. Reports display only patient data that users have permission to view, ensuring compliance with role-based access controls and data privacy requirements. This self-service reporting capability reduces administrative burden on SSG staff while providing timely access to actionable immunization data for coverage assessment and quality improvement initiatives.

Casetivity-IIS meets the requirement to generate coverage reports reflecting initiation of a vaccine series through both standardized and customizable reporting tools that support independent, on-demand analysis by authorized public health users.

4.2.2.4.3.3. Final dose needed to complete a series.

Casetivity-IIS generates coverage reports that reflect the final dose needed to complete a vaccine series. The system's coverage reporting capabilities allow authorized users to assess immunization status for patients who require additional doses to complete recommended vaccine series.

The solution provides both predefined and ad-hoc coverage reporting tools that support this requirement. Standard predefined coverage reports include the Standard Childhood Coverage Report, Standard Adolescent Coverage Report, Adolescent 13–17-Year-Old Coverage Report, Flu Coverage Report, COVID-19 Coverage Report, and CDC AFIX Report. These reports display immunization coverage by vaccine type and identify patients who need final doses to achieve series completion.

The system also offers Custom Coverage reports through a no-code/low-code reporting interface. Users can define the doses needed for each vaccine group of interest and generate reports that identify patients requiring final doses. All coverage reports include filter options such as geographic area, race, ethnicity, and VFC-eligibility, enabling targeted identification of populations needing series completion.

Authorized users can generate these reports on-demand without requiring technical intervention from SSG staff. This self-service capability supports timely identification of patients needing final doses and enables providers to take action to improve series completion rates. The configuration options allow alignment with CDC and state-defined coverage metrics, ensuring reports meet federal and jurisdictional reporting requirements.

Casetivity-IIS meets the requirement to generate coverage reports reflecting the final dose needed to complete a vaccine series.

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

Casetivity-IIS provides comprehensive configuration options for customizing coverage report parameters and aligning with CDC and state-defined coverage metrics. The system supports both predefined standardized reports and flexible ad-hoc reporting capabilities that allow jurisdictions to tailor coverage analysis to their specific program requirements and public health priorities.

The solution includes dashboards for providers, local health staff, and DOH administrators. Predefined reports (e.g., coverage, invalid doses, timeliness) can be run at the organization or statewide level. Users can also generate ad hoc reports without vendor intervention. The system can also be configured to generate standardized extracts for federal and state reporting, with the option for staff to review outputs prior to submission.

Predefined Coverage Reports Aligned with CDC Standards

The solution includes a suite of standardized coverage reports designed to meet CDC and federal program requirements. These reports are available out-of-the-box and can be run on-demand by authorized users, including Standard Childhood Coverage Report, Standard Adolescent Coverage Report, Adolescent 13-17 Year Old Coverage Report, Flu Coverage Report, COVID-19 Coverage Report, Standard Childhood Master Rate Comparison Report, Standard Adolescent Master Rate Comparison Report, and CDC AFIX Report. The CDC AFIX Report specifically supports the CDC Immunization Quality Improvement for Providers program guidance on immunization coverage among organization and facility patient populations.

User-Defined Parameters and Custom Coverage Reports

Beyond standardized reports, *Casetivity*-IIS offers ad-hoc Custom Coverage reporting that allows users to assess immunization coverage based on their own coverage criteria for various vaccine groups. Users can define the doses needed for each vaccine group of interest, enabling jurisdictions to align reporting with state-specific coverage metrics and program goals. The system supports coverage reporting by multiple user-defined parameters including user-defined geographic areas, age range, vaccine type, and patient cohort.

Flexible Filtering and Demographic Analysis

All coverage reports—both standard and custom—include various filter options that allow users to segment and analyze data by geographic area, race, ethnicity, VFC-eligibility, and patient sex. This filtering capability enables jurisdictions to generate reports for user-defined geographic areas, assess coverage rates among select populations, and identify under-immunized populations based on demographic characteristics. County organizations with user-level based access can generate reports for user-defined geographical areas independently.

No-Code Configuration by Jurisdictional Administrators

The system's built-in no-code and low-code reporting interface allows system administrators to create, configure, and share reports without requiring database access or technical intervention from SSG staff. This self-service capability ensures that jurisdictions can adapt reporting parameters to evolving program requirements, modify coverage criteria, and align with updated CDC or state-defined metrics without vendor dependency. Jurisdictional administrators can also

modify facility types according to immunization program descriptions and CDC VFC Program descriptions, ensuring that organizational classifications align with federal and state standards.

Operational Independence and Timely Analysis

All coverage reporting capabilities are fully accessible to authorized users without requiring assistance from SSG staff. Reports can be generated on-demand and will only include patient data the user has permission to view, supporting role-based access control and data security requirements. This operational independence ensures timely, self-directed analysis for program decision-making and population health planning.

Casetivity-IIS meets the requirement for configuration options that customize coverage report parameters and align with CDC and state-defined coverage metrics through its combination of standardized CDC-aligned reports, flexible user-defined parameters, comprehensive filtering options, and no-code administrative configuration tools.

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 IIS 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.

Yes. *Casetivity*-IIS supports downstream data access for reporting, analytics, and external system integration through multiple mechanisms designed to facilitate secure, scalable data exchange with the jurisdiction's Data Bridge data warehouse. The solution includes a read-only replica of data.

In addition, *Casetivity*-IIS provides direct read-only access to IIS databases for authorized internal users to perform data extracts and queries in accordance with established policies and procedures. The solution supports the export of IIS data for use in other systems through comprehensive Print/Export Reports functionality available out of the box. This capability enables data to be extracted from the solution and made available for downstream consumption by reporting tools, analytics platforms, and data warehouses.

The system architecture includes numerous Application Programming Interfaces (APIs) that enable automatic data exchange with external systems using industry standards and design patterns, including loose coupling and transactional integrity. *Casetivity*-IIS is built with Service Oriented Architectures in mind and exposes service endpoints for use throughout the enterprise environment, including integration with any existing Enterprise Service Bus (ESB). These capabilities allow secure capture and sharing of appropriate data with agencies and business partners, supporting the jurisdiction's need to minimize vendor-dependent development efforts while ensuring timely access to immunization data for cross-system use, public health analysis, and operational reporting.

The solution stores IIS Core Data Elements and supports the ability to store saved report templates, enabling consistent and repeatable data access patterns for downstream systems. This architecture facilitates the development of automated reports and analytical workflows while maintaining data security and integrity. Authorized users can connect to and extract data through APIs or other interfaces to meet reporting and analytical needs, providing the flexibility required for integration with the Data Bridge data warehouse and supporting the jurisdiction's broader data visualization, presentation, and analysis requirements.

4.2.2.5.2. The typical update frequency of the replica (e.g., near real-time, hourly, daily)

SSG's proposed architecture is designed to support near real-time data exchange and reporting workflows through scalable database replication technologies. Update frequency for the read replica can be configured based on jurisdictional requirements and reporting needs, including near real-time, hourly, or daily synchronization intervals. SSG recommends a near real-time approach to support timely analytics, interoperability, and operational reporting while minimizing impact on transactional IIS operations

4.2.2.5.3. How read-only access is managed to avoid performance or integrity impacts on the production environment.

Casetivity-IIS manages read-only access to the replica environment through architectural separation and resource isolation that protects production system performance and data integrity. The solution supports data extracts without degrading IIS performance and enables resource-intensive tasks to run concurrently without impacting production operations.

The system architecture prevents updates to IIS records from the replica environment, ensuring that read-only access cannot alter production data. This design maintains data integrity while supporting analytical workloads, reporting queries, and external system integration through the replica.

Casetivity-IIS supports multiple users executing the same function simultaneously without performance degradation. This capacity extends to the replica environment, where authorized users can query immunization data, generate reports, and perform analytical workflows independently of production system activity. The solution's cloud-enabled infrastructure provides the resource scalability needed to handle concurrent read operations while maintaining consistent response times for production users.

This approach delivers secure, scalable data access for the jurisdiction's Data Bridge integration, public health analysis, and operational reporting while preserving production system performance and protecting data integrity throughout all read-only operations.

4.2.2.5.4. The Vendor's approach to configuring, deploying, and maintaining the replication process.

SSG's approach to configuring, deploying, and maintaining the database replication process for *Casetivity*-IIS is designed to provide jurisdictions with secure, scalable access to immunization data while protecting production system performance and integrity.

Configuration and Deployment

SSG configures read-only replicas or equivalent mechanisms to support downstream data access for reporting, analytics, and integration with external systems such as the jurisdiction's Data Bridge. The replication architecture is established during implementation and can be tailored to meet jurisdictional requirements for update frequency—whether near real-time, hourly, or daily—based on operational needs and infrastructure capacity. SSG works with jurisdictional IT teams to define access protocols, establish secure connection methods, and configure the replica environment to align with the jurisdiction's data governance policies.

Performance and Integrity Protection

Read-only access is managed through dedicated infrastructure that isolates query activity from the production environment. This separation ensures that reporting and analytical workloads do not impact the performance or integrity of the live IIS.

Ongoing Maintenance and Monitoring

SSG provides comprehensive support services for monitoring, troubleshooting, and ensuring data consistency between the production database and the read replica. The replication process is monitored continuously to detect and resolve synchronization issues, latency, or data integrity concerns. SSG's support team responds to incidents through documented escalation procedures and works proactively to address potential issues before they affect data availability or accuracy.

Documentation and Access Methods

SSG delivers documentation describing the replication architecture, update cadence, and access protocols. This documentation supports jurisdictional administrators and authorized users in understanding how to query the replica securely and efficiently. SSG enables secure querying methods through role-based access control and provides guidance on optimizing query performance to support timely access to immunization data for cross-system use, public health analysis, and operational reporting.

Data Volume Quantification

SSG supports methods for quantifying the volume of data interfaced inbound and outbound from the primary database, whether through established interface traffic or one-time data extracts. This capability enables jurisdictions to monitor data flows, assess system capacity, and plan for future scalability needs.

This approach minimizes vendor-dependent development efforts, ensures timely access to immunization data, and provides jurisdictions with the flexibility to develop automated reports and analytical workflows that support public health decision-making and operational efficiency.

4.2.2.5.5. Support services provided for monitoring, troubleshooting, and ensuring data consistency between environments.

SSG provides comprehensive support services to ensure data consistency, system reliability, and operational continuity between production and replica environments for *Casetivity*-IIS. These

services are delivered through a structured support model that includes continuous monitoring, proactive issue resolution, and documented escalation procedures.

24/7/365 System Monitoring and Incident Management: SSG maintains continuous monitoring of the *Casetivity*-IIS solution using AWS CloudWatch to track system performance, response times, and operational health. All traffic to the site has response status and response time recorded in ongoing metrics. The solution employs robust error handling strategies, including monitoring API response times to maintain operational efficiency and ensure proper logging of system warnings and errors. This continuous monitoring capability enables SSG to identify and address potential data consistency issues between environments before they impact operations.

- *Tiered Support Structure:* For critical and high-severity incidents outside business hours, live Tier 3 technical staff are available on-call 24/7/365. This approach ensures that data consistency issues and replication anomalies receive appropriate technical attention based on severity and operational impact.
- *Proactive Issue Resolution:* SSG provides system performance monitoring and proactive issue resolution for all hosted or managed environments. The support model includes planning and executing tasks for system component relevance, resolving functional issues, applying patches, and performing preventative maintenance. Regular performance reports document system health and identify potential consistency concerns between production and replica environments.
- *Data Quality and Consistency Monitoring: Casetivity*-IIS includes built-in capabilities to monitor and troubleshoot data exchange, which extend to monitoring data consistency between environments. The solution logs acknowledgement messages indicating warnings and errors, providing visibility into any discrepancies that may arise during replication processes. Jurisdictional administrators can adjust data quality business rules and create reports to monitor consistency metrics across environments.
- *Infrastructure Management and Disaster Recovery:* SSG provides infrastructure management, application monitoring, incident management, business continuity, and disaster recovery as part of all Software as a Service (SaaS) projects. The FedRAMP-authorized, HIPAA-compliant cloud environment includes managed disaster recovery capabilities with annual disaster recovery exercises conducted to ensure backup and recovery procedures meet jurisdictional requirements. SSG maintains a formal disaster recovery plan that governs backup procedures and ensures compliance with state IT policies and data protection standards.
- *Documentation and Transparency:* SSG maintains comprehensive documentation describing system architecture, monitoring protocols, and support procedures. Every system action—including those related to data replication and consistency—is logged in an audit trail including user ID, timestamp, action type, and before/after values, ensuring

full transparency and accountability. Documentation is updated to reflect any changes made during the maintenance period.

These integrated support services ensure that the State maintains reliable, consistent data across production and replica environments while minimizing operational risk and supporting informed decision-making for public health programs.

4.2.2.5.6. Availability of documentation describing the replication architecture, update cadence, and access protocols.

SSG provides design and architecture documentation that describes the replication architecture, update cadence and access protocols. Since the solution will be single-tenant (as opposed to multi-tenant), West Virginia will have its own dedicated environment.

4.2.2.5.7. Methods for enabling secure, efficient querying by authorized users.

Casetivity-IIS enables secure, efficient querying of the read replica through role-based access control, comprehensive authentication mechanisms, and audit logging that together ensure authorized users can access immunization data while maintaining system integrity and compliance with jurisdictional policies.

All access attempts are tracked through detailed logging and audit trails that monitor user access and authentication events. The system maintains comprehensive audit capabilities that track all accesses successfully complying with identification, authentication, and authorization requirements. This logging supports rapid issue resolution, security compliance, and accountability for all query activities against the read replica.

The read replica architecture is managed to avoid performance or integrity impacts on the production environment. SSG's approach to configuring, deploying, and maintaining the replication process includes support services for monitoring, troubleshooting, and ensuring data consistency between environments. Documentation describing the replication architecture, update cadence, and access protocols is provided to support authorized users in conducting secure, efficient queries.

This combination of role-based access control, strong authentication, comprehensive audit logging, and managed replication infrastructure enables authorized users to query the read replica securely and efficiently while protecting production system performance and maintaining data integrity in accordance with jurisdictional policies and procedures.

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

SSG provides comprehensive methods for quantifying the volume of data interfaced inbound and outbound from the primary *Casetivity*-IIS database through both established interface traffic monitoring and one-time data extract tracking.

For established interface traffic, *Casetivity*-IIS continuously monitors data exchange volumes through AWS CloudWatch and built-in system monitoring capabilities. The solution tracks real-time transaction volumes, including over 130,000 Query by Parameter (QBP) messages per hour and over 35,000 Vaccination Update (VXU) messages per hour. This monitoring provides visibility into the volume of HL7 messages flowing through approximately 1,000 connections to local medical providers, federal reporting systems including the IZ Gateway, and other external systems. The solution maintains detailed logs of all inbound and outbound interface transactions, enabling jurisdictional administrators to quantify data exchange volumes by interface type, time period, and data partner.

For one-time data extracts, *Casetivity*-IIS supports data extraction operations while maintaining optimal performance through efficient resource utilization. The system architecture enables authorized users to perform ad hoc queries and generate data extracts without measurable impact on system performance. Jurisdictional administrators can track and quantify extract volumes through system reporting capabilities that capture IIS Core Data Elements and document extraction activities. The solution's design ensures that resource-intensive tasks, including large-scale data extracts, do not degrade performance for concurrent users or ongoing interface operations.

The solution's monitoring and reporting capabilities provide jurisdictional oversight of all data movement—whether through continuous interface traffic or periodic extracts—supporting data governance requirements, capacity planning, and operational transparency. This comprehensive approach to volume quantification enables public health programs to understand data flow patterns, validate data exchange agreements, and ensure the IIS meets performance benchmarks under varying load conditions.

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.

SSG provides comprehensive database schema documentation and entity-relationship diagrams for *Casetivity*-IIS to support jurisdictional oversight, data governance, and system transparency. This documentation enables public health programs to understand how immunization data is stored, validated, and exchanged within the system.

The schema documentation includes entity-relationship diagrams that illustrate the logical structure and relationships between core data entities in *Casetivity*-IIS. These diagrams map how patient records, vaccination events, inventory management, exemptions, and school roster modules connect and interact within the database architecture. Visual representation helps technical staff and data governance teams understand data flow, dependencies, and integration points across the system.

SSG's documentation approach supports both initial implementation planning and ongoing system enhancement. Jurisdictional administrators and technical staff can reference the schema to assess the impact of configuration changes, plan data extracts and reporting workflows, and ensure alignment with CDC HL7 v2.5.1 standards where applicable. The documentation also facilitates integration planning with external systems such as the Data Bridge, VTrckS, and the IZ Gateway by clarifying how *Casetivity*-IIS structures and stores immunization data elements.

This level of transparency reduces dependency on vendor-specific knowledge for routine data governance activities and empowers jurisdictional teams to make informed decisions about system configuration, reporting requirements, and future enhancements. SSG maintains versioning and update protocols for schema changes to ensure documentation remains current throughout the contract term.

SSG's provision of entity-relationship diagrams and equivalent schema documentation meets the requirement and supports the jurisdiction's need for increased visibility into the structure and logic of the immunization information system.

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

SSG provides comprehensive field-level definitions for the *Casetivity*-IIS database through a detailed data dictionary that supports jurisdictional oversight, data governance, and system transparency. The data dictionary identifies all fields captured by the system and includes the following components:

- Data types — specification of the format and structure for each field (e.g., text, numeric, date, boolean)
- Labels — clear, descriptive names for each data element
- Auditing — tracking specifications for data changes and access
- Security specifications for data sharing — controls governing how data elements can be accessed and shared
- Hierarchy — relationships between data elements and organizational structures
- Validation rules — constraints and business logic applied to ensure data quality and integrity
- Answer selection values — allowable values and permissible entries for constrained fields

SSG's approach to field-level definitions extends beyond static documentation. During implementation, SSG creates a high-level source-to-target mapping specification and detailed mapping design specification that define how data elements align with CDC HL7 v2.5.1 standards and jurisdictional requirements. The data dictionary supports jurisdictional administrators in configuring default values to minimize data input, establishing validation rules at Error, Warning, or Informational levels, and managing data quality business rules through the system interface.

The field-level definitions enable authorized users to understand how immunization data is stored, validated, and exchanged across the IIS. This transparency supports data governance activities, quality assurance planning, and future system enhancements while ensuring that data extracts and queries can be performed without degrading system performance.

SSG delivers these field-level definitions as part of the comprehensive database schema and data dictionary documentation, ensuring that OEPS has full visibility into the structure and logic of patient records, vaccination events, inventory, exemptions, and other core data tables within *Casetivity*-IIS.

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

SSG provides comprehensive database schema documentation and data dictionaries for *Casetivity*-IIS to support jurisdictional oversight, data governance, and system transparency. The documentation includes definitions of key database tables that store and manage immunization program data.

- *Patient Records:* The patient demographic table captures and stores individual demographic information including name, date of birth, address, contact information, and unique identifiers. The system maintains patient status at both provider site and jurisdiction levels, supporting assignment of patients to provider organizations and jurisdictional boundaries. Patient records link to geographic hierarchies and support geocoding for statistical reporting and coverage analysis.
- *Vaccination Events:* The vaccination event table documents administered immunizations with dose-level detail including vaccine product (NDC, CVX, MVX codes), administration date, administering provider, facility location, and eligibility tracking for publicly purchased vaccines. The system maintains separate inventory designations (VFC-supplied, jurisdiction-supplied, private stock) at the dose level and automatically decrements administered doses from active inventory. Vaccination records support duplicate event identification and resolution workflows.
- *Inventory:* The vaccine inventory tables track vaccine doses across multiple dimensions including product information, lot numbers, expiration dates, funding source designation, and location. The system maintains separate inventories for VFC-supplied, jurisdiction-supplied, and private stock vaccines. Inventory tables support ordering, transfers, wastage reporting, reconciliation, and integration with the national Vaccine Tracking System (VTrckS). The schema enables provider site level and jurisdiction level inventory management according to federal and state program requirements.
- *Exemptions:* The exemption tables record vaccine exemptions by vaccine or disease category with support for exemption types (permanent, temporary with expiration date, provisional with review date) and exemption reasons (medical, religious, philosophical). Exemption records link to patient demographics including age, race/ethnicity, and geography to support reporting by school, grade, district, exemption type, and compliance status.
- School Roster Modules: The school roster tables link students to schools, grades, and geographic boundaries to enable targeted outreach and reporting. The roster structure supports compliance reporting for childcare, school, and college immunization requirements and integrates with exemption tracking for longitudinal monitoring. The schema supports both immunization and oral health module functionality with role-based access for school nurses and dental professionals.

The database schema documentation includes entity-relationship diagrams, field-level definitions with data types and constraints, mapping to CDC HL7 v2.5.1 standards where

applicable, and versioning protocols for schema changes. This transparency enables jurisdictional administrators to understand data storage, validation rules, and exchange protocols while supporting future system enhancements and data governance requirements.

4.2.2.6.4. Mapping to CDC HL7 v2.5.l standards, where applicable.

Casetivity-IIS implements HL7 v2 messaging in full alignment with the CDC's HL7 Implementation Guide for Immunization Messaging. The solution exposes its HL7 interface using the standard CDC SOAP WSDL for IIS messaging and supports the most common HL7 v2 message types used in immunization systems.

The platform maps CDC HL7 v2.5.1 standards to the following core message types and data elements:

- VXU messages — vaccine record submissions and demographic updates are mapped to patient demographic tables and vaccination event tables within the database schema
- QBP messages — patient history and forecast queries (bulk and individual) are mapped to patient records and clinical decision support tables that store evaluation and forecasting data
- ADT messages — demographic-only updates are mapped to patient demographic fields and support real-time synchronization with external systems

The solution includes message validation tools that enforce CDC HL7 v2.5.1 field-level requirements, including data types, constraints, and allowable values. Configurable error handling supports onboarding and long-term quality monitoring by identifying discrepancies between incoming HL7 messages and the database schema. Logging and audit trails capture all HL7 transactions, enabling jurisdictional oversight of how immunization data is received, validated, stored, and exchanged.

Jurisdictional administrators can adjust data quality business rules to set validation levels (Error, Warning, Informational) for HL7 message processing. These rules govern how inbound HL7 data elements are validated against the database schema and CDC standards before being persisted to patient records, vaccination events, inventory, and other key tables.

This mapping ensures that *Casetivity*-IIS maintains compliance with CDC interoperability standards while providing transparency into how HL7 data elements correspond to the underlying database structure, supporting data governance, system enhancements, and cross-system integration.

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

Casetivity-IIS supports versioning and update protocols for database schema changes through a structured, configurable approach that enables jurisdictions to evolve their system logic and data structures over time without requiring code changes or vendor intervention.

The solution allows jurisdictional administrators to manage deduplication logic, match expressions, confidence thresholds, and field-level merge rules at runtime. Administrators can update match expressions to reflect changes in data patterns or comply with new best practices, adjust confidence thresholds for auto-merge and manual review scenarios independently for each entity type, and define or modify merge logic as policies or practices change. This configurability enables jurisdictions to iterate and refine their logic in response to observed needs, making updates operationally feasible and responsive to evolving requirements.

SSG maintains a collaborative approach with jurisdictions to define and refine match criteria based on program-specific needs, review outcomes, and adjust thresholds or logic where needed. The solution combines real-time processing with background reprocessing and robust auditing to ensure that schema-related updates maintain high standards of data quality and accuracy. Every configuration change is logged in an audit trail, including user identity, timestamp, action type, and before-and-after values, ensuring full transparency and accountability throughout the update process.

SSG also anticipates and supports annual updates aligned with CDC IIS Functional Standards releases. Updates outside the CDC's 90-day IZ Gateway implementation window are evaluated and authorized through the State's standard contract governance and change-order process. SSG accounts for these updates in ongoing maintenance planning and proposes an approach for scoping, estimating, and implementing future CDC-driven changes to ensure continued compliance with federal and state interoperability standards.

This approach ensures that *Casetivity*-IIS can adapt to changing jurisdictional policies, federal standards, and operational needs while maintaining system stability, data integrity, and compliance over time.

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.

Casetivity-IIS supports roster integration that links students to schools, enabling targeted outreach and reporting by school, grade, and county. School nurses can upload student cohorts to prepopulate survey fields using IIS match logic, allowing the system to identify which students already have records in the IIS and which do not. This roster-based approach supports identification of geographic and demographic gaps in oral health coverage by enabling filtering and reporting at the school, grade, and county levels.

The system tracks compliance and coverage through preconfigured dashboards that monitor survey responses, compliance status, and immunization coverage across student populations. These dashboards are preconfigured for childcare, school, and college populations and can be extended to support additional levels as needed. When rosters are uploaded, the system applies match logic to associate students with existing patient records, creating a foundation for targeted reporting and outreach.

School nurses access reporting tools that generate school-level compliance reports showing counts of students who have met each vaccine series, have exemptions, or have no records on file. The School Immunization Report and School Compliance Report provide summary views of student immunization data with all vaccine series listed, supporting identification of students who may need follow-up for oral health services. These reports can be filtered by school, grade, and county to prioritize outreach efforts for high-need populations.

This roster integration capability reduces administrative burden for school nurses, improves data consistency across student populations, and enables the jurisdiction to identify and address gaps in oral health coverage through structured, reportable workflows that support equitable access to preventive services.

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.

Dental professionals can enter administered oral health records directly into *Casetivity*-IIS through a dedicated Oral Health module that supports timely documentation of care delivered during school-based dental screenings and clinical encounters. The module is designed to

reduce disparities in access to preventive oral health services by enabling real-time data capture at the point of care.

The system leverages role-based access control to assign dental professionals appropriate roles and permissions within the IIS. Once configured, dental professionals appear in the provider dropdown menu and can access the oral health documentation workflow through the same unified interface used for immunization records. This approach eliminates the need for separate systems or duplicate data entry, streamlining documentation and reducing administrative burden.

When entering oral health records, dental professionals document screening results, treatments administered, and follow-up recommendations directly into patient records. The module links students to schools via rosters, enabling targeted reporting by school, grade, and county. This roster integration supports identification of geographic and demographic gaps in oral health coverage, allowing jurisdictional administrators to prioritize outreach and follow-up for high-need populations.

Jurisdictional administrators configure user roles and permissions in accordance with state policies. The permissions "Enable Oral Health Reports" and "Enable Health Service" can be assigned individually or applied in bulk using the system's master role update capability. This flexibility ensures that dental professionals receive appropriate access levels while maintaining data security and compliance with privacy requirements.

The Oral Health module operates within the same security, audit, and compliance framework as the core IIS. All actions taken on oral health records are logged with user ID, action type, timestamps, and field-level change history, supporting accountability and regulatory compliance. Administrators can access built-in reports or request tailored audit outputs to meet operational review needs.

By enabling dental professionals to enter administered oral health records directly into *Casetivity*-IIS, the solution ensures timely documentation of care, supports continuity across school-based and clinical settings, and advances health equity through improved access to preventive oral health services for underserved student populations.

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.

School nurses use *Casetivity*-IIS to enter historical oral health records and manage student rosters through a dual-workflow design that supports both retrospective documentation and ongoing roster administration. This capability ensures continuity of care by consolidating historical oral health data with current student enrollment information in a single, unified system.

School nurses access the system through role-based permissions that grant them the ability to enter historical oral health records directly into student profiles. When entering retrospective data, nurses can document past dental screenings, treatments, and oral health assessments that occurred outside the IIS. The system links these historical records to individual students through the same patient matching logic used for immunization data, ensuring accurate association with the correct student record even when entering data after the fact.

For roster management, school nurses can upload student cohorts to prepopulate fields using the IIS match logic. This roster integration capability allows nurses to link students to specific schools, grades, and geographic locations, creating the foundation for targeted outreach and reporting. The roster upload process leverages the system's deduplication functionality to match uploaded student information against existing records, preventing duplicate entries while ensuring all students are properly represented in the system.

The unified record view consolidates all oral health data—whether entered as historical records by school nurses, submitted via roster upload, or documented in real time by dental professionals—into a single patient record. This consolidation supports continuity of care by providing a complete oral health history accessible to authorized users across different care settings and time periods.

School nurses receive access to oral health reports and health service functionality through assignable permissions that can be configured individually or applied in bulk using the system's master role update capability. Jurisdictional administrators maintain control over role definitions and can modify permissions in accordance with state policies, ensuring appropriate access levels while maintaining data security and privacy protections.

Casetivity-IIS meets the requirement for school nurses to enter historical oral health records and manage rosters by providing dedicated workflow support, intelligent data matching, consolidated record views, and configurable role-based access that together enable effective retrospective data entry and ongoing roster administration.

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.

The Oral Health module in *Casetivity*-IIS supports reporting that identifies students with or without oral health records and enables filtering by urgency of care, school, grade, and county. This capability allows jurisdictional administrators and school health staff to prioritize outreach and follow-up for high-need populations and identify geographic and demographic gaps in oral health coverage.

The module leverages the platform's robust and flexible reporting framework, which allows authorized users to generate both predefined and ad-hoc reports without requiring assistance from SSG staff. Reports are accessible on-demand and include only patient data the user has permission to view, ensuring compliance with role-based access control policies.

For school-based oral health programs, the system supports uploading student cohorts to prepopulate fields using IIS match logic. When patient matches are found, the system returns compliance reports with counts of students who have oral health records, exemptions, or no records on file. Reports can be filtered by individual school, grade level, county, and urgency of care, enabling targeted intervention strategies.

The reporting capability integrates with the module's roster functionality, which links students to schools via rosters. This integration supports identification of underserved populations and enables jurisdictional staff to assess oral health coverage across schools, grades, and geographic areas. School nurses and dental professionals can access summary and detail-level reports to support continuity of care and retrospective data entry.

Casetivity-IIS meets the requirement by providing configurable, role-based reporting that identifies students with or without oral health records and supports filtering by urgency, school, grade, and county to advance health equity and reduce disparities in access to preventive oral health services.

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.

The Oral Health module in *Casetivity*-IIS includes reporting capabilities that enable jurisdictional administrators and authorized users to filter and prioritize outreach efforts based on urgency of care, school, grade, and county. These filters support the identification of high-need populations and geographic or demographic gaps in oral health coverage, directly advancing health equity goals for underserved student populations.

The module leverages the system's standard reporting framework to generate reports that identify students with or without oral health records. Users can apply filters across multiple dimensions—including urgency of care designation, individual school assignment, grade level, and county location—to segment student populations and prioritize follow-up activities. This filtering capability allows school nurses, dental professionals, and public health staff to focus outreach on students who require immediate attention or who are located in areas with documented service gaps.

Reports are accessible through role-based dashboards and can be configured to display compliance status, coverage rates, and care urgency indicators. The system supports both predefined report templates and ad-hoc queries, enabling users to tailor reporting parameters to meet evolving program needs without requiring vendor support. Reports can be exported in

multiple formats, including PDF, CSV, and XLSX, to facilitate coordination with external partners and support data-driven decision-making.

The Oral Health module integrates with the system's roster management functionality, linking students to schools and enabling targeted reporting by school, grade, and county. This integration ensures that reporting reflects current enrollment data and supports longitudinal tracking of oral health service delivery across the jurisdiction. Jurisdictional administrators retain full control over report configuration, access permissions, and data visibility in accordance with state policies and privacy requirements.

Casetivity-IIS meets the requirement for reporting capabilities that filter 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.

Casetivity-IIS assigns dental professionals appropriate roles and includes them in the provider dropdown menu through its configurable role-based access control framework. The system supports function-based roles tailored for different user types, including providers and clinical staff responsible for vaccine and health service data entry. Dental professionals are assigned roles that grant them the necessary permissions to enter administered oral health records directly into the system, ensuring timely documentation of care delivered during school-based dental screenings.

The role assignment process operates through both state-level control and delegated administration. Department administrators maintain authority over global role definitions and can define and manage new roles or adjust existing ones to meet program requirements. Each role is configured with field-level access permissions that determine which data elements users can view or edit, entity-level permissions that control access to specific modules such as oral health records, and functional access that determines which dashboards and reports are available. Once dental professional roles are defined with appropriate oral health module permissions, these users appear in the provider dropdown menu and can document care within their designated scope.

At the facility level, each provider site designates an Access Administrator who adds users, assigns roles based on local workflows, and monitors user activity. This delegated administration model enables dental professionals to be onboarded efficiently while maintaining security and

data privacy standards. The system enforces organization and location-based segregation, associating users with specific organizations or provider sites and restricting access to data relevant to their assignments. This ensures dental professionals access only the student oral health records and school rosters appropriate to their assigned facilities and geographic scope.

This role-based framework supports the dual workflow requirements of the Oral Health module by enabling dental professionals to enter administered records while school nurses manage historical records and rosters under separate role configurations. The approach reduces administrative burden, maintains accountability through role-specific audit trails, and ensures compliance with jurisdictional policies governing access to protected health information. *Casetivity*-IIS meets the requirement for assigning dental professionals appropriate roles and including them in the provider dropdown menu within the Oral Health module's access control framework.

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

School nurses are granted access to oral health reports and health service functionality through *Casetivity*-IIS's role-based access control framework. Jurisdictional administrators configure user roles and assign the permissions "Enable Oral Health Reports" and "Enable Health Service" to school nurse accounts. These permissions can be assigned individually or applied in bulk using the system's master role update capability, allowing efficient onboarding of multiple school nurse users across the jurisdiction.

Once permissions are assigned, school nurses log into the School Nurse Module from the Department of Health side of the system. This module provides functionality specific to the Department of Health and enables school nurses to access oral health reports that identify students with or without oral health records. The reporting interface supports filtering by urgency of care, school, grade, and county, allowing school nurses to prioritize outreach and follow-up for high-need populations and identify geographic and demographic gaps in oral health coverage.

In addition to reporting access, school nurses can enter historical oral health records and manage school rosters within the module. This dual workflow supports continuity of care and retrospective data entry while maintaining appropriate separation between clinical documentation entered by dental professionals and roster management performed by school staff.

Jurisdictional administrators retain full control over role configuration and can modify or inactivate school nurse roles and permissions at any time in accordance with jurisdictional policies. This governance structure ensures that access remains appropriate, auditable, and aligned with the State's health equity objectives for school-based oral health services.

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.

Casetivity-IIS supports both individual and bulk assignment of the 'Enable Oral Health Reports' and 'Enable Health Service' permissions through its master role update capability. The system uses role hierarchies that automatically update all users assigned to a role based on changes made to the master role attributes. All updates occur in real time.

System administrators configure role-based authorization through explicit associations—such as users to roles and roles to permissions—or through expression-based rules. This flexibility allows permissions to be granted or restricted based on business rules down to the field level. Users can be assigned multiple roles with different permissions, supporting secure and dynamic workflows while enabling jurisdictional administrators to configure security access over time to meet evolving program needs.

For the Oral Health module, administrators can assign the 'Enable Oral Health Reports' and 'Enable Health Service' permissions individually to specific roles—such as School Nurse or Dental Professional—or apply them in bulk by updating the master role definition. When a master role is updated with these permissions, all users assigned to that role receive the updated access automatically and immediately. This eliminates the need to update individual user accounts one by one and ensures consistent access control across the jurisdiction.

Jurisdictional administrators maintain authority over global role definitions and system-wide security settings, while provider-level Access Administrators can assign roles based on local workflows within their facilities. This delegated administration model supports both centralized governance and operational flexibility, ensuring that Dental Professionals and School Nurses receive appropriate access to oral health functionality in accordance with jurisdictional policies.

Casetivity-IIS meets the requirement for individual and bulk permission assignment through its master role update capability, providing real-time, scalable access management for the Oral Health module.

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

Jurisdictional administrators configure, modify, and inactivate roles and permissions for the Oral Health module using the same comprehensive role-based access control framework that governs all *Casetivity*-IIS functionality. The system provides out-of-the-box support for administrators to manage user access in accordance with jurisdictional policies through a robust Admin Console.

- *Role Configuration and Modification:* Jurisdictional administrators define and manage roles tailored to Oral Health module users, including Dental Professionals and School

Nurses. Each role can be configured with field-level access controls that determine which data elements users can view or edit, entity-level permissions that govern access to specific records or functions, and functional access that controls visibility of dashboards, reports, and data exchange capabilities. For the Oral Health module specifically, administrators assign the permissions "Enable Oral Health Reports" and "Enable Health Service" individually or in bulk using the system's master role update capability. Dental Professionals are assigned appropriate roles and included in the provider dropdown menu, while School Nurses are granted access to oral health reports and health service functionality based on their assigned roles.

- *Organizational and Jurisdictional Scoping:* The system enforces data partitioning based on organizational and jurisdictional assignments. Users associated with specific schools, facilities, or geographic areas access only the data relevant to their assignments. This supports complex jurisdictional hierarchies such as cities spanning multiple counties or public health regions made up of grouped municipalities. Access to oral health reports, dashboards, and student data is scoped to the jurisdictional level assigned to each user's group, ensuring compliance with local privacy policies and operational boundaries.
- *Role Inactivation and Oversight:* Jurisdictional administrators inactivate user roles through role review and deactivation tools available out-of-the-box. Administrators can review assigned roles and deactivate or adjust them as operational needs or jurisdictional policies change. The system supports automatic suspension of inactive users after a defined period of non-use. Full audit logging tracks all actions by user ID, role, and timestamp, providing administrators with detailed oversight to ensure users operate within their assigned access levels and comply with jurisdictional data governance requirements.
- *Delegated Administration:* The solution supports delegated administration through Access Administrators designated at each provider site or organizational level. These administrators can add and deactivate users, assign roles based on local workflows, and monitor user activity within their facility or jurisdiction. State-level administrators maintain authority over global role definitions, jurisdictional access configurations, and system-wide security settings, ensuring consistent policy enforcement across the Oral Health module and all other system functions.

This role-based framework enables jurisdictional administrators to configure, modify, and inactivate Oral Health module roles and permissions in full accordance with jurisdictional policies while maintaining the flexibility to adapt to evolving program requirements and user needs.

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.l remains the mandatory baseline, FHIR support provides increased flexibility, transparency, and scalability for secure, standards-based exchange of immunization data with 11S 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 HL 7 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.

Casetivity-IIS supports HL7 FHIR for public health immunization data exchange. The solution integrates with Electronic Health Record Systems using HL7 v2.x, FHIR, and other public health data standards, enabling bidirectional data exchange and automated processing of vaccination data, demographic updates, and clinical messages from provider systems. The platform supports both real-time and batch interfaces to facilitate secure, standards-based exchange of immunization data with IIS partners.

SSG's approach positions FHIR as an addition to the mandatory HL7 v2.5.1 baseline, providing increased flexibility, transparency, and scalability for immunization data exchange while maintaining full compliance with current CDC-endorsed interoperability standards. This dual-standard capability ensures *Casetivity*-IIS can evolve alongside emerging federal and jurisdictional priorities while preserving continuity with existing data exchange workflows.

The solution's FHIR support enables the Agency to participate in national interoperability initiatives and public health modernization efforts without disrupting established HL7 v2.x interfaces. This approach reduces implementation risk, supports long-term system sustainability, and positions the jurisdiction to adopt next-generation data exchange capabilities as federal standards and partner readiness advance.

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.

SSG has established technical capability to integrate with Electronic Health Record Systems using HL7 v2.x, FHIR, and other public health data standards. The solution supports both real-time and batch interfaces, enabling bidirectional data exchange and automated processing of vaccination data, demographic updates, and clinical messages from provider systems. This foundation positions *Casetivity*-IIS to extend its interoperability capabilities to include FHIR-based data exchange as national standards and jurisdictional priorities evolve.

While the current production implementation of *Casetivity*-IIS is built on HL7 v2.x messaging—the mandatory baseline for immunization data exchange—SSG recognizes the importance of advancing toward FHIR-based interoperability to support national modernization initiatives and future system enhancements. The solution's existing architecture supports standards-based integration and can be extended to securely generate and receive data using HL7 FHIR resources, including the Immunization resource for vaccine administration events and the Immunization Recommendation resource for patient-specific forecasting. SSG is prepared to work collaboratively with the Agency to develop a detailed roadmap and timeline for implementing FHIR capabilities in alignment with the applicable FHIR Release (such as R4) as an addition to the existing HL7 v2.5.1 interfaces.

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 HL 7 v2.5.1 interfaces.

SSG is committed to advancing immunization data exchange through adoption of HL7 Fast Healthcare Interoperability Resources (FHIR) as an addition to the existing mandatory HL7 v2.5.1 interfaces. *Casetivity*-IIS integrates with Electronic Health Record Systems using HL7 v2.x, FHIR, and other public health data standards, supporting both real-time and batch interfaces for bidirectional data exchange. Any FHIR based support can be done in ***parallel*** with the existing

mandatory HL7 v2.5.1 interfaces. SSG is dedicated to working with West Virginia on FHIR support as reporting providers obtain the capability to utilize it.

FHIR Development and Testing Roadmap:

SSG's FHIR implementation roadmap follows a phased approach that ensures continuity of existing HL7 v2.5.1 operations while introducing FHIR capabilities in parallel:

- *Phase 1: Assessment and Planning (Months 1-2)*
  SSG will conduct a thorough assessment of current system architecture against FHIR Release 4 (R4) requirements for public health immunization data exchange. This phase includes identifying required FHIR resources, defining API endpoints, establishing security protocols, and documenting integration points with existing HL7 v2.5.1 interfaces. SSG will work with the Agency to prioritize FHIR use cases and establish success criteria for pilot testing.
- *Phase 2: Development and Configuration (Months 3-6)*
  SSG will develop FHIR-based data exchange capabilities using RESTful APIs that expose secured endpoints for immunization data. The solution will support the HL7 FHIR Immunization resource for vaccine administration events and the HL7 FHIR Immunization Recommendation resource for patient-specific forecasting. All FHIR interfaces will utilize HTTPS/TLS encryption with JWT-based authorization for stateless authentication. Development will occur in parallel with existing HL7 v2.5.1 operations, ensuring no disruption to current data flows.
- *Phase 3: Testing and Validation (Months 7-9)*
  SSG will conduct comprehensive testing of FHIR endpoints in a dedicated test environment. Testing will include unit testing of individual FHIR resources, integration testing with partner systems, performance testing under expected load conditions, and security testing to validate authentication and authorization controls. SSG will coordinate with IIS partners to conduct pilot exchanges using FHIR alongside existing HL7 v2.5.1 interfaces, validating data accuracy and completeness across both standards.
- *Phase 4: Deployment and Documentation (Months 10-12)*
  Following successful testing, SSG will deploy FHIR capabilities to production and provide comprehensive, public-facing API documentation for all FHIR endpoints to the Agency and potential IIS partners. Documentation will include resource schemas, authentication requirements, error handling procedures, and example transactions. SSG will provide training to Agency staff and IIS partners on FHIR-based data exchange and establish ongoing support procedures.

Parallel Operations and Standards Compliance:

Throughout this roadmap, HL7 v2.5.1 interfaces will remain fully operational and continue to serve as the mandatory baseline for immunization data exchange. FHIR capabilities will be introduced as an additional option, allowing IIS partners to adopt FHIR-based exchange on their own timeline while maintaining existing HL7 v2.5.1 connectivity. SSG's architecture supports workflow and ESB orchestration to make data-related processes more efficient in event-driven environments, enabling seamless operation of both HL7 v2.5.1 and FHIR standards simultaneously.

This phased approach ensures the Agency benefits from increased flexibility, transparency, and scalability for standards-based immunization data exchange while maintaining continuity of current operations and minimizing implementation risk.

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.

SSG confirms that comprehensive, public-facing API documentation for all FHIR endpoints will be provided to the Agency and potential IIS partners. As part of our commitment to advancing immunization data exchange through HL7 Fast Healthcare Interoperability Resources (FHIR), SSG is actively developing FHIR capabilities for *Casetivity*-IIS, including FHIR for Query by Parameter (QBP) and Bulk QBP Batching functionality. This development builds on our current interoperability processes to provide a more robust way for users to process QBP requests and exchange immunization data.

SSG's approach to FHIR implementation prioritizes transparency and accessibility for all critical partners. The API documentation will include detailed specifications for FHIR endpoints, resource definitions, authentication and authorization protocols, data exchange workflows, and integration guidance. This documentation will be made available to the Agency and shared with IIS partners to facilitate seamless, standards-based data exchange and support national interoperability initiatives.

SSG recognizes that comprehensive API documentation is essential for enabling the Agency and IIS partners to integrate effectively with *Casetivity*-IIS, develop custom reporting solutions, and leverage FHIR-based data exchange capabilities. The documentation will support both technical implementation teams and public health critical partners in understanding and utilizing FHIR endpoints for immunization data exchange, forecasting, and reporting purposes.

4.2.3 Mandatory Project Requirements

4.2.3.1. 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.

Casetivity-IIS can meet all Essential requirements outlined in Attachment B – HS Baseline Requirements RTM as required by the CDC either out of the box or with customization. There are no Essential requirements that cannot be met.

The State can find the completed responses for Attachment B – HS Baseline Requirements RTM on the pages that follow.

4.2.3.1.1. Administer System

Capability	Requirement: The IIS must/should..	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	
Hierarchy Configuration	ability to associate user(s) to a facility	E	Yes	
Hierarchy Configuration	ability to associate clinician(s) to a facility	E	Yes	
Hierarchy Configuration	ability to associate facility/facilities to an organization	E	Yes	
Hierarchy Configuration	ability to establish geographic jurisdictional hierarchy	E	Yes	
Hierarchy Configuration	ability to aggregate data across user-defined hierarchies	E	Yes	
System Configuration	ability to maintain inventory availability in IIS visible to authorized users	E	Yes	
System Configuration	ability for jurisdictional admin to maintain separate VFC supplied inventory in the IIS	E	Yes	
System Configuration	ability for jurisdictional admin to maintain separate jurisdiction supplied inventory	E	Yes	
System Configuration	ability for jurisdictional admin to maintain separate private stock inventory	E	Yes	
System Configuration	ability for jurisdictional admin to manage code sets	E	Yes	
System Configuration	ability for jurisdictional admin to update NDC codes	E	Yes	
System Configuration	ability for jurisdictional admin to update CVX codes	E	Yes	
System Configuration	ability for jurisdictional admin to update MVX codes	E	Yes	
System Configuration	ability to configure default values to minimize data input	E	Yes	
System Configuration	ability to display an error message in the user interface when minimum information required is not complete	E	Yes	
System Configuration	ability to standardize addresses per US Postal conventions and codes	E	Yes	
System Configuration	ability to verify validity of addresses (as valid USPS addresses) in the IIS through electronic means (e.g., SmartyStreets)	E	Yes	
System Configuration	ability to geocode addresses	E	Yes	
System Configuration	ability to validate accurate assignment of address to an individual through electronic means (e.g., LexisNexis)	O	Yes	
System Configuration	ability for jurisdictional admin to modify facility types according to immunization program descriptions and CDC VFC Program descriptions	E	Yes	
System Configuration	ability for jurisdictional admin to configure rules governing data validation of incoming HL7 messages	E	Yes	
System Configuration	ability to configure an authorization agreement as per jurisdictional policy	O	Yes	
System Configuration	ability to configure a user agreement as per jurisdictional policy	O	Yes	
System Configuration	ability to display age in year/month/day format in all age display fields (e.g., 2 years, 4 months, 3 days)	E	Yes	
System Configuration	ability to provide optional calendar to select a date in a web client	O	Yes	
System Configuration	ability to add patient priority group indicators	E	Yes	
System Configuration	ability to modify patient priority group indicators	E	Yes	
System Configuration	ability for jurisdictional admin to manage business rules related to data quality	E	Yes	
System Configuration	ability for jurisdictional admin to specify business rules for monitoring data quality	E	Yes	
System Configuration	ability for jurisdictional admin to modify business rules for monitoring data quality	E	Yes	
System Configuration	ability to configure the organization enrollment form	E	Yes	
System Configuration	support rules-based logic to suggest approval or rejection of enrollment form based on review of completed fields	E	Yes	
System Configuration	ability to manage rules-based logic for approval or rejection of enrollment form	E	Yes	
System Configuration	ability for jurisdictional admin to create enrollment forms based on program requirements	E	Yes	
System Configuration	ability for jurisdictional admin to modify an enrollment form	E	Yes	
System Configuration	ability to auto-populate existing user information in the IIS with the information on the enrollment form when creating a new facility in the IIS	O	Yes	
System Configuration	ability to auto-populate the organization information in the IIS with information on the enrollment form when creating a new organization in the IIS	O	Yes	
System Configuration	ability for jurisdictional admin to configure vaccine forecasting business rules	E	Yes	*Cozetivity*-IIS supports configurable vaccine forecasting to accommodate jurisdiction-specific business requirements. Depending on the implementation approach selected by the jurisdiction, forecasting may be provided through the integrated HLN ICE (Immunization Calculation Engine) forecaster or through *Cozetivity*-IIS forecasting capabilities. Authorized jurisdictional administrators can configure supported forecasting business rules and parameters in accordance with the capabilities of the selected forecasting approach and role-based security permissions.
System Configuration	ability to apply effective dates to vaccine rules	O	Yes	
System Configuration	ability to incorporate new vaccines per ACIP into the forecasting algorithm	E	Yes	
System Configuration	ability to support a record search algorithm to return "best matches"	E	Yes	
System Configuration	ability for jurisdictional admin to configure the number of search results to be displayed per jurisdictional policy	E	Yes	
System Configuration	ability for jurisdictional admin to modify required parameters for patient searches	E	Yes	
System Configuration	ability to restrict certain data from being included in reports such as sensitive demographic information e.g., address, phone number, mother's maiden	E	Yes	
System Configuration	ability to open multiple screens simultaneously within the application	O	Yes	
User Roles and Permissio	ability for jurisdictional admin to manage user roles and permissions by task per jurisdictional policy	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to add user roles with distinct permissions	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to modify user roles with distinct permissions	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to inactivate user roles	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to modify permissions to IIS processes and data for specific user roles	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to restrict system functionality by user role	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to restrict authorized user access to data based on user role	E	Yes	
User Roles and Permissio	ability for jurisdictional admin to enable access to standard reports based on user role	E	Yes	
User Roles and Permissio	ability to automatically update all users assigned to a role based on changes made to the "master" role attributes	E	Yes	
System Alerts	ability for jurisdictional admin to manage system alerts	E	Yes	
System Alerts	ability to view global messages upon logging into the application	E	Yes	
System Alerts	ability for jurisdictional admin to add system alerts for specific IIS users to view when logging into application	O	Yes	
System Alerts	ability for jurisdictional admin to add global messages	E	Yes	
System Alerts	ability for jurisdictional admin to edit global messages	E	Yes	
System Alerts	ability for jurisdictional admin to inactivate global messages	E	Yes	

4.2.3.1.2. Manage Organizations and Facilities

Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
ability to search organization/facility information stored in the IIS	E	Yes	
ability for jurisdictional admin to search organizations/facilities by user-defined parameters	E	Yes	
ability to clear and re-enter search criteria when searching for an organization/facility	E	Yes	
ability for applicant from unauthorized (non-participating/enrolled) organization to enroll electronically for participation in the IIS	E	Yes	
ability for applicant from unauthorized organization to add IIS enrollment information online	E	Yes	
ability for applicant from unauthorized org to submit IIS enrollment information online	E	Yes	
ability for applicant from unauthorized org to save partially complete IIS enrollment information	O	Yes with customization*	Allowing users who do not yet have accounts to return to partially completed IIS enrollment information will require customization of Cosentry-HS. SSG can customize Cosentry-HS to provide this capability.
ability for applicant from unauthorized org to return to a partially complete IIS enrollment information	O	Yes with customization*	Allowing users who do not yet have accounts to return to partially completed IIS enrollment information will require customization of Cosentry-HS. SSG can customize Cosentry-HS to provide this capability.
ability to prevent submission of incomplete IIS enrollment information when required field(s) are missing	E	Yes	
ability to electronically notify the applicant of incomplete IIS enrollment information specifying the missing required fields	E	Yes	
ability to electronically notify applicant that IIS enrollment information has been submitted	E	Yes	
ability for applicant from unauthorized org to edit rejected IIS enrollment information	E	Yes	
ability for applicant from unauthorized org to resubmit a rejected IIS enrollment	E	Yes	
ability to capture electronic signature for enrollment, for an authorization agreement	O	Yes	
ability for jurisdictional admin to manage organization/facility IIS enrollment	E	Yes	
ability for jurisdictional admin to manage organization/facility IIS enrollment status	E	Yes	
ability for jurisdictional admin to inactivate an organization	E	Yes	
ability for jurisdictional admin to reactivate an organization	E	Yes	
ability to store IIS enrollment status for an organization/facility	E	Yes	
ability for jurisdictional admin to inactivate a facility	E	Yes	
ability for jurisdictional admin to reactivate a facility	E	Yes	
ability for jurisdictional admin to electronically approve IIS enrollment	E	Yes	
ability to include reason for rejecting IIS enrollment of an organization	E	Yes	
ability to electronically notify the organization that the submitted enrollment was rejected along with the reason	E	Yes	
ability for jurisdictional admin to manage organization and facility records within the IIS	E	Yes	
ability for jurisdictional admin to add an organization	E	Yes	
ability for jurisdictional admin to modify an organization record	E	Yes	
ability for jurisdictional admin to add a facility	E	Yes	
ability for jurisdictional admin to modify a facility record	E	Yes	
ability to automatically generate unique facility IIS ID	E	Yes	
ability for jurisdictional admin to associate a facility to an organization	E	Yes	
ability for jurisdictional admin to edit association between a facility an organization	E	Yes	
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	
ability to capture a facility's mailing address	E	Yes	
ability to capture a facility's shipping address	E	Yes	
ability to enter contact information for the facility contact	E	Yes	
ability to enter contact information for an optional contact	E	Yes	
ability to indicate if an organization/facility is a site where immunizations are administered	E	Yes	
ability to indicate if an organization/facility is a site where vaccines are stored for redistribution	O	Yes	
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	
ability for jurisdictional admin to retrieve electronic files from provider file folder	E	Yes	
ability for jurisdictional admin to record notes related to a organization/facility	E	Yes	
ability to flag an organization as participating in VFC and/or other user-defined vaccine program(s)	E	Yes	
ability to retrieve organization/facility information from scanned forms and automatically fill required data fields with retrieved information	O	Yes	
ability for an organization to submit vaccine program enrollment information electronically	E	Yes	
ability to capture electronic signature for vaccine program enrollment	E	Yes	
ability to access the vaccine program agreement in a separate window from the vaccine program enrollment	E	Yes	
ability to provide link to the blank formatted vaccine program enrollment form	E	Yes	
ability for the jurisdictional vaccine program admin to assign a VFC pin number to a newly enrolled VFC site	E	Yes	
ability to select the type of certified monitoring device being used to record temperatures	E	Yes	
ability for the jurisdictional vaccine program admin to document that a facility has a certificate of calibration for the temperature monitoring device	O	Yes	
ability for the jurisdictional vaccine program admin to approve a vaccine program enrollment	E	Yes	
ability for the jurisdictional vaccine program admin to enter an expiration date for a vaccine program enrollment	E	Yes	
ability for the jurisdictional vaccine program admin to document that the vaccine program facility has a routine and emergency vaccine management plan	E	Yes	
ability for the jurisdictional vaccine program admin to document that a facility participating in VFC has a VFC Coordinator annual training certificate	E	Yes	
ability for the jurisdictional vaccine program admin to document that a facility participating in VFC has a Backup Coordinator annual training certificate	E	Yes	
ability for the jurisdictional vaccine program admin to add comments during the vaccine program enrollment approval process	O	Yes	
ability to require the vaccine program facility to indicate the number of vaccine storage units being monitored	O	Yes	
ability to require the vaccine program facility to indicate the types of vaccine storage units being monitored	O	Yes	
ability to require the vaccine program facility to indicate whether they store Varicella and MMRV vaccine	E	Yes	
ability to enter contact information for the facility Primary Vaccine Coordinator	E	Yes	
ability to enter contact information for the facility Backup Vaccine Coordinator	E	Yes	
ability to enter contact information for the facility vaccine program Agreement Signatory	E	Yes	
ability to capture the day of the week that a vaccine program facility may receive vaccine shipments	E	Yes	

ability to capture the time that a vaccine program facility may receive vaccine shipments	E	Yes	
ability to automatically turn off vaccine ordering capabilities for a facility that does not have an up-to-date vaccine program enrollment	E	Yes	
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	
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	
ability for IIS staff to retrieve electronic files from organization/facility file folder	O	Yes	
ability to automatically validate clinician license number against Professional Licensing Agency record database	O	Yes with customization*	This capability would need to be developed based on the specifications of the Professional Licensing Agency's API. SSG can develop the required integration to meet the Agency's requirements.
ability to submit vaccine program re-enrollment data electronically	E	Yes	
ability to electronically notify a facility VFC/vaccine program coordinator of an upcoming need for VFC/vaccine program re-enrollment	O	Yes	
ability for the jurisdictional vaccine program admin to modify the date for online renewal electronic notifications for each vaccine program facility	E	Yes	
ability to suspend ordering capabilities for a facility pending approval of vaccine program enrollment	E	Yes	
ability to re-activate ordering capabilities for a facility when a vaccine program enrollment is approved	E	Yes	
ability to send electronic communications to organization/facility contacts	E	Yes	
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	
ability to send electronic communications directly from the IIS	O	Yes	
ability to send electronic communications directly from the IIS to multiple recipients	O	Yes	
ability to notify more than one user at a participating vaccine program facility of any vaccine program notification	O	Yes	
ability for the jurisdictional vaccine program admin to customize vaccine program enrollment alerts to participating vaccine program facilities when needed	O	Yes	
ability for the jurisdictional vaccine program admin to modify the date for online renewal electronic notifications for each participating vaccine program facility	O	Yes	
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	

4.2.3.1.3. Manage Users

Requirement: The IIS must/should have…	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
ability for jurisdictional admin to search for user accounts by user-defined criteria	**E**	**Yes**	
ability for jurisdictional admin to view all user accounts	E	Yes	
ability for organization admin to search all user accounts associated with their organization	E	Yes	
ability for organization admin to view all user accounts associated with their organization	E	Yes	
ability to sort users by user defined-criteria	O	Yes	
ability for admin to manage user accounts	**E**	**Yes**	
ability to track the progress of a new user registration	O	Yes	
ability for admin to add new users	E	Yes	
ability for admin to modify user accounts	E	Yes	
ability for admin to inactivate user accounts	E	Yes	
ability for jurisdictional admin to inactivate multiple accounts in one transaction	O	Yes with customization*	A custom workflow can be configured to enable jurisdictional admins to inactivate multiple accounts in one transaction, including capturing the reason for inactivation. This applies to accounts the admin is authorized to manage within their jurisdiction. SSG can configure this workflow to meet the Agency's requirements.
ability for organization admin to inactivate user accounts associated with their organization	E	Yes	
ability to store reason for inactivation of user account	E	Yes	
ability for jurisdictional admin to reactivate an inactivated account	E	Yes	
ability to electronically notify a user that their account is locked (inaccessible) as per jurisdictional security policy	O	Yes	
ability to electronically notify a user that their account is inactive	O	Yes	
capture clinician activity status (out of state, loss of certification, change of practice status, other)	O	Yes	
ability for jurisdictional admin to assign a role to authorized users	E	Yes	
ability for organization admin to assign a role to authorized users within their organization	E	Yes	
ability to authenticate user	**E**	**Yes**	
ability to access the system through an authorized username and password	E	Yes	
ability to support access via single-sign in for jurisdictional users	O	Yes	
ability to switch between multiple organizations	O	Yes	
ability to view jurisdictional policy agreements	E	Yes	
support multi-factor authentication per jurisdictional policy	O	Yes	
ability to generate electronic notification to authorized user of account credentials	**E**	**Yes**	
ability to electronically notify authorized users of their username	E	Yes	
ability to electronically notify authorized users of their temporary password in a separate notification	E	Yes	
ability to generate electronic notification at periodic intervals to authorized users of their pending account password expiration	E	Yes	
ability for jurisdictional admin to configure the periodic intervals for generation of notifications to authorized users of their pending account password expiration	O	Yes	
ability to support temporary password which will be required to change during initial log in	E	Yes	
ability to support temporary password which will expire in X number of days determined by policy	E	Yes	
ability for users to change their own passwords per program/jurisdiction security policy	E	Yes	
ability for users to reset their password per program/jurisdiction security policy	E	Yes	
ability to prompt users to change their password at time intervals per program/jurisdiction security policy	E	Yes	

4.2.3.1.4. Support Interoperability

Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
ability to onboard organizations/facilities to facilitate electronic data exchange	E	Yes	
ability to track an organization's/facility's progress through the onboarding process	O	Yes	
ability to capture EHR system specification details	E	Yes	
ability to create a unique username to assign to the organizations/facilities during the test phase	E	Yes	
ability to create a unique password to assign to the organizations/facilities during the test phase	E	Yes	
ability to electronically alert the vendor/organization when the certificate for transport is going to expire in X time period	E	Yes	
ability to store digital certificate information	E	Yes	
ability to validate that the transport layer between the test site and IIS is functional	E	Yes	
ability to validate system connectivity prior to the submission of test data	E	Yes	
ability to identify data formatting errors during testing	E	Yes	
ability to provide test message submission summary report to the EHR vendor	E	Yes	
ability for EHR vendor to view details regarding the processing of test data in terms of errors and warnings in the messages	E	Yes	
ability for IIS authorized staff to review and approve onboarding forms	E	Yes	
ability for IIS staff to review and reject onboarding forms	E	Yes	
ability for applicant to edit a rejected onboarding application	E	Yes	
ability for applicant to save a rejected onboarding application	E	Yes	
ability for applicant to resubmit a rejected onboarding application	E	Yes	
ability to compare onboarding application information to current records to determine most current data	E	Yes	
ability to interface with other systems to facilitate electronic data sharing/exchange per jurisdictional policy	E	Yes	
ability to interface with electronic health record systems	E	Yes	
ability to interface with the Immunization Gateway	E	Yes	
ability to interface with an application that facilitates patient scheduling	E	Yes	
ability to exchange data with CDC Vaccine Tracking System (VTrckS) based on most current CDC ExIS Specifications	E	Yes	
ability to order vaccine via electronic interface with VTrckS	E	Yes	
ability to receive vaccine inventory/shipping information	E	Yes	
ability to batch export vaccine inventory for submission to VTrckS	E	Yes	
ability to batch export vaccine ordering information for submission to VTrckS	E	Yes	
ability to batch export facility information	E	Yes	
ability to export vaccine return and wastage data to VTrckS	E	Yes	
ability to use the VTrckS-API for file exchange between the IIS and VTrckS based on CDC requirements and API file specifications	O	Yes	
ability to receive data through an interface with jurisdictional vital records system	E	Yes	***Casetivity*-IIS has the capability to receive data through an interface with jurisdictional vital records systems. The solution supports flat file and HL7-based integration with vital records systems, enabling automatic ingestion of birth data. The IIS solution currently supports birth records via HL7.**
ability to update IIS data from Vital Records for birth events	E	Yes	The IIS solution currently supports birth records via HL7 for birth events. We will work with you to synchronize requirements for all of the Vitals provided data based on the system's capabilities. These birth data records are marked as originating from a trusted source (vitals) and may be restricted to read-only access depending on the user's role. The solution uses a neural network engine to match incoming vital records to existing patients, minimizing duplication while preserving data integrity. Matching configurations can leverage birth certificate number, birth order, and birth mother fields.
ability to update IIS data from Vital Records for death events	E	Yes	
ability to update IIS data from Vital Records for adoption events	E	Yes	
ability to update IIS data from Vital Records for name change events	E	Yes	
ability to detect if a newborn record is a potential duplicate in the IIS	E	Yes	
ability to use new Vital Record data for matched records to update patient demographic data	E	Yes	
ability to update the IIS with date of death from Vital Records data	E	Yes	
ability to prevent updates to IIS records	O	Yes	

ability to support real-time data exchange per the CDC HL7 implementation guide	E	Yes	
ability to process an HL7 message	E	Yes	
ability to respond to an HL7 message	E	Yes	
ability to create an HL7 message	E	Yes	
ability to capture IIS Core Data Elements	E	Yes	
ability to store IIS Core Data Elements	E	Yes	
ability to accept last prior version of HL7 messages	E	Yes	
ability to manually correct a submitted record and resubmit for processing	O	Yes	
ability to support data exchange in non-HL7 format	E	Yes	
ability to import bulk patient demographic information into IIS	E	Yes	
ability to import bulk immunization information into IIS	E	Yes	
ability to export routine, seasonal, and emergency vaccination files (aggregate and de-identified)	E	Yes	
ability to export routine, seasonal, and emergency vaccination files (aggregate and de-identified) automatically via CDC approved	O	Yes	
ability to monitor and troubleshoot data exchange	E	Yes	
ability to view VXU messages submitted by an organization	E	Yes	
ability to view HL7 messages for an organization within a defined date range per jurisdictional policy	E	Yes	
ability to view HL7 ACK messages generated for an organization	E	Yes	
ability to view incoming HL7 QBP messages submitted by an organization	E	Yes	
ability to view RSP messages generated for an organization	E	Yes	
ability to log acknowledgement messages indicating warnings and errors	E	Yes	
ability to retrieve error messages within a specified date range by organization	E	Yes	
ability to retrieve acknowledgment messages within a specified date range by organization	E	Yes	
ability to filter error messages	E	Yes	
ability to filter acknowledgement messages	E	Yes	
ability to sort error messages	E	Yes	
ability to sort acknowledgement messages	E	Yes	

4.2.3.1.5. Ensure Data Quality

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
Patient Matching &	**ability to prevent duplicate patient records in the IIS database**	**E**	**Yes**	
Patient Matching &	ability to automatically identify incoming patient records as potential duplicates	E	Yes	
Patient Matching &	ability to automatically identify existing patient records as potential duplicates	E	Yes	
Patient Matching &	ability to automatically consolidate two or more duplicate records	E	Yes	
Patient Matching &	ability to generate electronic notification of potential duplicates for manual review	E	Yes	
Patient Matching &	ability to automatically match an incoming patient record with existing records to avoid a duplicate record being created	E	Yes	
Patient Matching & Deduplication	**ability to set thresholds for patient matching**	**E**	**Yes**	
Patient Matching &	ability to view all potential duplicate patient records for an individual patient simultaneously	E	Yes	
Patient Matching &	ability for jurisdictional admin to edit thresholds to increase the probability of a match	E	Yes	
Patient Matching &	ability for jurisdictional admin to edit thresholds to reduce the probability of a match	E	Yes	
Patient Matching &	**ability to flag potential duplicate patient records for manual review that cannot be resolved automatically**	**E**	**Yes**	
Patient Matching &	ability to view all potential duplicate patient records simultaneously	E	Yes	
Patient Matching &	ability for admin to manually merge patient records	E	Yes	
Patient Matching &	ability for organizational/facility user to manually merge patient records from their own organization/facility	E	Yes	
Patient Matching &	ability to manually flag two or more patient records as potential duplicates	E	Yes	
Patient Matching &	ability to prevent manual review of records previously indicated as "not a duplicate"	E	Yes	
Patient Matching &	ability to flag a patient as "not a duplicate" during manual review	E	Yes	
Patient Matching &	ability to maintain "not a duplicate" flag for resolved patient records	E	Yes	
Patient Matching &	ability to select data elements from the patient records to maintain within the consolidated record	E	Yes	
Patient Matching &	ability to retain "pre-merged" records for reference	E	Yes	
Patient Matching &	ability to separate patient records that were incorrectly merged	E	Yes	
Vaccination Event	**ability to prevent potential duplicate vaccination events at the immunization level**	**E**	**Yes**	
Vaccination Event	ability to automatically identify incoming vaccination event as potential duplicates	E	Yes	
Vaccination Event	ability to automatically select the most accurate vaccination event based on deduplication rules	E	Yes	
Vaccination Event	ability to automatically identify existing vaccination events as potential duplicates	E	Yes	
Vaccination Event	ability to manually flag potential duplicate vaccination events for manual review	E	Yes	
Vaccination Event	ability to display potential duplicate vaccine records for an individual patient	E	Yes	
Vaccination Event	ability to manually merge a duplicate vaccination event	E	Yes	
Vaccination Event	ability to manually delete a duplicate vaccination event	E	Yes	
Vaccination Event	ability to automatically consolidate two or more duplicate vaccination events	E	Yes	
Vaccination Event	ability to retain "pre-merged" or "pre-consolidated" vaccination events for reference	E	Yes	
Vaccination Event	ability to separate vaccination events that were incorrectly merged or consolidated	E	Yes	

4.2.3.1.6. Evaluate and Forecast

Capability	Requirement: The IIS must/should have...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
Clinical Decision Support	ability to provide immunization clinical decision support according to ACIP recommendations	E	Yes	
Clinical Decision Support	ability to support a vaccine clinical decision support algorithm aligned with the CDC CDSi logic specifications	E	Yes	
Clinical Decision Support	ability for jurisdictional admin to update the CDS rules	E	Yes	
Clinical Decision Support	ability to evaluate a patient's' immunization history according to the ACIP Child and Adolescent	E	Yes	
Clinical Decision Support	ability to evaluate a patient's' immunization history according to the ACIP Recommended Catch-up	E	Yes	
Clinical Decision Support	ability to evaluate a patient's' immunization history according to the ACIP Adult Immunization Schedule	E	Yes	
Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Child and Adolescent Immunization Schedule and	E	Yes	
Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Recommended Catch-up Immunization Schedule	E	Yes	
Clinical Decision Support	ability to generate a vaccine forecast according to the ACIP Adult Immunization Schedule and a patient's	E	Yes	
Clinical Decision Support	ability to display and highlight vaccines that are due	E	Yes	
Clinical Decision Support	ability to display and highlight vaccines that are overdue	E	Yes	
Clinical Decision Support	ability to display an indication when a vaccine series is complete	E	Yes	
Clinical Decision Support	ability to display vaccine-specific contraindications according to CDC lists of vaccine contraindications	O	Yes	
Clinical Decision Support	ability to take into account contraindications and precautions in the vaccine forecast	E	Yes with customization*	*Casetivity*- IIS supports immunization forecasting based on the forecasting approach selected by the jurisdiction. When using the integrated HLN ICE (Immunization Calculation Engine) forecaster, contraindications and precautions are not incorporated into vaccine forecasting because this capability is not currently supported by the ICE forecasting engine. If the jurisdiction elects to use *Casetivity* -IIS forecasting capabilities, SSG can implement support for incorporating contraindications and precautions into vaccine forecasting through customization to meet jurisdiction-specific business requirements.
Clinical Decision Support	ability to take into account evidence of immunity in the vaccine forecast	E	Yes	*Casetivity* -IIS supports consideration of documented evidence of immunity when generating vaccine forecasts. Depending on the implementation approach selected by the jurisdiction, forecasting may be provided through the integrated HLN ICE (Immunization Calculation Engine) forecaster or through *Casetivity* -IIS forecasting capabilities. The selected forecasting approach can incorporate documented evidence of immunity, such as laboratory-confirmed disease history or serologic evidence, when determining vaccine recommendations. This ensures that clinical decision support reflects the patient's documented immune status and avoids unnecessary vaccination recommendations where evidence of immunity has been established.
Clinical Decision Support	ability to generate a forecast of specific vaccines required for individuals who travel outside the US	O	Yes with customization*	*Casetivity* -IIS generates vaccine forecasts for travel-related immunizations to support individuals traveling outside the United States. Depending on the implementation approach selected by the jurisdiction, forecasting may be provided through the integrated HLN ICE (Immunization Calculation Engine) forecaster or through *Casetivity* -IIS forecasting capabilities. When using the integrated HLN ICE forecaster, the current forecasting engine supports travel and non-routine vaccine forecasting for Cholera, Japanese Encephalitis, Typhoid, and Yellow Fever. Vaccine forecasts are generated in accordance with the forecasting rules supported by the selected forecasting approach.
Clinical Decision Support	ability to maintain historical records of effective dates of previous forecast schedules	O	Yes	*Casetivity* -IIS provides this capability out-of-the-box (OOTB). The system maintains historical records of effective dates of previous forecast schedules as part of its Clinical Decision Support functionality for evaluation and forecasting.
Clinical Decision Support	ability to review an immunization schedule that was appropriate at the time of administration	O	Yes with customization*	*Casetivity*- IIS currently uses the most current immunization schedule when evaluating immunization events and providing patient immunization forecasts. The ability to review an immunization schedule that was appropriate at the time of administration—meaning a historical schedule from a past point in time—is not available in the base solution but can be achieved through configuration. This configuration would enable the system to apply and display the immunization schedule that was in effect when a particular dose was administered, rather than evaluating historical doses against today's current schedule. This functionality is valuable for accurately assessing whether past immunizations were compliant with the guidelines in place at the time they were given.

Clinical Decision Support	ability to apply an immunization schedule that was appropriate at the time of administration	O	Yes with customization*	*Cosetivity*- IIS currently uses the most current immunization schedule when evaluating immunization events and providing patient immunization forecasts. The ability to apply an immunization schedule that was appropriate at the time of administration—meaning the schedule that was in effect when a historical vaccination was given—is not part of the base solution but can be added through configuration. This configuration will enable the system to evaluate past immunization events using the clinical decision support rules and schedules that were valid at the time those doses were administered, rather than applying today's schedule retroactively. This ensures accurate historical assessments and supports proper forecasting based on what was clinically appropriate at the point of care.
Clinical Decision Support	ability to account for immune globulins in vaccine forecasting	E	Yes with customization*	*Cosetivity*- IIS supports immunization forecasting based on the forecasting approach selected by the jurisdiction. When using the integrated HLN ICE (Immunization Calculation Engine) forecaster, immune globulins are not incorporated into vaccine forecasting because this capability is not currently supported by the ICE forecasting engine. If the jurisdiction elects to use *Cosetivity* -IIS forecasting capabilities, SSG can implement support for incorporating immune globulins into vaccine forecasting through customization to meet jurisdiction-specific business requirements.
Clinical Decision Support	ability to create test cases for reuse during user acceptance testing	E	Yes	
Clinical Decision Support	ability to save test cases for reuse during user acceptance testing	E	Yes	
Clinical Decision Support	ability to compare the expected results of the forecasting test case to the actual results observed by the	E	Yes	
Reminder/Recall	**ability to generate patient-specific reminder/recall notifications**	**E**	**Yes**	
Reminder/Recall	ability to select one or more vaccines for generating reminder/recall notifications	E	Yes	
Reminder/Recall	ability to view the date the reminder/recall notice was sent to a patient	O	Yes	
Reminder/Recall	ability to generate lists of patients in need of a reminder or recall notification by organization	E	Yes	
Reminder/Recall	ability to generate reminder/recall notifications per consent designation	E	Yes	
Reminder/Recall	**ability to generate patient-specific reminder/recall notices by user-defined parameters**	**E**	**Yes**	
Reminder/Recall	ability to generate reminder/recall in user-defined format	E	Yes	
Reminder/Recall	ability to select the age of the cohort when generating reminder/recall notifications	E	Yes	
Reminder/Recall	ability to print patient-specific reminder/recall notices by user-defined parameters	E	Yes	
Reminder/Recall	ability to generate patient specific reminder/recalls in a user-defined format	E	Yes	
Reminder/Recall	ability for an end user to generate patient specific reminder/recalls in accordance with HIPAA and	E	Yes	
Reminder/Recall	ability for an end user to print patient specific reminder/recalls in accordance with HIPAA and jurisdictional	E	Yes	
Reminder/Recall	ability to generate vaccine recall notices by facility based on vaccine name, vaccination date range, and lot	O	Yes	
Reminder/Recall	ability to generate vaccine recall notices by administering provider based on vaccine name, vaccination date	O	Yes	
Reminder/Recall	ability to set the limit/number of times a patient will receive a reminder/recall	O	Yes	
Reminder/Recall	ability to modify the limit/number of times a patient will receive a reminder/recall	O	Yes	
Reminder/Recall	ability to exclude a patient who has met the limit/number of times to receive a reminder/recall	O	Yes	
Reminder/Recall	ability to generate a list of phone numbers for patients needing reminder/recall	O	Yes	
Reminder/Recall	**ability to manually review a patient list for a reminder/recall notification**	**E**	**Yes**	
Reminder/Recall	ability to flag patients to exclude before sending a reminder/recall notification	O	Yes	
Reminder/Recall	ability to establish a time interval between reminder recall notices (e.g., 90 days or 60 days)	O	Yes	
Reminder/Recall	ability to generate a reminder/recall notifications for patients with an active status for their organization	E	Yes	
Reminder/Recall	ability to generate reports that include reminder/recall history for specific date range	O	Yes	
Reminder/Recall	ability to make all reminder/recall data accessible to authorized users for a predetermined period of time	O	Yes	
Reminder/Recall	ability to aggregate multiple notices going to the same address into one notification	O	Yes with customization*	*Cosetivity* -IIS generates a single notice containing all vaccine groups that require attention. However, out of the box, the system does not combine notices for different patients going to the same address (e.g., siblings living at the same household). SSG can customize *Cosetivity* -IIS to combine notices for patients sharing the same address to meet this requirement.
Coverage Reports	**ability to generate report(s) displaying information on immunization coverage rate(s) among select**	**E**	**Yes**	
Coverage Reports	ability to generate report(s) for organizations and facilities per CDC Immunization Quality Improvement for	E	Yes	
Coverage Reports	ability to generate report(s) on immunization coverage for a user-defined geographic area	E	Yes	
Coverage Reports	ability to generate report(s) on immunization coverage for a patient cohort	E	Yes	
Coverage Reports	ability to view and modify list of patients to be included in immunization coverage report	O	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage trends over time, over a selected timeframe	E	Yes	
Coverage Reports	ability to generate report(s) that display the number of missed opportunities for vaccination	E	Yes	
Coverage Reports	ability to generate report(s) displaying the number of patients late up-to-date for immunization who are up-	E	Yes	

Coverage Reports	ability to generate report(s) that display the number of invalid vaccine doses	E	Yes	
Coverage Reports	ability to generate report(s) displaying vaccine exemption rates	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by user-defined parameters	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by vaccine type	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by age range	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by ethnicity	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by race	E	Yes	
Coverage Reports	ability to generate report(s) displaying immunization coverage by patient sex	O	Yes	

4.2.3.1.7. Manage Patient and Immunization Record

Capability	Requirement: The IIS must/should have…	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**	
Patient Search	ability to search patient record based on one or multiple user-defined parameters	E	Yes	
Patient Search	ability to re-search for a patient record by modifying existing search parameters	E	Yes	
Patient Search	ability to display the list of returned possible patient matches per jurisdictional policy	E	Yes	
Patient Search	ability to select a patient record from the list of possible patient matches	E	Yes	
Add, Edit Patient	**ability to add demographic information to a patient record**	**E**	**Yes**	
Add, Edit Patient	ability to create a new patient record	E	Yes	
Add, Edit Patient	ability to edit demographic information in a patient record	E	Yes	
Add, Edit Patient	ability to insert permanent comments in a patient's record that can be viewed based on	E	Yes	
Add, Edit Patient	ability to display the user who created the permanent comment in a patient's record	E	Yes	
Add, Edit Patient	ability to prevent a patient record from being saved unless required fields are completed, per	E	Yes	
Add, Edit Patient	ability to automatically notify a user when attempting to submit an incomplete patient record	E	Yes	
Add, Edit Patient	ability to store CDC-endorsed core data elements for all patient records	E	Yes	
Add, Edit Patient	ability to store multiple of reported names for each patient to include: first name, middle name, last	E	Yes	
Add, Edit Patient	ability to store multiple patient addresses	O	Yes	
Add, Edit Patient	ability to support multiple patient address type designations (e.g. primary address, vacation address)	O	Yes	
Add, Edit Patient	ability to identify effective dates for use of a patient address	O	Yes	
Add, Edit Patient	ability to store all historic addresses for a patient	O	Yes	
Add, Edit Patient	ability to store country information related to where the patient was born	O	Yes	
demographics	SmartyStreets)	O	Yes	
Add, edit patient	SmartyStreets)	O	Yes	
Add, Edit Patient	ability to automatically create a unique patient ID number	E	Yes	
Add, Edit Patient	ability to automatically associate patient ID number to the patient's record	E	Yes	
Add, Edit Patient	ability to track patients of all ages per jurisdictional law or policy	E	Yes	
Add, Edit Patient	ability to store mother's HBsAg status for a patient	O	Yes	
Add, Edit Patient	ability to store a patient's occupation	E	Yes	
Add, Edit Patient	ability to designate patient as belonging to a priority group for vaccination	O	Yes	
Add, Edit Patient	ability to store multiple patient identifiers	E	Yes	
Add, Edit Patient	ability to assign patient records to a cohort	E	Yes	
Add, Edit Patient	ability to assign patient records to multiple cohorts	E	Yes	
Add, Edit Patient	ability to view patient records by cohort	E	Yes	
Add, Edit Patient	ability to remove patient records from a cohort	E	Yes	
Patient Status	**ability to manage patient status at the organization/facility level**	**E**	**Yes**	
Patient Status	ability to store active patient status at the organization/facility level	E	Yes	
Patient Status	ability to store inactive patient status at the organization/facility level	E	Yes	
Patient Status	ability to edit active patient status at the organization/facility level	E	Yes	
Patient Status	ability to edit inactive patient status at the organization/facility level	E	Yes	
Patient Status	ability to store reason for inactive status of patients at the organizational/facility level	E	Yes	
Patient Status	ability to edit multiple patients status in one action	O	Yes with customization*	SSG can meet the requirement to edit multiple patients' statuses in a single action through customization. The proposed approach is to create a workflow that enables authorized users to search for patients by organization and applicable demographic and location criteria, as determined with the Agency.
Patient Status	**ability to manage patient status at the geographic jurisdictional level**	**E**	**Yes**	
Patient Status	ability to store active patient status at the geographic jurisdiction level	E	Yes	
Patient Status	ability to store inactive patient status at the geographic jurisdictional level	E	Yes	
Patient Status	ability to edit active patient status at the geographic jurisdictional level	E	Yes	
Patient Status	ability to edit inactive patient status at the geographic jurisdictional level	E	Yes	
Patient Status	ability to store reason for inactive status of patients at the geographic jurisdictional level	O	Yes	
Patient Status	ability to restrict access to patient records that have been placed in an inactive status	O	Yes	
Patient Status	ability to restrict edits to patient records that have been placed in an inactive status	O	Yes	
Patient Consent	**ability to manage patient consent per jurisdictional policy**	**E**	**Yes**	
Patient Consent	ability to update patient consent on a patient's record	E	Yes	
Patient Consent	ability to opt out a patient from participating in the IIS	E	Yes	Supports jurisdiction-configurable patient participation and consent management workflows.

Patient Consent	ability to opt in a patient for participation in the IIS	E	Yes	Supports jurisdiction-configurable patient participation and consent management workflows.
Patient Consent	ability to enable access to a patient record per consent designation	E	Yes	
Patient Consent	ability to enable updates to a patient record per consent designation	E	Yes	
Add, Edit Patient	ability to add vaccination event information to a patient record	E	Yes	
Add, Edit Patient	ability to edit vaccine information in a patient record	E	Yes	
Add, Edit Patient Immunization	ability to mark vaccine information in a patient record for deletion	O	Yes	Supports administrative review and data correction workflows by allowing immunization records to be flagged for deletion processing.
Add, Edit Patient	ability to add reason for deletion of vaccine information in a patient record	O	Yes	
Add, Edit Patient	ability to capture vaccine eligibility by vaccine dose for publicly purchased vaccine	E	Yes	
Add, Edit Patient	ability to store vaccine eligibility by vaccine dose for publicly purchased vaccine	E	Yes	
Add, Edit Patient	ability to report multiple doses administered to the same patient on the same administration date via	E	Yes	
Add, Edit Patient	ability to store all CDC-endorsed core data elements related to vaccine events	E	Yes	
Add, Edit Patient Immunization	ability to enter vaccination substandard or otherwise compromised flag	E	Yes	
Add, Edit Patient	ability to view submitted vaccination event information on a patient's record	E	Yes	
Add, Edit Patient	ability to store adverse reactions in accordance with Vaccine Recommendations and Guidelines of	E	Yes	
Add, Edit Patient Immunization	ability to flag an adverse reaction as having been reported to VAERS	E	Yes	Supports adverse event tracking workflows by allowing reported reactions to be associated with VAERS reporting status within the patient immunization record.
Add, Edit Patient	ability to store patient vaccination event funding eligibility information	E	Yes	
Add, Edit Patient	ability to print form for signature of vaccine refusal by patient for each individual vaccine antigen	O	Yes	
Add, Edit Patient	ability to ensure that the default lot number is from the oldest lot when entering an administered	E	Yes	
Add, Edit Patient	ability to record administration of vaccination regardless if vaccine has since expired in inventory	E	Yes	
Add, Edit Patient	ability to track vaccinations that require adjuvant	E	Yes	
Print/Export Record	ability to securely print a patient immunization record	E	Yes	
Print/Export Record	ability to include evaluated history in the printable version of the patient record	E	Yes	
Print/Export Record	ability to include the forecast in the printable version of the patient record	E	Yes	
Print/Export Record	ability to include immunity in the printable version of the patient record	E	Yes	
Print/Export Record	ability to securely export a patient immunization record	E	Yes	
Print/Export Record	ability to export a patient record in user-defined format	O	Yes	
Mass Vaccination	ability to support mass vaccination operations	E	Yes	
Mass Vaccination	ability to rapidly capture patient demographic information offline during mass vaccination clinic for	E	Yes	
Mass Vaccination	ability to rapidly capture vaccine information offline during mass vaccination clinic for later	E	Yes	
Mass Vaccination	ability to support rapid capture of patient demographic information during mass vaccination clinic	E	Yes	
Mass Vaccination	ability to support rapid capture of vaccine information during mass vaccination clinic	E	Yes	
Mass Vaccination	ability to administer vaccines during public health emergency without impacting the patient's status	O	Yes	
Mass Vaccination	ability for jurisdictional admin to flag/indicate org/facility participation in mass vaccination event	O	Yes	

4.2.3.1.8. Manage Vaccine Inventory

Capability	Requirement: The IIS must/should have…	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
Vaccine Inventory	ability to search inventory by user-defined parameters	E	Yes	
Vaccine Inventory	ability to search the inventory by funding source	E	Yes	
Vaccine Inventory	ability to search inventory by vaccine type	E	Yes	
Vaccine Inventory	ability to search inventory by vaccine lot number	E	Yes	
Vaccine Inventory	ability to search inventory by vaccine NDC code	E	Yes	
Add, Edit Vaccine	ability to manage vaccine inventory	E	Yes	
Add, Edit Vaccine Inventory	ability to support visualization of current vaccine inventory	E	Yes	
Add, Edit Vaccine	ability to edit inventory funding source at the lot level	E	Yes	
Add, Edit Vaccine	ability to edit inventory funding source at the vaccine level	E	Yes	
Add, Edit Vaccine	ability to add vaccine information to inventory	E	Yes	
Add, Edit Vaccine	ability to support barcode scanning system to electronically upload vaccine inventory to the IIS	O	Yes	
Add, Edit Vaccine	ability to view current inventory list by facility	E	Yes	
Add, Edit Vaccine	ability to view current inventory list by organization	E	Yes	
Add, Edit Vaccine	ability for jurisdictional admin to edit organization/facility inventory	E	Yes	
Add, Edit Vaccine	ability to manage vaccine borrowed from lots belonging to one funding source to lots belonging to another funding source	O	Yes	
Add, Edit Vaccine	ability to reclassify funding source of borrowed vaccine from private to public or vice versa for replacement cases	O	Yes	
Add, Edit Vaccine	ability to view storage capability	E	Yes	
Add, Edit Vaccine	ability to document vaccine storage and handling events such as temperature excursions	E	Yes	
Add, Edit Vaccine	ability to store storage capability	E	Yes	
Vaccine Ordering	ability for rule based logic to recommend vaccine order quantity	E	Yes	
Vaccine Ordering	ability to alert user when "reorder recommendation" inventory level is reached	O	Yes	
Vaccine Ordering	ability to pre-populate order with recommended quantities based on inventory, doses reported as administered to IIS	E	Yes	
Vaccine Ordering	ability to edit pre-populated order quantity	E	Yes	
Vaccine Ordering	ability to order vaccines	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to activate vaccines available for ordering	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to inactivate vaccines available for ordering	E	Yes	
Vaccine Ordering	ability to order publicly-purchased vaccines	E	Yes	
Vaccine Ordering	ability to view all orders by user-defined parameters	O	Yes	
Vaccine Ordering	ability to update delivery hours to receive shipments	E	Yes	
Vaccine Ordering	ability to enter a reason for vaccine orders outside the recommended order quantity	E	Yes	
Vaccine Ordering	ability to search and view past vaccine orders by facility within a specified timeframe	E	Yes	
Vaccine Ordering	ability to verify contact information during each order without leaving ordering workflow	E	Yes	
Vaccine Ordering	ability to update contact information during each order without leaving ordering workflow	E	Yes	
Vaccine Ordering	ability to save an unsubmitted order	E	Yes	
Vaccine Ordering	ability to update organization/facility contact information before submitting a vaccine order	E	Yes	
Vaccine Ordering	ability to cancel unsubmitted or unprocessed vaccine orders	E	Yes	
Vaccine Ordering	ability to edit unsubmitted or unprocessed vaccine orders	E	Yes	
Vaccine Ordering	ability to save an unsubmitted order after rejection	E	Yes	
Vaccine Ordering	ability to verify order information before order submitted	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to reject a vaccine order	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to select a reason code when rejecting an order	E	Yes	
Vaccine Ordering	ability to edit an order after rejection	E	Yes	
Vaccine Ordering	ability to resubmit an order after rejection	E	Yes	
Vaccine Ordering	ability to electronically notify the facility of a rejected order	E	Yes	
Vaccine Ordering	ability to track the shipping status of orders	E	Yes	
Vaccine Ordering	ability to verify packing slip information after order is shipped	O	Yes	
Vaccine Ordering	ability to receive electronic notification when order quantity received does not match vaccine order	O	Yes	
Vaccine Ordering	ability to receive electronic notification when vaccine order received is damaged	O	Yes	
Vaccine Ordering	ability to request shipping label(s) for nonviable vaccine subject to return	O	Yes	
Vaccine Ordering	ability to search for past vaccine returns within a specified timeframe	E	Yes	
Vaccine Ordering	ability to view past vaccine returns within a specified time frame	E	Yes	
Vaccine Ordering	ability to pre-book vaccine orders	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to allocate vaccine inventory per user defined parameters	E	Yes	
Vaccine Ordering	ability to activate vaccine ordering functionality for all designated organizations/facilities during a public health emergency	E	Yes	
Vaccine Ordering	ability for jurisdictional admin to create order sets	E	Yes	
Review/Approve Order	ability for jurisdictional admin to review order	E	Yes	
Review/Approve Order	ability to support a rules-based decision logic to approve or reject order if above or below recommended order quantity	O	Yes	
Review/Approve Order	ability for jurisdictional admin to approve order	E	Yes	
Review/Approve Order	ability for jurisdictional admin to adjust order	E	Yes	
Review/Approve Order	ability for jurisdictional admin to electronically accept VFC vaccine into inventory	E	Yes	
Review/Approve Order	ability to accept each vaccine product in the IIS after shipment is received	E	Yes	
Vaccine Dose	ability to automatically decrement vaccine doses from inventory when matched vaccine doses are reported as administered	E	Yes	
Vaccine Dose	ability to automatically match vaccine doses reported as administered to vaccine doses in inventory to facilitate dose decrementing	E	Yes	
Vaccine Dose	ability to automatically decrement vaccine inventory in real-time via HL7 messaging	E	Yes	

Vaccine Dose	ability to automatically decrement vaccine inventory in real-time via UI data entry	E	Yes	
Vaccine Inventory	ability to reconcile vaccine doses currently in physical storage with vaccine doses reflected in system inventory	E	Yes	
Vaccine Inventory	ability to document reductions in vaccine inventory due to outgoing vaccine transfers	E	Yes	
Vaccine Inventory	ability to electronically document reductions in vaccine inventory due to outgoing vaccine wastage	E	Yes	
Vaccine Inventory	ability to enter current number of vaccine doses on-hand in physical storage	E	Yes	
Vaccine Inventory	ability to track and manage doses for vaccines: on hand, administered, wasted, expired, ordered, recalled, returned, transferred	E	Yes	
Vaccine Inventory	ability to enable removal of recalled lots from active inventory	E	Yes	
Vaccine Inventory	ability to print a reconciliation worksheet	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to approve vaccine transfers	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to initiate VFC vaccine transfers	O	Yes	
Vaccine Transfers	ability to accept VFC vaccine transfers	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to reject vaccine transfers	O	Yes	
Vaccine Transfers	ability to search and view past vaccine transfers within a specified timeframe	O	Yes	
Vaccine Transfers	ability for jurisdictional admin to allow for direct vaccine transfer between facilities without jurisdictional pre-approval, but with jurisdictional visibility/oversight.	O	Yes	
Vaccine Wastage	ability to manage vaccine wastage	E	Yes	
Vaccine Wastage	ability to determine the total cost of wasted vaccine by user-defined parameters	E	Yes	
Vaccine Wastage	ability for jurisdictional admin to modify inventory quantity to reflect wastage	E	Yes	
Vaccine Wastage	ability for jurisdictional admin to assign reason for inventory wastage	E	Yes	
Vaccine Wastage	ability to determine the total doses of vaccine wasted by user-defined parameters	E	Yes	
Vaccine Expiration	ability to manage vaccine expiration	E	Yes	
Vaccine Expiration	ability to alert users to vaccine nearing expiration	O	Yes	
Vaccine Expiration	ability to provide alerts for inventory already expired	O	Yes	
Vaccine Expiration	ability for jurisdictional admin to modify inventory quantity removed from available inventory	E	Yes	

4.2.3.1.9. Provide Data Access

Capability	Requirement: The IIS must/should have...	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 includes history and forecast	E	Yes	
Standard Reports	ability to generate a data quality report displaying information on the quality of submitted data	E	Yes	
Standard Reports	ability to generate a report that provides information on patient and vaccine matching and deduplication	E	Yes	
Standard Reports	ability to generate a report that provides information on data quality of data at rest	E	Yes	
Standard Reports	ability to generate data quality reports for HL7 submissions	E	Yes	
Standard Reports	ability to generate VFC reports	E	Yes	
Standard Reports	ability to generate a practice-level patient data report for VFC enrolled sites	E	Yes	
Standard Reports	ability to generate a doses administered report to support accountability for publicly-purchased vaccine	E	Yes	
Standard Reports	ability to generate a doses administered report for VFC enrolled sites	E	Yes	
Standard Reports	ability to generate VFC provider practice profiles	E	Yes	
Standard Reports	ability to generate a report showing the total number of select vaccines administered each month by facility	E	Yes	
Standard Reports	ability to generate a report displaying a change in vaccine administration patterns over a selected timeframe	E	Yes	
Standard Reports	ability to generate duplicate/merge record reports	E	Yes	
Standard Reports	ability to generate reports about IIS users	E	Yes	
Standard Reports	ability to generate vaccine management reports	E	Yes	
Standard Reports	ability to generate a report listing/identifying patients who received a recalled vaccine	E	Yes	
Standard Reports	ability to generate a report of patients declining or refusing vaccinations	O	Yes	
Standard Reports	ability to generate a report to calculate a facility's average vaccine usage	O	Yes	
Standard Reports	ability to generate VFC accountability reports for managing VFC inventories and orders	E	Yes	
Standard Reports	ability to generate vaccine inventory reports	E	Yes	
Standard Reports	hand	E	Yes	
Standard Reports	ability to generate a report that provides/displays information about inventory transactions	E	Yes	
Standard Reports	ability to generate report(s) that display information about vaccine order history	O	Yes	
Standard Reports	ability to generate report(s) that display information about vaccine wastage and returns	E	Yes	
Standard Reports	specific timeframe	E	Yes	
Standard Reports	ability to generate a report providing information about influenza pre-book orders	E	Yes with customization*	This capability can be customized during the project to meet the Agency's requirements.
Standard Reports	ability to query vaccine ordering patterns over a selected timeframe to indicate trends	O	Yes	
Standard Reports	ability to generate reports that provide information about organizations and facilities	O	Yes	
Standard Reports	ability for jurisdictional admin to generate report that lists immunizing facilities	O	Yes	
Standard Reports	ability for jurisdictional admin to generate a report that provides information on	O	Yes	
Standard Reports	ability for jurisdictional admin to access utilization of report/usage statistics	O	Yes	
Standard Reports	ability to generate reports that provide information about students and their immunization histories for school compliance	E	Yes	
Standard Reports	ability to generate report of student exemptions by type (medical, religious)	E	Yes	
Standard Reports	ability to generate a record of students' immunizations for school purposes	E	Yes	
Standard Reports	ability to generate exclusion letters stating which vaccine(s) a student needs to come into compliance with requirements and be permitted to attend school	E	Yes with customization*	SSG can provide this customization during the project to meet the Agency's requirements.
Standard Reports	ability to generate reports for individuals vaccinated during a mass vaccination event	E	Yes	
Standard Reports	ability to generate doses administered reports for priority groups during a public health	E	Yes	
Standard Reports	ability to generate a report that provides information about the status of the system in	E	Yes	
Ad Hoc Queries &	ability to generate queries and reports based on user-defined parameters	E	Yes	
Ad Hoc Queries &	ability to schedule an ad hoc query to run on a predetermined interval (i.e., daily, weekly,	E	Yes	

Ad Hoc Queries & Reports	ability to generate reports with a user-defined report format	E	Yes	*Casetivity* provides a ReportBuilder page to assist users in creating and configuring reports, giving them the power to decide the available input filters, output fields, sorting, and report logic. Administrators can publish a base report that can be customized further by end users, allowing them to default their own input filter values, hide/show filter fields, and customize the output columns and sorting. Reports can be exported in multiple formats including PDF, XLSX, CSV, TXT, and XML to meet various user-defined format needs.
Ad Hoc Queries &	ability to generate reports across geographic hierarchy levels	E	Yes	
Ad Hoc Queries &	ability to generate data to inform the public via website dashboards or similar means	E	Yes	
Ad Hoc Queries &	ability to store saved report templates	E	Yes	
Ad Hoc Queries &	ability to modify saved report templates	E	Yes	
Ad Hoc Queries & Reports	ability to inactivate (archive) saved report templates	E	Yes with customization*	Currently, report definitions can be deleted and manually restored from a previous copy of the configuration files. If this approach does not meet the Agency's requirements, SSG can add a custom mechanism that applies a status to report definitions, enabling authorized users to inactivate (archive) saved report templates rather than delete them. This capability can be developed within *Casetivity*- IIS through customization.
Ad Hoc Queries &	ability to modify a query	E	Yes	
Ad Hoc Queries &	ability to delete a query	E	Yes	
Ad Hoc Queries &	ability to save an ad hoc query	E	Yes	
Ad Hoc Queries & Reports	ability to create a map using geocodes for statistical reporting	O	Yes with customization*	*Casetivity* -IIS provides dashboard report tiles that show a geocoded map for a single statistic. Allowing the user to choose and adjust the filters on-demand for the report would require additional configuration, SSG can configure this capability to meet the Agency's requirements. Additionally, *Casetivity* -IIS can interface with data warehouses or enterprise tools such as Tableau for enhanced data visualization capabilities.
Print/Export Reports	**ability to export IIS data for use in other systems**	**E**	**Yes**	
Print/Export Reports	ability to export data in user-defined formats	E	Yes	
Print/Export Reports	ability to export aggregate level de-identified data	E	Yes	
Print/Export Reports	ability to export record level de-identified data	E	Yes	
Print/Export Reports	**ability to print reports**	**E**	**Yes**	
Consumer Access	**ability for authorized consumers to access personal IIS data per jurisdictional policy**	**E**	**Yes**	
Consumer Access	ability for authorized consumer to print forecast	O	Yes	
Consumer Access	ability for authorized consumer to print patient immunization record	E	Yes	
Consumer Access	ability for authorized consumer to print an official immunization history	E	Yes	
Consumer Access	ability for authorized consumer to retrieve a verifiable digital vaccine credential without	E	Yes	
Consumer Access	ability for authorized consumer to view immunization forecast	E	Yes	
Consumer Access	ability for authorized consumer to view patient information	E	Yes	
Consumer Access	ability for authorized consumer to view patient immunization record	E	Yes	
Consumer Access	ability for patient/patient representative to opt in for reminder/recall notifications	O	Yes	
Consumer Access	ability for patient/patient representative to opt out of reminder/recall notifications	O	Yes	

4.2.3.1.10 Non-functional

Attribute	Sub Characteristic	Requirement: The IIS must/should...	Priority: E, O (essential, optional)	Vendor response: Yes, Yes with customization*, No *Comment required	Vendor comment(s)
Performance	Time Behavior	support a responsive user interface	E	Yes	
Performance	Time Behavior	support application launch, i.e. time between user initiation and application start, in less than 10 seconds	E	Yes	
Performance	Time Behavior	support response to a user navigation action (e.g., mouse movement, keypresses, navigation) in less than 1 second	E	Yes	
Performance	Time Behavior	support response to process submitted information via direct data entry in less than 4 seconds	E	Yes	
Performance	Time Behavior	support generation of a standard, pre-configured report in less than 30 seconds	E	Yes	
Performance	Time Behavior	support responsive data exchange system interfaces	E	Yes	
Performance	Time Behavior	support electronic response to a submitted HL7 message in 5 seconds or less, 95% of the time	E	Yes	
Performance	Capacity	support up to 1000 concurrent users of the user interface without performance degradation	E	Yes	
Performance	Capacity	support multiple users viewing the same data at the same time	E	Yes	
Performance	Capacity	support users using the same function at the same time without degrading IIS performance	E	Yes	
Performance	Resource	support resource-intensive tasks without degrading IIS performance	E	Yes	
Performance	Resource	support user queries via the user interface without degrading IIS performance	E	Yes	
Performance	Resource	support generation of ad hoc reports without degrading IIS performance	E	Yes	
Performance	Resource	support data extracts without degrading IIS performance	E	Yes	
Performance	Capacity	support efficient processing of HL7 messages without performance degradation, as per jurisdictional capacity	E	Yes	
Performance	Capacity	support processing of up to 200 of HL7 VXU messages per hour without performance degradation	E	Yes	
Performance	Capacity	support processing of up to 8000 of HL7 QBP messages per hour without performance degradation	E	Yes	
Performance	Capacity	support permanent storage of records as per jurisdictional policy	E	Yes	
Performance	Capacity	support storage of unlimited number of organization records	E	Yes	
Performance	Capacity	support storage of unlimited number of user records	E	Yes	
Performance	Capacity	support storage of unlimited number of patient records	E	Yes	
Performance	Capacity	support storage of unlimited number of patient immunization records	E	Yes	
Usability	Accessibility	meet the United States Access Board Section 508 Standards	E	Yes	
Usability	Operability	support best practices for web application session management (e.g., cookies, cache) as recommended by the Open Web Application Security Project (OWASP)	E	Yes	*Cosetivity-IIS implements secure web application session management in alignment with industry best practices. The solution uses secure, HttpOnly, and SameSite-flagged cookies, configurable session timeout policies, and server-side session invalidation upon logout. Cache controls are applied to prevent sensitive data from being stored in browser cache. These controls are configurable by jurisdictional administrators to meet WVDHHR security policy requirements.*
Usability	Operability	ability to execute Boolean searches	E	Yes	
Usability	Operability	ability to execute a wildcard searches	E	Yes	
Usability	User error	minimize data entry errors	E	Yes	
Usability	User error	assist in entering data correctly via pick-lists, drop-down boxes, or other easy-to-use options such as predictive	E	Yes	
Usability	User error	indicate required fields for data entry	E	Yes	
Usability	User error	ability to provide alert when required fields are left blank	E	Yes	
Usability	User error	support cross-field checks to ensure accuracy of information where dependencies exist (e.g., warning that a child	E	Yes	
Usability	User error	support spell check functionality with medical terminology for all free text fields	O	Yes	
Usability	User error	error messages (error must be fixed prior to continuing)	E	Yes	
Usability	User interface	support alerts related to user interface response time	O	Yes	
Usability	User interface	support user feedback with a simple indicator for response times between 2-4 seconds	O	Yes	

Usability	User interface	support user feedback with expected response time and percent-done indicator for response times greater than 4 seconds	O	Yes with customization*	*Casetivity*-IIS currently supports user feedback with a simple indicator for response times between 2-4 seconds with most of our response times under 4 seconds. For actions that initiate additional processing, such as saving records or moving to the next step in flows, we display a spinning icon indicator showing that processing is occurring. However, we do not currently provide expected response time estimates or percent done indicators for response times greater than 4 seconds. SSG can configure this capability to meet the Agency's requirements. Users can utilize multiple browser tabs and perform other actions within the system while waiting for the operation to complete so that they aren't ever blocked by a single response. For reports and exports that are expected to be long-running, the system can be configured to process the report asynchronously. When this occurs the user will be informed that the report will run in the background so they can continue with their work. The user will receive an email when the report is complete at which point they can retrieve the report in the UI.
Usability	User interface	support users in stopping an operation expected to take longer than 10 seconds	O	No	*Casetivity*-IIS does not provide a mechanism for users to stop or terminate processing once an operation has been initiated. However, users are not blocked from continuing their work and can work in multiple browser tabs. For operations expected to take longer than 10 seconds, such as long-running reports, the system executes these tasks asynchronously. This allows users to navigate away from the processing screen and perform other actions within the system while waiting for the operation to complete. While users cannot actively cancel an operation in progress, the asynchronous processing design enables them to remain productive rather than waiting for the operation to complete.
Usability	User interface	support users in performing other tasks while waiting for the system to complete tasks expected to take longer	O	Yes	
Reliability	Availability	support availability of the system as per jurisdictional needs	E	Yes	
Reliability	Availability	support access to the web application 99.9% of the time	E	Yes	
Reliability	Availability	support processing of and response to HL7 messages 99.9% of the time	E	Yes	
Reliability	Recoverability	ability to backup the IIS data as per jurisdictional policy	E	Yes	
Reliability	Recoverability	support redundancy of the IIS as per jurisdictional recovery plan	E	Yes	
Reliability	Recoverability	support real-time failover	E	Yes	
Reliability	Recoverability	support the recovery of backed up data as needed	E	Yes	
Reliability	Recoverability	support the restoration of IIS data after an outage or loss	E	Yes	
Reliability	Fault tolerance	support the efficient roll back of software changes as needed	E	Yes	
Security	Non-repudiation	support audit logs for security purposes	E	Yes	
Security	Integrity	ability to electronically notify the system administrator of unauthorized activity	E	Yes	
Security	Authenticity	ability to track all attempted accesses that fail identification, authentication and authorization requirements	E	Yes	
Security	Authenticity	ability to track all accesses that successfully comply with identification, authentication and authorization	E	Yes	
Security	Non-repudiation	ability to maintain audit logs for specified time per jurisdictional policy	E	Yes	*Casetivity*-IIS maintains comprehensive audit logs across the entire solution scope, including application logs, database logs, infrastructure logs, security system logs, user activity logs, and forensic audit logs. The system retains logs online for a minimum of 90 days per jurisdictional policy and maintains backups for 1 year, ensuring compliance with jurisdictional retention requirements. The audit capabilities include: • Configurable retention periods that can be adjusted to meet specific jurisdictional policies • Application-level audit tracking with rich detail accessible through the UI and reporting database • Infrastructure-level logging through AWS CloudTrail for all infrastructure changes • API access logs capturing request details, sources, and timestamps • Custom reporting capabilities to meet specific compliance requirements Jurisdictions can configure audit log retention and access patterns to align with their specific regulatory and operational requirements.
Security	Non-repudiation	ability for jurisdictional admin to search audit log by function performed	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by date and time period	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by date range	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to search audit log by user defined parameters	E	Yes	Jurisdictional administrators can search audit logs by user-defined parameters. The solution includes predefined audit reports and dashboards that can be filtered by user, date, entity type, or action. Administrators can also configure custom reports to meet specific monitoring needs or compliance requirements. For specific use cases, audit searches can be configured as canned reports or exposed directly in the UI. Direct access to the reporting database is also available for jurisdictions that want to perform deeper investigations or conduct more advanced analysis using their own parameters.
Security	Non-repudiation	ability for jurisdictional admin to search audit log by patient identifiers	E	Yes	
Security	Non-repudiation	ability for jurisdictional admin to filter audit log search by user defined parameters	O	Yes	
Security	Non-repudiation	ability for jurisdictional admin to sort audit log search results	O	Yes	
Security	Integrity	store audit data related to user access/viewing of patient records in the system	E	Yes	

Security	Integrity	store date of user access to a patient record	E	Yes	
Security	Integrity	store time of user access to a patient record	E	Yes	
Security	Integrity	store user ID of user access to a patient record	E	Yes	
Security	**Non-repudiation**	**store audit data related to data changes in the system**	**E**	**Yes**	
Security	Non-repudiation	store 'date received' for data modified in the system	E	Yes	
Security	Non-repudiation	store 'time received' for data modified in the system	E	Yes	
Security	Non-repudiation	store 'date updated' for data modified in the system	E	Yes	
Security	Non-repudiation	store 'time updated' for data modified in the system	E	Yes	
Security	Non-repudiation	store user associated with data modified in the system	E	Yes	
Security	**Integrity**	**automatically enforce session timeout for a user when idle period is reached**	**E**	**Yes**	
Security	Integrity	ability for automatic session timeout to be customized per jurisdictional policy	O	Yes	
Security	Integrity	ability to notify the user the session will expire	O	Yes	
Security	Confidentiality	support masking of passwords as they are typed or entered into the user interface	E	Yes	
Security	**Integrity**	**ability for system administrator to terminate user connections**	**E**	**Yes**	
Security	**Confidentiality**	**Safeguard electronic personally identifiable information by implementing the appropriate technical best practices**	**E**	**Yes**	
Security	Confidentiality	ability to encrypt personally identifiable information at rest	E	Yes	
Security	Confidentiality	ability to decrypt personally identifiable information at rest	E	Yes	
Security	Confidentiality	ability to encrypt personally identifiable information during transmission	E	Yes	
Security	Confidentiality	ability to decrypt personally identifiable information during transmission	E	Yes	
Security	**Integrity**	**ability to maintain firewalls per AIRA's Security Guidance Considerations for Immunization Information Systems**	**E**	**Yes**	
Security	Integrity	ability to maintain firewalls for protection of the hosting network	E	Yes	
Security	Integrity	ability to maintain firewalls for protection of the hosting environment	E	Yes	
Security	**Integrity**	**ability to electronically notify the system admin of unauthorized activity**	**E**	**Yes**	
Security	**Integrity**	**ability to support anti-virus protection at current critical patch levels in the hosting environment**	**E**	**Yes**	
Maintainabilit	**Analyzability**	**support event logging**	**E**	**Yes**	
Maintainabilit	Analyzability	ability for system admin to enable event logging on all servers	O	Yes	
Maintainabilit	Analyzability	ability for system admin to enable event logging on all devices	O	No	This is a web-based application, so end user devices are not in scope. However, certain types of errors and information are available in the browser console for troubleshooting with end users. *Casetivity*-IIS does not provide system administrator functionality to enable or disable event logging on individual end user devices, as the application operates through standard web browsers and logging is managed at the application and server level rather than at the device level.
Maintainabilit	Analyzability	ability for system admin to disable event logging on all devices	O	No	This is a web-based application, so end user devices are not in scope. However, certain types of errors and information are available in the browser console for troubleshooting with end users. *Casetivity*-IIS does not provide system administrator functionality to enable or disable event logging on individual end user devices, as the application operates through standard web browsers and logging is managed at the application and server level rather than at the device level.
Maintainabilit	Analyzability	ability for system admin to limit access to event logs, including System, Application, Web and Database logs	O	Yes	
Portability	**Adaptability**	**support use of web browsers per jurisdictional policy**	**E**	**Yes**	
Portability	Adaptability	support use of current version of web browsers	E	Yes	
Portability	Adaptability	support use of last prior version of web browsers	E	Yes	
Portability	**Adaptability**	**support a responsive design that renders properly on multiple devices**	**E**	**Yes**	
Portability	Adaptability	support web client use on a desktop	E	Yes	
Portability	Adaptability	support web client use on a laptop	E	Yes	
Portability	Adaptability	support web client use on a tablet	E	Yes	
Portability	Adaptability	support web client use on a smartphone	E	Yes	
Portability	**Installability**	**be containerized (e.g., Docker or Kubernetes) to support easy installation and system updates**	**E**	**Yes**	
Portability	Installability	be containerized for cloud based environments	O	Yes	

4.2.3.2. System Compatibility Requirements: The IIS must be designed to operate reliably and efficiently within a variety of standard computing environments.

Casetivity-IIS is a cloud-based, vendor-hosted Software as a Service (SaaS) solution designed to operate reliably and efficiently across standard computing environments. The system is fully accessible through current versions of major web browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari, and requires no specialized hardware, local software installation, plugins, or elevated user permissions. This browser-based architecture simplifies deployment, reduces IT overhead, and provides secure, high-performance access for users across public health agencies, providers, and partner organizations.

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

Yes. SSG confirms that the proposed Immunization Information System (IIS) is cloud-based software with hosting provided by SSG as the vendor.

Casetivity-IIS is a Commercial Off-The-Shelf (COTS) product hosted on a secure cloud platform. SSG hosts *Casetivity*-IIS within Amazon Web Services (AWS), a cloud-based infrastructure that supports containerized deployment for cloud-based environments. The solution leverages AWS's government-grade cloud environment with geographically distinct facilities, implementing advanced cloud infrastructure with rigorous monitoring and redundancy strategies to ensure high availability and scalability.

SSG provides fully managed Software as a Service (SaaS) hosting, which reduces the burden on the Agency's IT resources. The Agency does not need to manage the underlying hosting infrastructure or application environment. SSG handles infrastructure management, periodic vulnerability scans, annual disaster recovery exercises, and ongoing system optimization as part of the hosting service.

The cloud-based architecture provides scalability, reliability, and support for applicable security requirements, providing a robust infrastructure for managing immunization data efficiently. The solution places no limits on the number of users, receives annual updates, and enables SSG to efficiently provision and decommission environments as needed.

This fully managed cloud-based approach meets the requirement for vendor-provided hosting while delivering flexibility, performance, and long-term operational value for the Agency's immunization program.

Casetivity-IIS is architected from the ground up as a modern, cloud-enabled solution. Unlike solutions that rely on legacy architectures, Casetivity-IIS uses a modern, industry-standard design that delivers a scalable, secure, and interoperable solution.

Technical debt is the future cost of extra work caused by choosing software that is old or implemented over time with fast short-term shortcuts over a clean, perfect design. SSG designed *Casetivity*-IIS from the ground up with modern technology, cloud enabled services, and IIS programmatic requirements in mind. *Casetivity*-IIS likely has the least technical debt of all the solutions on the market which makes it much more sustainable.

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.

Yes. *Casetivity*-IIS is fully compatible with major, up-to-date web browsers including Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari. The solution is designed as a modern, cloud-based solution with browser compatibility built into the system architecture. *Casetivity*-IIS operates efficiently on standard desktop and laptop computers without requiring specialized hardware or software installations, elevated user permissions, or local software installation. Only a supported web browser and internet access are required for full functionality. This design ensures that authorized users across the State can access the system reliably from their existing computing environments without additional technical barriers or IT overhead.

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

Yes. *Casetivity*-IIS operates efficiently on standard desktop and laptop computers without requiring specialized hardware or software installations. The solution is a cloud-based platform accessible through major web browsers including Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari. Users require only a supported web browser and internet access to access full system functionality—no elevated user permissions or local software installations are necessary.

The solution's cloud infrastructure maintains 99.9% uptime and delivers 90% of response times in less than two seconds and 98% of response times in less than 10 seconds. This performance ensures responsive user experiences across both desktop and laptop environments during

normal business operations. SSG employs continuous monitoring and adaptive scaling using AWS CloudWatch to track API response times and maintain optimal performance as users access the system through standard computing devices.

The system's user-centric design includes customizable modules tailored for different critical partner roles, ensuring ease of use and accessibility across desktop and laptop platforms without additional hardware or software requirements. SSG's maintenance approach includes base updates needed to maintain performance and optimization, ensuring that the solution continues to operate efficiently on standard computing environments throughout the contract term.

Casetivity-IIS meets the requirement for efficient operation on standard desktop and laptop computers without specialized 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.

Configuration of the existing system to meet the Agency's workflows, business rules, and data requirements is expected and acceptable.

Yes. *Casetivity*-IIS is accessible without requiring elevated user permissions or local software installation. Users need only a supported web browser and internet access to access the full functionality of the system.

The solution is a cloud-based, web-native application that operates through standard web browsers including Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari. No client-side software, plugins, or administrative privileges are required on user devices. This browser-only access model ensures that staff across provider organizations, public health agencies, and partner entities can securely access the system from standard desktop and laptop computers without IT intervention or specialized configuration.

The solution's role-based access control framework manages user permissions centrally within the application itself, eliminating the need for elevated system-level permissions on local machines. Authorized users authenticate through the web interface and receive access to functions and data based on their assigned roles and permissions, all managed within the IIS. This approach reduces deployment complexity, accelerates onboarding for new users and partner organizations, and minimizes ongoing support requirements for local IT teams.

SSG's cloud infrastructure maintains 99.9% uptime with 90% of response times under two seconds, ensuring consistent performance for browser-based access across diverse user environments. The system's web-based architecture supports the State's need for broad accessibility while maintaining security, compliance, and operational reliability without imposing technical barriers on end users.

4.2.3.2.5. The IIS solution must be a fully developed, market-ready and production-ready system at the time of proposal. The Agency will not consider solutions that require new system development, creation of a custom IIS, or substantial software build-out.

Configuration of the existing system to meet the Agency's workflows, business rules, and data requirements is expected and acceptable.

Casetivity-IIS is a fully developed, market-ready, and production-ready Immunization Information System. SSG is proposing an existing production solution, not the development of a new or custom IIS. The Agency will receive a proven platform with established functionality that has been designed specifically to support immunization information management, interoperability, vaccine inventory, provider management, school compliance, reporting, and public health operations.

SSG's implementation approach focuses on configuration rather than custom software development. During implementation, SSG will configure *Casetivity*-IIS to align with the Agency's business processes, jurisdiction-specific workflows, business rules, user roles, security requirements, reporting needs, and data requirements. Configuration activities include system settings, workflow configuration, business rule configuration, user permissions, interface configuration, forms, notifications, reports, and jurisdiction-specific operational preferences.

Because *Casetivity*-IIS is an established solution, implementation activities emphasize requirements validation, configuration, testing, data migration, interface deployment, training, and production readiness rather than designing or building new core application functionality. This approach reduces implementation risk, shortens deployment timelines, and provides the Agency with a stable, proven solution that can be configured to meet its operational needs while remaining on a supported product roadmap.

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)

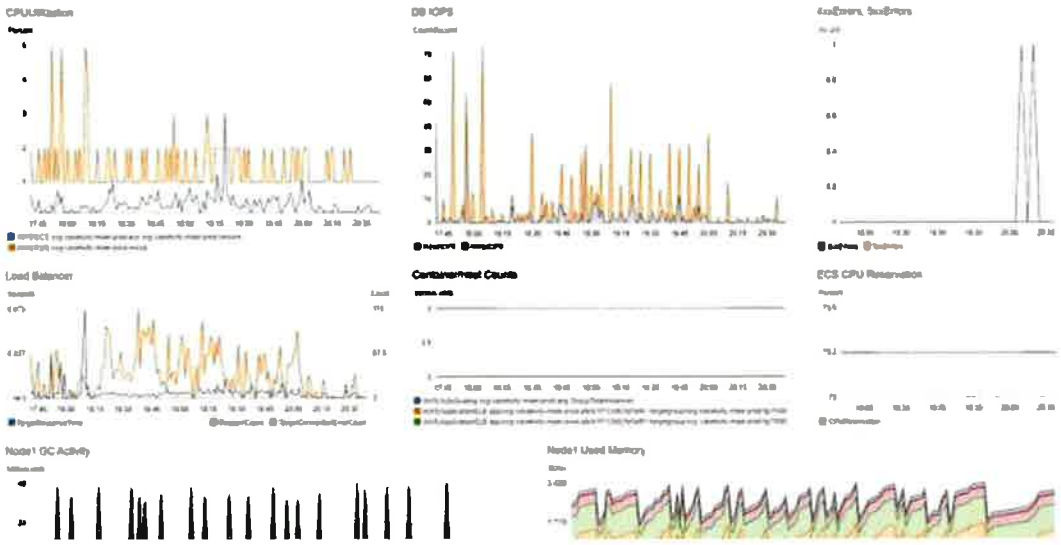
SSG accepts the Service Level Agreement (SLA) provided as Attachment C and commits to full compliance with all service levels, response times, resolution targets, and associated penalties governing the proposed Immunization Information System (IIS).

Casetivity-IIS is designed to support the Agency's SLA requirements through a comprehensive infrastructure and support framework. SSG provides annual maintenance and support services for all implemented system components, including software, databases, interfaces, and infrastructure. Help desk support is available during standard business hours (Monday through Friday, 8:00 AM to 5:00 PM local time) with documented escalation procedures to ensure timely resolution of issues. SSG delivers bug fixes and security patches within industry-standard timeframes, with critical vulnerabilities addressed promptly to maintain system security and stability.

System performance monitoring and proactive issue resolution are maintained for all hosted and managed environments. SSG's cloud-based hosting environment is FedRAMP-authorized and HIPAA-compliant, providing the technical foundation necessary to meet availability and performance targets. The infrastructure includes managed disaster recovery capabilities with annual disaster recovery exercises conducted to validate backup and recovery procedures. SSG maintains a formal disaster recovery plan that governs backup procedures and ensures compliance with state IT policies and data protection standards.

Casetivity-IIS implements and maintains the infrastructure to fulfill service-level agreements between the program and entities providing information technology support. This ensures system availability and uninterrupted data flows as required by the SLA. System configuration, monitoring tools, and automated processes support consistent achievement of performance thresholds.

As an example of some of the pro-active real-time monitoring we perform to provide this level of service and quality, the below are infrastructure dashboards.



SSG's acceptance of the SLA is formalized through the contract governance process. All defects identified during Acceptance Testing will be remediated per SSG's warranty. The Agency will issue written Acceptance of the IIS solution only after verifying that all functional, technical, security, interoperability, and performance requirements—including SLA compliance—have been fully met. No annual, recurring, subscription, hosting, or maintenance fees will begin prior to formal written Acceptance by the Agency.

SSG confirms full acceptance of and compliance with the Service Level Agreement governing the proposed IIS solution.

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 a vendor-hosted ticketing system of record with Agency visibility and reporting, and a tiered support structure jointly managed by the State and Vendor, as described below:

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.

SSG provides comprehensive help desk support during standard business hours (Monday–Friday, 8:00 AM–5:00 PM local time) through a structured, multi-tiered support model with documented escalation procedures. All support activity is tracked and managed within SSG's vendor-hosted Jira environment, which serves as the system of record and provides the State with full visibility into ticket status, history, and reporting. SSG brings direct experience operating Tier 1 functions and has implemented hybrid models across multiple state clients; the final division of responsibilities will be jointly defined with the State during implementation planning.

Help Desk Availability and Access

During business hours, SSG's help desk staff address all incoming calls and emails in a professional and timely manner, with initial response to help requests generally occurring within 24 hours. Users can access support through multiple channels including phone, email, an online ticketing portal, and a central help desk email account that automatically creates support tickets. When a ticket is created, users receive an automated acknowledgement with the ticket number and issue details, and any updates or notes added to the ticket are automatically emailed to the user for streamlined communication.

Tiered Support Structure

SSG can employ a two-tiered escalation system during business hours. Tier 1 help desk staff provide technical assistance for initial questions and issues. When staff cannot address an issue or a technical problem requires further attention, the inquiry is escalated to Tier 2 status and sent to the technical support team. Resolution of Tier 2 requests typically occurs within four business days. The help desk utilizes robust tracking software tools to centrally manage and report operational issues, fostering continuity of support among help desk staff and enabling rapid escalation and resolution.

Issue Classification and Prioritization

Known technical issues are categorized on a sliding scale: Critical, Major, Average, Minor, and Enhancement. Items classified as critical are communicated to users and addressed immediately, ensuring that high-priority issues receive appropriate attention and resources.

Escalation Procedures

SSG's documented escalation process routes unresolved issues through a two-tier structure. Issues escalate from front-line analysts to technical leads, and ultimately to the SSG Engagement Lead for resolution assurance. A centrally managed tracking system allows for rapid escalation and resolution by bringing together help desk support staff, client staff, and development and operations teams as an integrated unit. The solution also incorporates the ability to include key client staff as part of the support structure for easy escalation and monitoring, enabling them to provide business and policy guidance, monitor tickets, assign tickets to other staff, escalate issues in a timely manner, and create tickets directly through the central help desk portal.

This structured approach ensures that users receive consistent, professional support during business hours with clear pathways for issue resolution and escalation when needed.

4.2.3.4.1.1. The Vendor must support a Tier 1 / Tier 2 / Tier 3 model consistent with industry standards. The State and Vendor will jointly define the final responsibility split (e.g., password resets, role provisioning, interface triage) during implementation planning. Vendors must describe their proposed support model and recommended division of responsibilities in their proposal.

SSG fully supports a Tier 1 / Tier 2 / Tier 3 model consistent with industry standards and welcomes joint definition of the final responsibility split during implementation planning. SSG's proposed baseline assigns Tier 1 responsibilities — including password resets, user account inquiries, and initial triage — to the State, with SSG assuming Tier 2 and Tier 3 responsibilities for application-level support, configuration, escalated interface issues, and defect resolution.

SSG recognizes that the right model depends on each client's operational capacity and staffing structure. SSG brings direct experience operating Tier 1 support functions on behalf of state clients and has implemented hybrid models in which responsibilities are shared or redistributed across tiers based on agency preference. SSG remains open to discussing alternative structures — including a State-led hybrid or an SSG-led Tier 1 function — and will work collaboratively with the State during implementation planning to finalize a division of responsibilities that best serves operational needs and end users. It is our understanding that the State plans to handle Tier 1 interactions — including initial user contact, password resets, and first-level triage — while SSG will provide Tier 2 and Tier 3 support covering application-level issues, configuration, and defect resolution. SSG is certainly willing and able to provide Tier 1 support if desired by the State.

4.2.3.4.1.2. The Vendor must provide and maintain a vendor-hosted ticketing system of record for all support requests. The solution will not integrate with the State's ticketing system. The State must have full visibility into ticket status, history, and reporting within the Vendor-hosted system.

SSG provides and maintains a vendor-hosted Jira environment as the system of record for all support requests. Jira serves as SSG's standard platform for both software development lifecycle (SDLC) tracking and full-service desk operations, giving the State a single, unified view of all tickets from initial submission through resolution.

The State receives direct access to the Jira Service Desk portal, where authorized users can submit requests, monitor ticket status in real time, review full ticket history, and access reporting across open and closed items. SSG configures role-based access to ensure State staff have the visibility they need without requiring integration with the State's own ticketing infrastructure.

SSG's Jira environment supports configurable dashboards, queue management, priority classification, and audit-ready reporting — providing the State with continuous transparency into support activity and response performance throughout the engagement.

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

SSG delivers bug fixes and security patches through a structured maintenance program that prioritizes rapid response to critical vulnerabilities while maintaining system stability and operational continuity. The approach combines proactive monitoring, scheduled maintenance windows, and expedited remediation protocols aligned with industry-standard timeframes and federal cybersecurity requirements.

SSG addresses security patches and bug fixes through regular maintenance support that includes scheduled maintenance windows conducted during off-hours to minimize disruptions to operations. Security patches are applied regularly to address potential vulnerabilities and ensure the *Casetivity*-IIS solution remains secure. The maintenance program incorporates platform upgrades that provide access to the latest features and improvements, as well as interoperability updates to support seamless integration with external systems.

For critical vulnerabilities, SSG follows an expedited remediation process. The vendor performs Static Application Security Testing (SAST) scans integrated into the development pipeline for every code commit or build, and Dynamic Application Security Testing (DAST) scans at least

quarterly and following any major release or production update. Critical and high-risk findings identified through these scans are resolved within 30 calendar days unless otherwise approved by the Agency. All findings from SAST and DAST are incorporated into SSG's vulnerability management program to ensure consistent tracking and timely resolution.

SSG pairs regular maintenance activities with proactive monitoring to identify and address potential issues before they impact operations. This includes message throughput monitoring that tracks HL7 response times and flags delays to ensure real-time performance, and auto-scaling capabilities that dynamically adjust infrastructure during high-demand events. The vendor implements continuous monitoring practices consistent with FedRAMP and NIST guidance, including automated code scanning and penetration testing at least annually.

The defect management process follows a structured workflow that includes pre-fix verification to recreate the defect using documented steps, post-build verification to confirm the defect no longer occurs once the build is completed, and production issue handling for in-flight and new tasks. This systematic approach ensures that bug fixes are thoroughly tested before deployment and that critical issues are addressed promptly to maintain system reliability and security.

SSG tracks and documents all third-party libraries and modules, ensuring they are updated and free of known critical vulnerabilities. This comprehensive approach to maintenance and security patch management ensures that the *Casetivity*-IIS solution remains secure, stable, and compliant with federal and state cybersecurity standards while minimizing operational disruptions.

The following describes our industry leading Warranty program.

SSG Lifetime Warranty

At SSG, stewardship takes precedence over salesmanship. SSG's sense of responsibility drives the team to deliver solutions that make a measurable impact, and this is reflected in SSG's lifetime warranty for all solutions.

Warranty Coverage

SSG provides a comprehensive warranty that ensures:

- Warranty Coverage and compliance with all terms and conditions as specified in the RFQ and policies
- The *Casetivity-IIS* solution functions in accordance with the agreed-upon scope, specifications, terms, and requirements outlined in the contract.

- Any portion of the SSG-provided solution that is found to be deficient against the agreed-upon scope is included in SSG's O&M warranty.
- Deficient or erroneous documentation will be updated to reflect current, accurate solution specifications.

Warranty Services Details

To maintain transparency and accountability, SSG Warranty Services include:

- Collecting and maintaining detailed records for all warranty items, including:
- Nature and description of the deficiency.
- Status of the deficiency.
- Action plans with dates and times.
- Expected and actual completion times.
- Resolution details, including responsible personnel and resolution identifiers (e.g., work order number).

The SSG Lifetime Warranty is a testament to SSG's long-term dedication to public health. SSG honors those who work in public health and recognizes the importance of their work by warrantying that software built for them is void of any defects. That is what all software vendors should do.

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

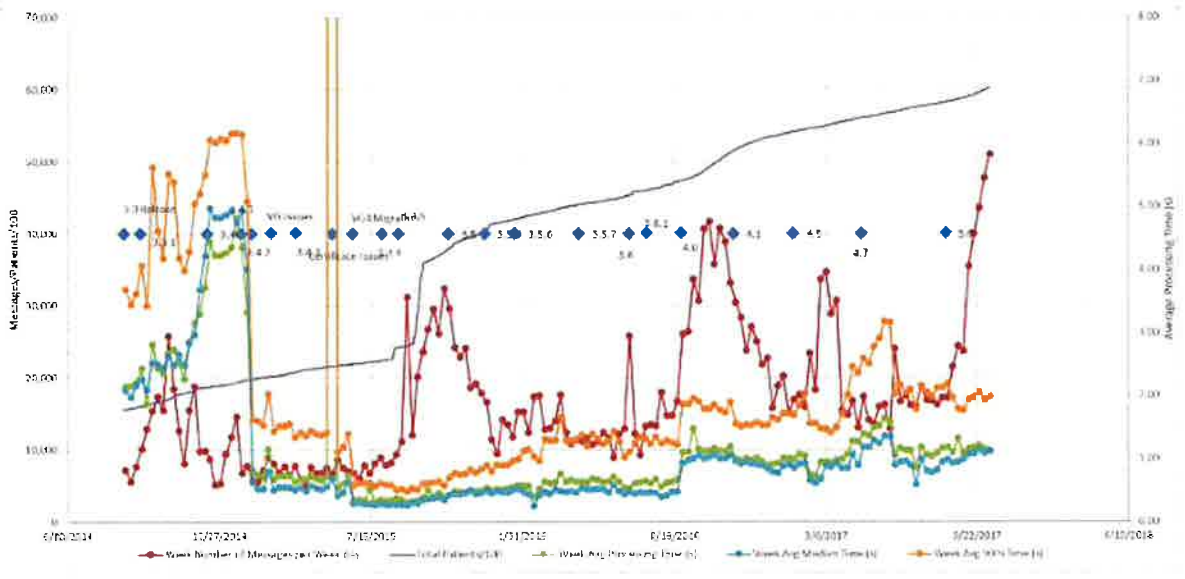
SSG employs a comprehensive approach to system performance monitoring and proactive issue resolution for all hosted *Casetivity*-IIS environments. This approach ensures minimal disruption, optimal performance, and prompt resolution of any issues that arise.

SSG uses a robust suite of monitoring tools to continuously track system performance and detect potential issues early. All traffic to the site has response status and response time recorded in an ongoing metric using AWS CloudWatch, which allows SSG to monitor API response times and maintain optimal performance. This proactive monitoring enables the SSG team to identify and address concerns before they escalate into major disruptions.

The system is designed to support high transaction volumes and resource-intensive tasks without degrading performance. *Casetivity*-IIS handles 130,000+ QBP per hour and 35,000+ VXU per hour with sub-second response times. SSG maintains 90 percent of response times under two seconds and 98 percent under 10 seconds (excluding complex reports and processes). Through continuous monitoring and adaptive scaling, SSG meets or exceeds performance

benchmarks, ensuring compliance with service levels and enhancing the resilience of business operations against disruptions.

The following is an example diagram with performance metrics.



If an outage or incident occurs, SSG initiates a structured response that includes evaluating the incident's scope and potential impact to determine the most effective resolution path and establishes a dedicated communication channel (typically via Microsoft Teams) for real-time coordination among team members. SSG monitors all system components to ensure availability and performance, tracks system performance metrics, and offers architecture or software and hardware adjustment recommendations semiannually.

SSG's approach includes robust error handling strategies and auto-scaling capabilities to ensure uninterrupted operations even during high-demand periods. This combination of continuous monitoring, adaptive scaling, and structured incident response ensures that *Casetivity*-IIS maintains optimal performance and availability for all hosted 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.

SSG provides comprehensive version upgrade and compatibility assurance services for all vendor-supplied components of *Casetivity*-IIS, ensuring continued compliance with CDC and state interoperability standards throughout the contract term.

- *Version Upgrades and Compatibility Assurance:* SSG delivers annual maintenance and support services covering all implemented system components, including software, databases, interfaces, and infrastructure. These services include version upgrades and compatibility assurance for all vendor-supplied components, ensuring continued compliance with CDC and state interoperability standards. SSG monitors evolving federal and state requirements and proactively updates the solution to maintain alignment with current specifications.
- *CDC IIS Functional Standards Support:* SSG anticipates and supports annual updates aligned with CDC IIS Functional Standards releases. The vendor accounts for these updates in ongoing maintenance planning and proposes a clear approach for scoping, estimating, and implementing future CDC-driven changes. Updates outside the CDC's 90-day IZ Gateway implementation window are evaluated and authorized through the State's standard contract governance and change-order process, ensuring transparency and controlled implementation.
- *Interoperability Standards Maintenance: Casetivity*-IIS maintains compliance with current CDC-endorsed interoperability standards for message content, format, and transport. The solution fully supports real-time data exchange per the CDC HL7 implementation guide, including VXU for vaccine record submissions, QBP for patient history and forecast queries, and ADT for demographic updates. The platform also supports comprehensive bidirectional integration with CDC VTrckS via the ExIS interface using standard CDC communication formats and protocols. SSG completes updates to ExIS functionality following publication of specifications, ensuring the solution remains current with federal requirements.
- *Documentation and Communication:* SSG provides documentation updates reflecting any changes made during the maintenance period. This ensures the State maintains current reference materials and operational guidance aligned with the latest system capabilities and compliance requirements.

This structured approach to version management, standards compliance, and proactive maintenance planning ensures the *Casetivity*-IIS solution remains fully compliant with evolving

CDC and state interoperability standards while minimizing disruption to operations and providing predictable pathways for implementing federally mandated updates.

4.2.3.4.4.1. The vendor must anticipate and support annual updates aligned with CDC IIS Functional Standards releases. Updates outside the CDC's 90-day IZ Gateway implementation window will be evaluated and authorized through the State's standard contract governance and change-order process. Vendors must account for these updates in their ongoing maintenance planning and propose an approach for scoping, estimating, and implementing future CDC-driven changes.

SSG applies a structured, transparent, and collaborative approach to scoping, estimating, and implementing future CDC-driven changes, including annual updates aligned with CDC IIS Functional Standards releases and changes outside the CDC's 90-day IZ Gateway implementation window.

- *Scoping and Estimation Process:* SSG is familiar with operating under time-and-materials or not-to-exceed arrangements to cover enhancements and maintenance and operations. When CDC releases updated functional standards or technical specifications, SSG works in partnership with the jurisdiction to assess the scope of required changes, identify affected system components, and develop cost and timeline estimates. This collaborative scoping process ensures transparency and allows the jurisdiction to evaluate and authorize changes through standard contract governance and change-order procedures.
- *Implementation Approach:* SSG's implementation methodology emphasizes stewardship, measurability, and continuous improvement to ensure CDC-driven changes are delivered predictably and with minimal risk. SSG maintains deep familiarity with CDC IIS Functional Standards, the Data Modernization Initiative, and NorthStar Architecture principles, enabling efficient alignment with evolving federal requirements. The low-code architecture of *Casetivity*-IIS supports rapid, adaptable delivery while preserving long-term value, allowing SSG to implement standards updates efficiently.
- *Reducing Jurisdictional Burden:* To prepare jurisdictional staff to implement certain system changes independently and reduce reliance on change requests, SSG provides select staff members with different levels of administrator training. This training enables jurisdictional administrators to make configuration changes without vendor support when appropriate. Depending on the level of risk and complexity a configuration change presents, jurisdictional staff may still choose to have SSG implement the change. SSG and the jurisdiction partner together to determine the best course of action to ensure enhancements or configuration changes are deployed successfully.

- *Standards Compliance and Governance:* All data exchange through the IZ Gateway and other CDC systems adheres to HL7 v2.5.1 Implementation Guide for Immunization Messaging, CDC's functional and technical standards, and AIRA guidance. SSG supports governance structures that fit each jurisdiction's operational model and can participate in joint working sessions, provide performance summaries, and assist with interpretation of trends to ensure transparency, repeatability, and shared accountability.

This approach ensures that CDC-driven changes are scoped accurately, estimated transparently, and implemented efficiently while maintaining compliance with federal standards and minimizing disruption to operations.

The SSG Maintenance and Compliance Guarantee

At SSG, stewardship takes precedence over salesmanship. The SSG Team is driven by a sense of responsibility to deliver solutions that make a measurable impact, and this drive is exemplified by our industry leading Compliance Guarantee. This Guarantee ensures that the *Casetivity*-IIS solution is delivered to the highest standards and maintains compliance throughout its lifecycle, providing your team with a reliable and sustainable system. Collectively, these programs reflect SSG's overarching commitment to Public Health and customer satisfaction.

SSG's Maintenance and Compliance Guarantee includes:

- **Security Patches:** Regular updates to address potential vulnerabilities and ensure system security.
- **CDC Compliance Enhancements:** Continuous updates to maintain full compliance with CDC standards and guidelines.
- **Platform Upgrades:** Regular updates to the *Casetivity-IIS* platform providing access to the latest system features and improvements.
- **Maintain Compliant Interoperability Interfaces:** Adjustments to ensure that all interfaces offer standard-compliant mechanisms to exchange data with the IIS. This ensures that external providers who develop in standard compliant ways will always be supported by WV.
- Compliance with all ADA standards and regulations

The SSG Maintenance and Compliance Guarantee is a testament to SSG's long-term dedication to public health. SSG ensures that software built for them is always compliant to state and federal standards and regulations. This is driven by the desire to make a difference in supporting the public health community.

Proactive Monitoring and Support

SSG pairs regular maintenance activities with proactive monitoring to identify and address potential issues before they impact operations. Some examples of proactive efforts include:

- **Message throughput monitoring:** Tracks HL7 response times and flags delays to ensure real-time performance.
- **Auto-scaling for surges:** Scales infrastructure dynamically during high-demand events like pandemics.
- **AI-powered deduplication checks:** Monitors match accuracy and prevents data quality issues.
- **HL7 data quality reports:** Identifies formatting errors and autocorrections before they impact reporting.
- **Proactive risk reviews:** Regular checkpoints address technical and operational risks early.

This ensures *Casetivity-IIS* continues to serve the State as a robust, reliable solution.

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

SSG maintains comprehensive documentation throughout the maintenance period and updates all materials to reflect system changes, enhancements, and configuration modifications. Documentation updates are managed through a structured process that ensures accuracy, accessibility, and alignment with current system specifications.

SSG uses collaborative platforms such as Confluence and SharePoint to maintain and update documentation in real time. These tools enable version control, change tracking, and centralized access for authorized users. When system changes occur—whether through routine maintenance, security patches, version upgrades, or configuration adjustments—SSG updates the corresponding documentation to reflect the current state of the solution. This includes technical specifications, user guides, administrative manuals, interface documentation, and operational procedures.

Under SSG's Maintenance Guarantee, any documentation found to be deficient or erroneous is updated to reflect accurate solution specifications. SSG collects and maintains detailed records for all warranty items, including the nature of deficiencies, action plans, resolution details, and completion timelines. This record-keeping ensures that documentation remains synchronized with system performance and configuration.

SSG's release management strategy coordinates documentation updates with software releases, program priorities, and core platform improvements. Documentation is updated regularly to reflect new system changes, ensuring materials remain accurate and relevant throughout the maintenance period. This approach supports transparency, reduces administrative burden, and ensures that users and administrators have access to current, reliable information for system operation and support.

SSG's documentation update process meets the requirement for maintaining accurate, up-to-date materials that reflect all changes made during the maintenance period.

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.

Yes. SSG will provide copies of its Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to the Agency within 60 calendar days of contract execution and upon request thereafter. SSG develops and maintains comprehensive BCP and DRP documentation within 30 calendar days after the commencement of services, ensuring alignment with HIPAA requirements and NIST SP 800-34 standards. These plans detail specific recovery steps, resource allocation, testing schedules, and verification processes for both disaster recovery and business continuity operations. SSG updates its BCP and DRP within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment, and annually certifies that plans remain current, tested, and compliant with federal and state requirements. This

commitment ensures the Agency receives complete, up-to-date documentation that supports rapid recovery and minimal disruption in the event of any disaster.

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.

Yes. SSG's Business Continuity Plan (BCP) and Disaster Recovery (DR) plans are 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. SSG will provide copies of its BCP and DR plans to the Agency within 60 calendar days of contract execution and upon request thereafter.

SSG conducts annual BCP/DR testing through tabletop or live failover exercises and provides a summary report of results, corrective actions, and remediation timelines to the Agency within 30 calendar days of test completion. All BCP/DR activities—including backups, failover, and recovery operations—comply with U.S.-based data residency requirements, ensuring that no data is transmitted, processed, or stored outside the continental United States at any time.

SSG maintains continuous improvement of its BCP/DR plans by updating them within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment. SSG annually certifies to the Agency that its BCP/DR plans remain current, tested, and compliant with federal and state requirements. This approach ensures uninterrupted operations, rapid recovery capability, and sustained alignment with NIST standards throughout the contract lifecycle.

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.

Yes. SSG will conduct annual Business Continuity Plan (BCP) and Disaster Recovery (DR) testing through either tabletop exercises or live failover exercises. SSG will provide a summary report of test results, corrective actions, and remediation timelines to the Agency within 30 calendar days of test completion. This annual testing requirement aligns with NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems) and ensures that SSG's BCP and DR plans remain current, tested, and operationally effective throughout the contract term.

SSG's approach to continuous improvement includes updating BCP and DR plans within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment. SSG will annually certify to the Agency that its BCP and DR plans remain current, tested, and compliant with federal and state requirements. All BCP and DR activities, including

backups, failover operations, and recovery procedures, comply with U.S.-based data residency requirements, ensuring that no data is transmitted, processed, or stored outside the continental United States at any time.

This requirement is met through SSG's documented and tested business continuity and disaster recovery framework for the *Casetivity*-IIS environments.

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).

Yes. SSG will provide documentation verifying U.S.-based data residency and maintain compliance with applicable federal and state data protection laws and regulations.

SSG hosts *Casetivity*-IIS in AWS data centers located exclusively within the continental United States. These data centers are designed to meet the highest standards of physical security and hold SOC 2 Type II and FedRAMP certifications, ensuring adherence to rigorous security protocols and controls required by industry standards. All IIS data—including backups, logs, and metadata—remains within U.S.-based facilities at all times, including during disaster recovery, failover, and support operations.

SSG will provide documentation confirming this U.S.-based data residency to West Virginia within the required timeframes. This documentation verifies that no data is transmitted, processed, or stored outside U.S. borders, including U.S. Territories, in full compliance with federal government and West Virginia's cybersecurity and data residency requirements.

SSG's *Casetivity* platform maintains SOC 2 Type 2 certification, demonstrating ongoing compliance with stringent security measures. The solution employs comprehensive data protection controls, including encryption of data in transit and at rest, role-based access control, and multi-factor authentication. SSG undergoes regular audits and vulnerability assessments to ensure continuous compliance with industry best practices and applicable federal and state data protection laws and regulations.

This approach ensures that West Virginia retains full control and visibility over where its IIS data resides, how it is protected, and that all operations meet the state's regulatory and security requirements throughout the contract term.

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.

Yes. SSG will update its Business Continuity Plan (BCP) and Disaster Recovery (DR) plans within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment. This commitment ensures that SSG's continuity and recovery strategies remain current, effective, and aligned with the operational realities of the *Casetivity*-IIS environment throughout the contract term.

SSG maintains documented BCP and DR plans that are continuously refined based on real-world experience. Following each annual test—whether tabletop exercise or live failover—SSG reviews results, identifies corrective actions, and incorporates lessons learned into updated plan documentation. Similarly, when incidents occur or when material changes are made to the hosting infrastructure, SSG evaluates the impact on continuity and recovery procedures and revises the plans accordingly. This 60-day update window provides sufficient time for thorough review, critical partner input, technical validation, and formal documentation while ensuring plans do not become outdated.

SSG provides updated plans to the Agency upon completion and remain aligned with the most current version of NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems) or successor publications. SSG also annually certifies to the Agency that its BCP and DR plans remain current, tested, and compliant with federal and state requirements. This continuous improvement cycle—testing, learning, updating, and certifying—ensures that the Agency's immunization data and operations are protected by recovery strategies that reflect the current state of the system, infrastructure, and threat landscape.

SSG confirms that it will update its BCP/DR plans within 60 calendar days of lessons learned from testing, incidents, or material changes to the hosting environment, as required.

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.

Yes. SSG will annually certify to the Agency that its Business Continuity Plan (BCP) and Disaster Recovery (DR) plans remain current, tested, and compliant with federal and state requirements. This annual certification is a formal commitment that ensures the Agency maintains visibility into the operational readiness and regulatory alignment of SSG's continuity and recovery capabilities throughout the contract term.

SSG maintains comprehensive BCP and DR plans that are continuously updated based on the evolution of data, infrastructure, architecture, and tools. The plans are tested annually through

disaster recovery and business continuity exercises, with detailed reports documenting test results, issue resolution, and certification of readiness. These annual testing reports verify that recovery objectives are achieved and that the plans reflect the current state of the system and its requirements.

The annual certification process provides the Agency with documented assurance that SSG's BCP and DR plans comply with applicable federal and state requirements, have been tested within the past year, and accurately reflect the operational environment. This certification supports the Agency's oversight responsibilities and ensures that continuity and recovery capabilities remain aligned with regulatory standards and contractual obligations as the system evolves.

4.2.3.6. Data Ownership

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

Yes. SSG confirms that the Agency retains full ownership of all Immunization Information System (IIS) data. All data collected, processed, or stored on behalf of the Agency remains solely the property of the Agency at all times.

SSG provides privacy and security safeguards that protect Agency data from unauthorized use or disclosure outside the scope of the contract. Upon request or contract termination, SSG will return the entire dataset in the format specified by the Agency at no additional cost, ensuring the data remains usable and accessible. SSG will cooperate fully with the Agency and any subsequent vendor during transition, delivering all data, documentation, and work products to the Agency or its designee within 30 working days of termination notice.

At contract end or upon Agency request, SSG will destroy all data in accordance with the most current NIST Special Publication 800-88. Data destruction will not begin prior to written authorization from the Agency Project Manager and will be completed within 30 days of authorization. SSG will not use IIS data for analytics, artificial intelligence or machine learning training, model development, or any secondary purpose without explicit written approval from the Agency.

This commitment to data ownership ensures the Agency maintains complete control over its immunization data throughout the contract term and beyond, supporting long-term data stewardship, regulatory compliance, and operational continuity.

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 solely the property of, the Agency.

Yes. SSG agrees that all data related to the execution of the contract is collected on behalf of, and remains solely the property of, the Agency. SSG recognizes that the Agency retains full ownership of all data at all times throughout the contract term and following contract termination. SSG provides privacy and security safeguards to protect all data from any use or disclosure for any purpose other than those described within the solicitation. SSG will return the entire dataset in a format specified by the Agency upon request or contract termination at no additional cost, ensuring usability and accessibility. Upon contract termination, SSG will cooperate with the Agency and any subsequent vendor to deliver all data, documentation, and associated work products to the Agency or its designee within thirty (30) working days of receipt of notice of contract termination. SSG will destroy all data in the system at the end of the contract or upon Agency request in accordance with the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-88, completing destruction within 30 days of written authorization from the Agency Project Manager. SSG will not use IIS data for analytics, artificial intelligence or machine learning training, model development, or any secondary purpose without explicit written approval from 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.

Yes. SSG agrees to provide privacy and security safeguards to protect all IIS data from any use or disclosure for any purpose other than those described within this solicitation.

SSG ensures that data maintained on behalf of the IIS is not used, released, or sold without specific authorization from the Agency, regardless of whether the data has been de-identified or included with a limited data set. The vendor provides privacy and security safeguards protecting data from use or disclosure outside the solicitation scope.

SSG will not use IIS data for analytics, artificial intelligence or machine learning (AI/ML) training, model development, or any secondary purpose without explicit written approval from the State. This commitment ensures that all immunization data collected and stored within *Casetivity*-IIS remains exclusively dedicated to the purposes defined in this procurement.

The solution implements confidentiality policies that protect the privacy of individuals whose data is contained in the system. Security and data privacy are paramount in the solution, with compliance with all relevant federal and state regulations, including HIPAA and CDC guidelines, ensuring the protection of sensitive health information. The system includes advanced security features such as encryption, role-based access control, and regular security audits.

SSG confirms full agreement to provide the privacy and security safeguards required to protect all IIS data from unauthorized use or disclosure beyond the scope of 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.

SSG confirms that the Agency retains full ownership of all IIS data and that SSG will return the entire dataset in a format specified by the Agency upon request or contract termination at no additional cost. This commitment ensures the Agency maintains complete control over its immunization data and can transition smoothly to another vendor or system if needed.

Upon contract termination or at the Agency's request, SSG will deliver all data, documentation, and work products to the Agency or its designee within 30 working days of termination notice. The Agency specifies the format for data return to ensure usability and accessibility for its intended purposes. SSG provides privacy and security safeguards that protect data from use or disclosure outside the scope of the solicitation throughout the contract term.

SSG will cooperate fully with the Agency and any subsequent vendor during transition activities. This includes coordinating data handoff, providing technical documentation, and supporting knowledge transfer to minimize disruption to immunization program operations. All data return activities occur at no additional cost to the Agency.

Following data return and upon written authorization from the Agency Project Manager, SSG will destroy all remaining data in accordance with the most current NIST Special Publication 800-88. Data destruction will not begin prior to written authorization and will be completed within 30 days of that authorization. This process ensures the Agency's data is handled securely through the entire lifecycle, from implementation through contract closeout.

This approach confirms that SSG meets the requirement to return the entire IIS dataset in an Agency-specified format at no additional cost, ensuring data usability, accessibility, and the Agency's ability to maintain continuity of immunization services.

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.

Yes. SSG confirms that it will cooperate fully with the Agency and any subsequent vendor upon contract termination. SSG will deliver all data, documentation, and associated work products to the Agency or its designee within thirty (30) working days of receipt of notice of contract termination.

SSG's standard project closeout process ensures orderly knowledge transfer and continuity. Upon contract termination, SSG will conduct a structured transition that includes review of all deliverables, confirmation of Agency sign-off, discussion of lessons learned, and documentation of any outstanding issues or follow-up tasks. SSG will prepare a comprehensive Project Closeout Report within three weeks that captures all transition activities and ensures the Agency has complete visibility into system operations, configurations, and administrative procedures.

All data will be returned in the format specified by the Agency to ensure usability and accessibility, at no additional cost. SSG will provide complete documentation including system architecture, configuration guides, user manuals, training materials, and administrative procedures to support seamless transition to the Agency or a successor vendor. This commitment ensures the Agency retains full control and ownership of its immunization information system and all associated work products throughout and beyond the contract term.

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.

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

This commitment ensures the Agency maintains full control over its data throughout the contract lifecycle and at contract conclusion. SSG's data destruction protocols align with federal standards for secure media sanitization, protecting the confidentiality and integrity of immunization records, personally identifiable information, and all system data. The 30-day completion timeline provides the Agency with predictable, timely data disposition while maintaining compliance with applicable federal and state data protection 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.

Yes. SSG confirms that the finalized Project Plan and Schedule will adhere to the Implementation Plan proposed in Section 4.2.2.2, subject to Agency review and approval. SSG has developed a detailed project plan that includes task-level sequencing, dependencies, and assigned resources for all major deliverables. This plan aligns directly with the proposed implementation schedule.

SSG's Project Manager will host an initial planning session with the Agency within 30 days after the project start date to collaboratively refine and finalize the project plan. During these sessions, SSG and the Agency will jointly establish implementation milestones, each with clear deliverables, objective acceptance criteria, documentation requirements, and proposed payments. The finalized plan will be submitted to the Agency for formal review and approval.

Any deviation from the proposed Implementation Plan will be documented, justified, and submitted to the Agency for written approval before implementation. SSG will not unilaterally add, remove, modify, subdivide, or consolidate milestones without the Agency's prior written consent. The Project Manager will track actual utilization against the baseline weekly, making adjustments as needed to preserve schedule and deliverable quality while maintaining alignment with the approved plan.

This approach ensures transparency, accountability, and Agency control throughout the implementation process, supporting a successful transition to the new IIS solution.

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

SSG confirms that any deviation from the proposed Implementation Plan will be documented, justified, and approved by the Agency prior to implementation. This requirement is embedded in SSG's project governance framework and aligns with the structured change control processes SSG applies across all public health implementations.

SSG's approach ensures that the finalized Project Plan and Schedule adheres to the Implementation Plan proposed in the vendor's response and remains subject to Agency review and approval throughout the project lifecycle. If circumstances require adjustments to scope, timeline, milestones, or deliverables, SSG will prepare a written justification that includes the root cause of the deviation, the anticipated impact on project objectives, and recommended corrective actions. This documentation will be submitted through the formal change control process for Agency review, discussion, and written approval before any changes are enacted.

SSG applies transparent communication and collaborative impact assessment to all schedule or scope adjustments. When deviations are identified, SSG immediately assesses the root cause, documents the specific deliverables affected, estimates the duration of impact, and proposes mitigation strategies. SSG works with the Agency to implement a formal recovery plan that may include resource reallocation, task sequencing adjustments, or parallel workstream acceleration—always ensuring that quality and compliance are preserved. All proposed adjustments are documented and submitted for Agency approval, and updated schedules and milestones are shared with critical partners to maintain alignment and accountability.

This governance structure protects the Agency's interests by ensuring that no unilateral changes occur, that all deviations are justified and traceable, and that the Agency retains full authority over project direction. SSG's commitment to formal change control, written documentation, and Agency approval for all Implementation Plan deviations supports a transparent, accountable, and collaborative partnership throughout the implementation period.

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.

SSG confirms that it will not assess, invoice, or charge the Agency for any fees during the Implementation Period. Payment for implementation services will be tied exclusively to the successful completion of mutually agreed-upon implementation milestones that are approved in writing by the Agency.

SSG's implementation approach aligns with the Agency's milestone-based payment structure. All implementation milestones will be jointly developed during initial planning sessions and incorporated into the finalized Project Plan. Each milestone will include clear deliverable descriptions, objective acceptance criteria, documentation requirements, and proposed payment amounts subject to Agency approval. SSG will not add, remove, modify, subdivide, or consolidate milestones without prior written approval from the Agency.

No milestone payment will be due until the Agency verifies in writing that all deliverables and acceptance criteria associated with that milestone have been fully met. SSG will not invoice for any annual licensing, subscription, hosting, maintenance, or support fees during the Implementation Period. These recurring fees will not begin or accrue until the system has been fully implemented, operational, and formally accepted by the Agency through a written Notice of Acceptance.

Upon the Agency's formal written Acceptance of the fully implemented *Casetivity*-IIS solution, SSG will invoice only for the prorated portion of annual fees corresponding to the remainder of the current contract year. SSG will calculate proration based on the number of days remaining in the contract year following the date of Acceptance. Under no circumstances will SSG invoice for a full annual fee for a partial contract year.

This milestone-based payment approach protects the Agency's investment, ensures accountability at each implementation phase, and ties all payments to verified completion of agreed-upon deliverables.

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 the 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 approved in writing by the Agency

SSG ensures that all implementation milestones are jointly developed during initial planning sessions through a structured, collaborative approach that establishes clear deliverables, acceptance criteria, documentation requirements, and Agency-approved payment terms for each milestone.

During the initial planning session held within 30 days after project start, SSG works directly with the Agency to finalize the Project Plan and Schedule. This collaborative planning process produces mutually agreed-upon implementation milestones that are formally incorporated into the approved Project Plan. Each milestone is defined with four required components: a clear description of required deliverables, objective acceptance criteria that enable verification, specific documentation requirements, and a proposed payment amount that must be approved in writing by the Agency before work proceeds.

SSG's milestone-based methodology structures implementation into distinct phases with measurable deliverables. For example, Implementation Milestone 1 focuses on Requirements Validation, Milestone 2 addresses Design and Development, Milestone 3 covers Testing, Milestone 4 encompasses Data Conversion and Migration, Milestone 5 includes Training and Organizational Change Management, and Milestone 6 marks final Implementation completion. Each milestone includes defined deliverables such as the Requirements Document, Technical and Information Architecture Review, test plans and results documentation, and configuration guides.

The acceptance criteria for each milestone are objective and verifiable. SSG documents completion through deliverables that the Agency can review and validate—such as functional walkthroughs, regression testing coverage, configuration documentation, and system performance validation. No milestone payment becomes due until the Agency verifies in writing that all associated deliverables and acceptance criteria have been fully met. This verification-before-payment approach ensures accountability and protects the Agency's interests throughout implementation.

SSG maintains strict governance over milestone definitions. 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. This requirement is built into SSG's project management approach, which uses tools like Microsoft Project and JIRA to track milestone completion and generate automated reports on project health and milestone achievement dates.

Documentation requirements are embedded in each milestone. SSG produces comprehensive documentation throughout implementation, including the Requirements Document, Technical and Information Architecture Review, Communication Plan, Risk Management Plan, Configuration Management Plan, test documentation, system architecture guides, user manuals, training materials, and administrative procedures. SSG delivers all documentation as part of milestone completion and subject to Agency review and acceptance.

This collaborative milestone development process ensures transparency, shared accountability, and alignment between SSG and the Agency throughout implementation. By jointly defining milestones during initial planning and requiring written Agency approval for all deliverables, acceptance criteria, documentation, and payments, SSG establishes a partnership approach that protects the Agency's investment and ensures successful system delivery.

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.

SSG confirms that the vendor will not add, remove, modify, subdivide, or consolidate implementation milestones without the Agency's prior written approval. All implementation milestones must be jointly developed during the initial planning sessions and incorporated into SSG's Project Plan. Any attempt to alter milestone definitions or payment amounts without the Agency's prior written approval is void and unenforceable.

SSG's project management approach ensures that milestone integrity is maintained throughout the implementation lifecycle. The team regularly updates tasks in Microsoft Project and JIRA, which generate automated reports providing insights into project health and tracking key metrics such as task completion rates and milestone achievement dates. This transparency enables the Agency to monitor progress against the approved Project Plan and ensures that any proposed changes are identified early and submitted for formal Agency review.

SSG will document, justify, and obtain Agency approval for any deviation from the proposed Implementation Plan before proceeding. No milestone payment will be requested until the Agency verifies and approves completion of the corresponding milestone in writing. This

governance structure protects the Agency's interests, maintains accountability, and ensures that the implementation proceeds according to mutually agreed-upon terms.

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.

Yes. SSG confirms that no milestone payment will be due until the Agency verifies in writing that all deliverables and acceptance criteria associated with that milestone have been fully met. This verification requirement is built into SSG's structured deliverable sign-off and acceptance procedures, which align with the Agency's acceptance requirements.

SSG follows a formal four-step acceptance process for all deliverables: SSG submits the draft deliverable to the Agency for review; the Agency provides consolidated feedback within the agreed timeframe; SSG incorporates revisions and resubmits the final version; and the Agency issues formal written acceptance. The Project Manager documents and maintains each step in the Deliverable Tracking Log to ensure full traceability and accountability.

This approach ensures that milestone payments are tied directly to verified completion of deliverables and acceptance criteria, with no payment released until the Agency has provided written confirmation that all requirements have been satisfied. SSG's implementation milestone structure—covering Requirements Validation, Design and Development, Testing, Data Conversion and Migration, Training and Organizational Change Management, and Implementation—supports clear verification points throughout the project lifecycle. Progress tracking through Microsoft Project and JIRA provides real-time visibility into task completion rates and milestone achievement, enabling the Agency to monitor readiness for each verification checkpoint.

This verification-before-payment model protects the Agency's interests, ensures accountability, and confirms that SSG fully meets the requirement that no milestone payment will be due until written verification of completion is provided.

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.

SSG acknowledges and accepts the Agency's milestone payment requirements. SSG understands that milestone payments are contingent upon the successful completion of all milestone deliverables and formal Agency review and approval. SSG acknowledges that partial or conditional payments will not be requested or expected for partially completed milestones and

that payment will be requested only after the applicable milestone has been fully completed and accepted by the Agency.

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.

SSG acknowledges and accepts the Agency's requirement that recurring fees, including subscription, hosting, maintenance, support, or other recurring charges, will not begin or accrue until the Agency has issued formal written Acceptance of the fully implemented IIS solution. SSG understands that recurring fees will be invoiced only after the Agency's final acceptance in accordance with the terms of the Contract.

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.

SSG acknowledges and accepts the Agency's milestone remediation requirements. If the Agency identifies deficiencies during milestone review or acceptance testing, SSG will promptly address and remediate all identified deficiencies at no additional cost to the Agency and will resubmit the applicable milestone for Agency verification. SSG understands that the Agency may perform additional testing, validation, or review as necessary to confirm that all deficiencies have been satisfactorily resolved before approving the milestone.

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.

SSG confirms acceptance of the liquidated damages provisions as specified. The Agency may assess liquidated damages in the amount of $500.00 per calendar day for any missed implementation milestone 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 total implementation costs.

SSG's project management approach is designed to prevent delays and ensure timely milestone completion. The team regularly updates tasks in Microsoft Project and JIRA, which generate automated reports providing real-time insights into project health, task completion rates, and milestone achievement dates. This proactive tracking enables early identification of potential schedule risks and supports corrective action before delays occur.

Payment for implementation services is tied to successful completion of mutually agreed-upon milestones, with no milestone payment due until the Agency has verified and approved completion of the corresponding milestone. Final implementation payment will be made only upon the Agency's formal written Acceptance of the fully implemented *Casetivity*-IIS solution.

SSG accepts these provisions and commits to meeting all implementation milestones according to the approved Project Schedule to avoid assessment of liquidated damages.

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)

SSG confirms that its internal hiring policies and procedures comply with WV Office of Technology Policies available at https://technology.wv.gov/policy-governance/ot-policies. SSG has reviewed the applicable policies governing vendor staffing and background check requirements and will ensure full adherence throughout the contract term.

SSG's hiring practices align with the requirements outlined in the WV Office of Technology Policies, Agency Office of Shared Administration Office of Management Information Services (OMIS) Policy #0529 (Vendor/Contractor Employee Background Check Policy), OMIS Procedure #OP-35 (Vendor/Contractor Employee Background Check Procedure), and Appendix A. All SSG personnel assigned to this project will undergo the required background checks and meet the standards established by these policies prior to accessing any Agency systems or data.

SSG maintains documented internal policies for personnel screening, onboarding, and ongoing compliance monitoring that support these requirements. SSG will provide all necessary documentation and certifications as requested by the Agency to verify compliance with WV Office of Technology Policies and related OMIS requirements.

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)

SSG's internal staffing policies and procedures for hiring comply with all applicable West Virginia Office of Technology Policies, Agency Office of Shared Administration Office of Management Information Services (OMIS) Policy #0529 (Vendor/Contractor Employee Background Check Policy), OMIS Procedure #OP-35 (Vendor/Contractor Employee Background Check Procedure), and Appendix A. SSG will provide staffing resources to successfully complete implementation tasks, including system configuration, customization, testing, training, and go-live support, in full alignment with these requirements.

SSG maintains comprehensive background check protocols that align with state and federal standards for government contracts. All personnel assigned to the West Virginia Immunization Information System project will undergo background screening consistent with OMIS Policy #0529 requirements prior to engagement. SSG's hiring and vetting procedures ensure that no individuals who have been excluded or debarred by federal or state government from participating in government programs or contracts are employed on state projects.

SSG will provide a dedicated project manager during the system implementation phase to coordinate with the Agency's project manager and ensure compliance with all staffing, security, and operational requirements throughout the contract term. This approach ensures accountability, continuity, and adherence to West Virginia's established policies governing vendor staffing and contractor employee background checks.

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

SSG confirms that its staffing policies comply with OMIS Procedure #OP-35 (Attachment E): Vendor/Contractor Employee Background Check Procedure and Appendix A (Attachment F). SSG's internal hiring policies and procedures align with the requirements outlined in the West Virginia Office of Technology Policies, OMIS Policy #0529 (Vendor/Contractor Employee Background Check Policy), OMIS Procedure #OP-35, and Appendix A.SSG will provide staffing

resources to successfully complete implementation tasks, including system configuration, customization, testing, training, and go-live support. All personnel assigned to the project will undergo background checks in accordance with the procedures specified in OP-35 and Appendix A prior to accessing Agency systems or data. SSG maintains documented hiring and screening protocols that ensure compliance with state and federal requirements for vendor personnel working on government health and human services projects.

SSG will assign a dedicated project manager to work alongside the Agency's project manager throughout the system implementation phase. Staffing levels will flex appropriately based on project phase and workload, with all staffing changes communicated to and approved by the Agency. SSG's approach ensures that only properly vetted personnel support the immunization information system implementation and ongoing operations, protecting the integrity and security of West Virginia's public health data throughout the contract term.

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.

SSG will provide a dedicated Project Manager throughout the IIS system implementation phase to serve as the primary point of contact and ensure successful delivery of *Casetivity*-IIS. The Project Manager will be responsible for managing scope, schedule, risk, and reporting throughout implementation, working closely with the Agency's project manager to maintain alignment and accountability.

SSG's Project Manager will facilitate weekly status meetings with agendas and minutes distributed within three business days of each meeting. The Project Manager will also deliver monthly executive reports that include milestone tracking, risk assessments, and budget updates. To maintain transparency and enable proactive decision-making, the Project Manager will maintain a risk/issue/action log and decision tracker that remains accessible to the Agency throughout the implementation period.

The Project Manager operates within a clear governance structure that defines ownership, accountability, and escalation paths. This structure includes an Executive Sponsor for executive oversight and risk escalation, a Program Director accountable for delivery success, and the Project Manager who manages day-to-day execution. Supporting roles include a Solution Architect who oversees design and integration, a Data Migration Lead who manages data profiling and reconciliation, a Testing Lead who oversees test coverage and defect resolution,

and a Training and Adoption Lead who manages curricula and onboarding. The Agency's Product Owner validates priorities and accepts deliverables within this governance framework.

SSG will host an initial planning session with the Agency within 30 days after project start to finalize the project plan and schedule. The finalized Project Plan and Schedule will adhere to the Implementation Plan proposed in the response, subject to Agency review and approval. Any deviation from the proposed Implementation Plan will be documented, justified, and approved by the Agency before proceeding. The Project Manager will update the plan no less than every two weeks to reflect current status and maintain accuracy throughout implementation.

This dedicated project management approach ensures disciplined execution, clear communication, proactive risk management, and accountability from project initiation through final acceptance of the fully implemented IIS solution.

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 / Agency Administrator: Focus on system configuration, data quality monitoring, advanced reporting, and system maintenance tasks.

SSG provides a comprehensive, role-specific training plan for OEPS/Agency Administrators that focuses on the advanced system management capabilities required to configure, monitor, and maintain *Casetivity*-IIS. This training equips administrators with the skills needed to manage system-wide settings, enforce data quality standards, generate advanced reports, and perform ongoing system maintenance tasks.

- *System Configuration Training:* Administrator training covers the full range of system configuration capabilities available in *Casetivity*-IIS. Administrators learn to manage code

sets (NDC, MVX, CVX), configure default values to minimize data input requirements, establish geographic jurisdictional hierarchies, and associate users and facilities with organizations. Training includes hands-on instruction in configuring enrollment forms by program, modifying facility types per immunization program and CDC VFC descriptions, and establishing rules-based approval and rejection logic for enrollment workflows. Administrators also learn to configure authorization and user agreements per jurisdictional policy, manage inventory availability settings for VFC-supplied, jurisdiction-supplied, and private stock inventories, and customize system displays and user interface elements.

- *Data Quality Monitoring Training:* A core component of administrator training focuses on data quality management capabilities. Administrators learn to adjust data quality business rules within both HL7 message processing and the user interface, setting validation levels as Error, Warning, or Informational based on jurisdictional requirements. Training covers how to create and update data quality reports, specify and modify data quality monitoring rules, and configure data elements and target thresholds per organization. Administrators gain proficiency in managing rules governing HL7 message data validation and fine-tuning validation thresholds to balance data quality enforcement with external system adoption.
- *Advanced Reporting Training:* Administrator training includes instruction on generating and customizing advanced reports to support program oversight and decision-making. Administrators learn to aggregate data across user-defined hierarchies, configure report parameters, and create custom filters for patient reports. Training covers how to add and modify patient priority group indicators to support targeted reporting during mass vaccination events and public health emergencies.
- *System Maintenance Training:* Administrators receive training on ongoing system maintenance tasks, including managing user roles and permissions, monitoring system performance, and addressing help desk escalations. Training covers how to update code sets as CDC releases new standards, maintain system documentation, and coordinate with SSG support staff to resolve technical issues.
- *Training Deliverables:* SSG provides current, digital, and user-specific training resources tailored to administrator needs. These include on-demand video instructions and demonstrations for each administrative function, digital user guides and manuals for both functional and technical reference, and PowerPoint slide decks presenting system overviews. SSG maintains all training materials as part of ongoing maintenance and updates them with each major system release. Materials are posted on a dedicated resource website for easy access and reference.

- *Post-Implementation Support:* Following go-live, SSG provides ongoing system support to ensure administrators can fully utilize all system capabilities. SSG's help desk support is available during standard business hours with documented escalation procedures, and administrators receive prompt assistance with configuration questions, system issues, and optimization opportunities. As system updates are released, SSG updates training materials and schedules refresher training sessions as needed to ensure administrators remain proficient with new features and capabilities.

This comprehensive administrator training plan ensures OEPS/Agency Administrators achieve full proficiency in system configuration, data quality monitoring, advanced reporting, and system maintenance, enabling them to effectively manage *Casetivity*-IIS throughout the contract term.

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.

SSG's role-specific training plan for Provider Office Staff and End-Users focuses on building proficiency in the day-to-day workflows that support efficient immunization data management. The training strategy addresses data entry, patient search and query functions, clinical decision support usage, and basic troubleshooting to ensure end users can confidently navigate *Casetivity*-IIS from the first day of use.

SSG develops comprehensive user manuals that contain detailed descriptions and screen captures, allowing end users to research answers to questions about how to use the system. SSG maintains these manuals as part of ongoing maintenance and are updated as major releases are made to the system and as needed.

The training materials include PowerPoint slide decks tailored to various audiences, webinar recordings for self-paced training, and clinical integration materials. All materials are posted on a dedicated resource website, ensuring Provider Office Staff have continuous access to training resources. When major releases are made to the system, SSG updates these materials and posts them on the resource website. New training sessions can be scheduled with users as needed to cover system enhancements, new features, or changes to federal or jurisdictional standards.

SSG's training approach supports the specific workflows Provider Office Staff encounter daily. For patient search and query functions, *Casetivity*-IIS provides out-of-the-box support that allows users to search for patient records based on one or multiple user-defined parameters, re-search by modifying existing search parameters, and select from a list of possible patient matches per jurisdictional policy. For clinical decision support, the system applies immunization schedules appropriate at the time of administration, enabling Provider Office Staff to make

informed vaccination decisions. The role-based access control system is tailored for providers and clinical staff, with permissions configured for vaccine data entry and patient lookup functions.

Following implementation, SSG provides ongoing system support and maintenance to ensure that all end user questions and issues are addressed and that the system is fully utilized. SSG delivers customer-friendly support as requested and promptly addresses all identified issues. This post-implementation support resolves user-adoption challenges and ensures a smooth transition to full operational proficiency. The combination of comprehensive training materials, self-paced learning resources, role-specific job aides, and responsive ongoing support ensures Provider Office Staff and End-Users achieve and maintain full proficiency in day-to-day data entry, search and query functions, clinical decision support usage, and basic troubleshooting throughout the contract term.

4.2.3.10.1.3. School Nurses / Public Health Partners: Focus on roster management, exemption tracking, and public health follow-up workflows.

SSG provides a comprehensive, role-specific training plan for School Nurses and Public Health Partners that focuses on roster management, exemption tracking, and public health follow-up workflows. The training approach ensures these users gain full proficiency in the specialized functions they perform within *Casetivity*-IIS.

- *Roster Management Training:* School Nurses receive focused instruction on uploading student cohorts to prepopulate survey fields using IIS match logic. The training covers how to link students to schools via rosters, enabling targeted outreach and reporting by school, grade, and county. This capability supports identification of geographic and demographic gaps in oral health coverage and immunization compliance. School Nurses learn to manage rosters for preschool, kindergarten, grades seven and 12, and college populations, with the system preconfigured for these levels and extensible to support additional populations as needed.
- *Exemption Tracking Training:* The training plan addresses how School Nurses and Public Health Partners generate and interpret reports of student exemptions by type, including medical and religious exemptions. Users learn to filter exemption data by school, grade, district, exemption type, and compliance status. The training covers how to access these standard reports, which are available out-of-the-box and support school reporting requirements without requiring assistance from SSG staff.
- *Public Health Follow-Up Workflows:* School Nurses and Public Health Partners receive training on task-based workflows that assign follow-ups to the appropriate staff members. The instruction covers how to use role- and team-specific queues, track task

assignment and escalation across departments, and leverage complete audit trails for each task and workflow. Training addresses how these workflows support school survey coordination, compliance tracking, and certificate printing functions specific to their roles.

- *Training Deliverables:* SSG provides current, digital, and user-specific training resources tailored to School Nurses and Public Health Partners, including on-demand video instructions or demonstrations and digital user guides or manuals for both functional and technical reference. The training materials address the distinct needs and responsibilities of these user groups, ensuring they can effectively perform roster management, exemption tracking, and public health follow-up activities from day one and throughout the contract term.

This role-specific training strategy ensures School Nurses and Public Health Partners achieve full proficiency in the specialized workflows that support school-based immunization compliance, oral health screening documentation, and targeted public health outreach to underserved student populations.

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. On-demand video instructions or demonstrations for each user role.

SSG provides comprehensive on-demand video training resources designed to support role-specific learning and enable users to access instruction when and where they need it. These video deliverables are developed as part of the overall training strategy and complement other instructional materials to ensure all user groups achieve proficiency with *Casetivity*-IIS.

The on-demand video instructions include webinar recordings that support self-paced training for end users. These recordings capture live training sessions and allow users to review content at their own pace, revisit specific topics as needed, and access instruction outside of scheduled training windows. SSG delivers webinars using online meeting software such as GoTo Meetings, and recordings are posted on the resource website for ongoing access throughout the contract term.

Video content is tailored to address the distinct needs of different user audiences. SSG delivers training sessions separately for web-based users and electronic data exchange users when multiple user sites are trained simultaneously, ensuring that content remains relevant to each

group's workflows and responsibilities. This approach allows SSG to create targeted video demonstrations that align with the specific tasks, and system functions each role performs.

All video training materials are integrated with other instructional resources, including user manuals, PowerPoint slide decks, and clinical integration materials. This multi-format approach ensures users can access instruction in the format that best supports their learning style and operational context. When major system releases are deployed, video content is updated and new training sessions are recorded and posted to the resource website to reflect current functionality and workflows.

SSG's video training deliverables support the train-the-trainer model, enabling agency staff to become self-sufficient in training critical partners. SSG will provide around ten 15-minute training videos. By providing recorded sessions alongside live instruction, SSG ensures that training resources remain accessible for onboarding new users, supporting refresher training, and addressing ongoing learning needs throughout the life of the system.

4.2.3.10.2.2. Digital user guides or manuals for both functional and technical reference.

SSG provides comprehensive digital user guides and manuals designed to support both functional and technical users throughout the implementation and ongoing operation of *Casetivity*-IIS. These materials are developed to ensure users can independently research answers, complete core tasks, and maintain proficiency as the system evolves.

- *User Manuals:* SSG has standard user manuals that contain descriptions and screen captures allowing end users to research answers to questions about how to use the system. These manuals serve as comprehensive reference materials for functional users and are maintained by SSG as part of ongoing maintenance. Clients can add jurisdiction-specific content to the User Manuals as they see fit. The manuals are updated as major releases are made to the system and as needed to reflect new features, version upgrades, and changes to federal or jurisdictional standards.
- *Technical Reference Materials:* For technical users, including Information Technology staff and critical partners with role-based access, SSG provides technical training materials that address the structure and architecture of the system. These materials ensure sufficient knowledge transfer for ad-hoc query and report generation and cover technical system specifications.
- *Additional Training Resources:* SSG develops supplementary materials including PowerPoint slide decks that present system overviews tailored to various audiences, webinar recordings for self-paced training, clinical integration materials, and FAQs. All materials are posted on a resource website for easy access.

- *Ongoing Maintenance and Updates:* When major releases are made to the system, SSG updates all training materials and posts them on the resource website. New training sessions can be scheduled with users as needed to ensure continued proficiency with system enhancements and changes.

These digital user guides and manuals are designed to be responsive to a variety of learning styles and are user-centered, ensuring that both functional and technical users have the resources needed to achieve full proficiency and maintain it throughout the contract term.

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.

SSG provides a structured post-implementation support plan designed to ensure user adoption, operational stability, and a smooth transition following the Go-Live of *Casetivity*-IIS. This plan includes both enhanced dedicated support during the critical stabilization period and ongoing resources to sustain proficiency throughout the contract term.

- *Enhanced Dedicated Support Period:* Following Go-Live, SSG delivers a defined period of enhanced dedicated support focused on resolving user-adoption issues and ensuring smooth transition. During this stabilization period, SSG monitors system performance in the production environment to identify and address any material errors or operational concerns. The project team remains actively engaged to provide technical assistance, troubleshoot user challenges, and support workflow adjustments as end users and administrators adapt to the new system. This enhanced support period is structured to ensure the system operates reliably and users achieve full proficiency before transitioning to standard ongoing support.

SSG coordinates production deployment in collaboration with the State and provides go-live support and post-cutover stabilization. All readiness steps are planned jointly to ensure a successful transition and high adoption. The stabilization period allows SSG to validate that all system components function as intended under real-world conditions and that users can perform their roles effectively without disruption to immunization program operations.

- *Post-Implementation Training and Refreshers:* SSG's post-implementation support includes 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. SSG delivers training sessions and support materials to end users and administrators, ensuring all user groups maintain proficiency as the system evolves. Digital user guides, on-demand video instructions, and role-specific training resources remain available throughout the contract term to support continuous learning and adaptation.

This comprehensive post-implementation support plan ensures that the State's immunization program staff, provider office users, school nurses, and public health partners receive the assistance needed to achieve operational success and sustain system performance over time.

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.

SSG provides a comprehensive plan for annual and on-demand refresher training to ensure users remain proficient as the system evolves. This plan addresses new features, version upgrades, and changes to federal or jurisdictional standards through ongoing documentation updates and flexible training delivery methods.

SSG maintains all training materials as part of ongoing system maintenance. When major releases are made to the system, SSG updates user manuals, PowerPoint slide decks, webinar recordings, and clinical integration materials to reflect new functionality and changes. These updated materials are posted on the resource website, ensuring users have immediate access to current documentation that covers system enhancements and standards updates.

The user manual contains descriptions and screen captures that allow end users to research answers to questions about system use. These materials are maintained by SSG and updated as major releases are made and as needed to address evolving requirements.

When major releases occur or standards change, SSG schedules new training sessions with users as needed. This flexible approach allows the State to request refresher training aligned with specific system updates, new federal guidance, or jurisdictional policy changes. Based on the information in the solicitation, SSG proposes 1 refresher train-the-trainer session each year. SSG provides ongoing system support to ensure all end user questions and issues are addressed and that the system remains fully utilized.

This approach ensures users maintain proficiency throughout the contract term, can access current documentation on demand, and receive structured training when significant changes occur. SSG's commitment to maintaining training materials and providing responsive support reduces the administrative burden on State staff while ensuring compliance with evolving immunization standards.

4.2.3.11. Privacy:

4.2.3.11.1. The vendor must comply with all relevant State and Federal Data Privacy Laws, Regulations, and Policies.

Yes. SSG and *Casetivity*-IIS comply with all relevant state and federal data privacy laws, regulations, and policies. Security and data privacy are paramount in the solution. *Casetivity*-IIS complies with all relevant federal and state regulations, including HIPAA and CDC guidelines, ensuring the protection of sensitive health information.

The solution includes advanced security features such as encryption, role-based access control, and regular security audits. All provider and IIS users must complete a structured registration and legal acknowledgment process, including mandatory digital signature of all legal agreements confirming their understanding and acceptance of statutory reporting responsibilities. Solution-enforced access control ensures that users cannot interact with the solution unless this step is completed. Signed agreements are securely stored and auditable, serving as a compliance artifact.

Access to shared data is restricted based on user roles, organization jurisdiction, and data sensitivity—ensuring that only authorized personnel access patient-level details. Administrators may configure data elements included for each jurisdiction, including address granularity and demographic data based on privacy sensitivity. The system tracks and logs all outgoing and incoming cross-border data transactions to maintain compliance and accountability.

SSG confirms full compliance with all relevant state and federal data privacy laws, regulations, and policies governing immunization information systems.

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 time frames 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.

Casetivity-IIS maintains comprehensive internal audit logs that track all user access and activity across the solution, including logins, data additions, edits, deletions, and exports. The system captures detailed audit data at multiple levels to ensure full accountability and support compliance monitoring.

The solution logs every change made to patient records and related data, including immunizations, consent flags, and contact information. Each audit entry includes before-and-after values, timestamps, and the identity of the user who made the change. The system also tracks key lifecycle events such as record creation, merges, deletions, and restorations, as well as user session details including login and logout events and the roles used during each session.

For user access tracking specifically, *Casetivity*-IIS logs read access to patient records, capturing who viewed the record, what was accessed, and when. The system records the date and time of access, user ID and role information, and the specific data accessed. This ensures that all viewing activity—not just modifications—is captured for audit purposes.

The audit logging extends beyond the application layer to include infrastructure-level tracking. AWS CloudTrail logs all infrastructure changes, while API access logs capture request details, sources, and timestamps. Application logs record solution behavior, including errors and unusual performance patterns.

SSG configures audit log retention periods to meet jurisdictional requirements. The system retains logs online for a minimum of 90 days and maintains backups for one year by default. These retention periods can be extended to meet the Agency's six-year retention requirement through configuration adjustments during implementation.

Access to audit logs is restricted to authorized Agency staff through role-based permissions. Administrators can review audit data through multiple channels: built-in audit reports and dashboards that filter by user, date, entity type, or action; custom reports configured to meet specific monitoring or compliance requirements; audit history displayed directly in the user interface within patient records or tasks; and direct access to the reporting database for deeper investigations or advanced analysis.

SSG provides audit data to the Agency at designated timeframes or upon request in formats including Excel, CSV, and PDF for easy review and archiving. The comprehensive audit capabilities support compliance monitoring, investigation of suspected breaches, and adherence to HIPAA and CDC IIS Functional Standards requirements for tracking access to sensitive patient data.

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 OP-30 Incident Reporting and Response Procedures, (Attachment G) (https://www.wvdhhr.org/mis/policies/Incident_Reporting_and_Response.pdf)

4.2.3.11.3.1. OMIS Procedure IM-01 – Incident Management Plan (Attachment I) established the required incident-reporting channels and timelines. All incidents must be reported through the WVOT Incident Reporting System and to the OMIS Incident mailbox, consistent with OP-30.

SSG confirms that it will follow OMIS OP-30 Incident Reporting and Response Procedures and OMIS Procedure IM-01 Incident Management Plan (Attachment I) for reporting data breaches. All incidents will be reported through the WVOT Incident Reporting System and to the OMIS Incident mailbox, consistent with OP-30 requirements and the established incident-reporting channels and timelines outlined in IM-01.SSG maintains a comprehensive Incident Management Policy that emphasizes transparency, communication, and clarity to keep the Agency informed about the status of open incidents. SSG tracks and manages all incidents in JIRA, providing full visibility into incident status, resolution progress, and timelines. This approach ensures coordinated detection, reporting, containment, eradication, and recovery in alignment with Agency procedures.

SSG's incident management strategy is designed to meet all performance standards and timelines through robust tooling, dedicated resources, continuous monitoring, and proactive communication. Upon discovery or suspicion of a data breach, SSG will immediately follow the process outlined in the most recent version of OMIS OP-30, ensuring that all required reporting channels are utilized and timelines are met. This commitment guarantees efficient incident resolution and minimal disruption to Agency operations while maintaining full compliance with West Virginia's incident reporting requirements.

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.

Yes. SSG confirms that it will ensure IIS data is not used, released, or sold without specific authorization from the Agency, regardless of whether the data has been de-identified or included in a limited data set.

SSG maintains strict data governance policies that prohibit the use of client data for any purpose beyond the scope of the contracted services. The Agency retains full ownership of all data collected, stored, and processed within *Casetivity*-IIS. SSG provides privacy and security safeguards that protect Agency data from unauthorized use or disclosure. All data remains solely the property of the Agency throughout the contract term and beyond.

SSG will not use IIS data for analytics, artificial intelligence or machine learning (AI/ML) training, model development, or any secondary purpose without explicit written approval from the Agency. This prohibition applies to all forms of data, including de-identified datasets and limited data sets. SSG's data handling practices ensure that Agency data is accessed and processed only by authorized personnel for the express purpose of delivering and supporting the immunization information system services outlined in the contract.

Upon contract termination or at the Agency's request, SSG will return the entire dataset in the format specified by the Agency at no additional cost. SSG will cooperate fully with the Agency and any subsequent vendor to deliver all data, documentation, and work products within 30 working days of termination notice. Following Agency authorization, SSG will destroy all retained data in accordance with NIST Special Publication 800-88 within 30 days.

This commitment ensures that the Agency maintains complete control over its immunization data and that SSG operates as a trusted steward of sensitive public health information throughout the partnership.

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.

SSG certifies that it is not currently under investigation by any state or federal authority for a breach of data security. SSG maintains rigorous security protocols across its operations and hosting infrastructure to protect client data and ensure compliance with federal and state

requirements. The company hosts its solutions in AWS data centers that meet SOC 2 Type II and FedRAMP certification standards, and SSG's *Casetivity* platform itself maintains SOC 2 Type 2 certification. SSG undergoes regular audits and vulnerability assessments to ensure ongoing compliance with industry best practices and to proactively identify and address potential security concerns. This commitment to continuous security monitoring and improvement supports SSG's clean compliance record and its ability to serve as a trusted steward of sensitive public health information.

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. The reporting window is the last 10 years.

SSG certifies that it has not been involved in any breach of data security within the last 10 years. The company maintains a comprehensive Incident Management Policy that emphasizes transparency, communication, and clarity in managing information security incidents. This policy ensures a consistent and effective approach to incident response, with robust tooling, dedicated resources, continuous monitoring, and proactive communication to guarantee efficient incident resolution and minimal disruption to operations.

SSG's incident management strategy is designed to meet all performance standards and timelines required for secure handling of protected health information. The company's approach prioritizes accountability and stewardship in safeguarding data maintained on behalf of immunization programs and public health agencies.

4.2.3.11.7. The vendor must disclose any 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. The reporting window is the last 10 years.

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.

SSG has no 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.

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.

SSG certifies that it has never been convicted of, charged with, or is under investigation for violation of any criminal law or civil law governing health care fraud, abuse, or waste. SSG has not been the subject of an investigation, whether open or closed, by any government entity for a civil or criminal violation, nor has SSG been the subject of an indictment, grant of immunity, judgment, or conviction (including entering into a plea bargain) for conduct constituting a crime. SSG maintains a clean legal and regulatory record with no material pending litigation that would adversely affect its ability to meet contract requirements or have a material adverse effect on its financial condition.

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.

SSG certifies 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.

SSG confirms that it will not use IIS data for analytics, artificial intelligence/machine learning (AI/ML) training, model development, or any secondary purpose without explicit written approval from the State. This commitment is documented in the technical response and aligns with the State's requirement under Section 4.2.3.11.10.SSG ensures that data maintained on behalf of the IIS is not used, released, or sold without specific authorization from the Agency, regardless of whether the data has been de-identified or included with a limited data set. The

State retains full ownership of all IIS data, and SSG provides privacy and security safeguards that protect data from use or disclosure outside the scope of the solicitation. All data collected on behalf of the State remains solely the property of the Agency.

This data use restriction supports the State's data governance framework and ensures that immunization data is protected from unauthorized secondary uses. SSG's approach provides the State with complete control over how IIS data may be leveraged, ensuring compliance with applicable state and federal data privacy laws, regulations, and policies.

4.2.3.12. Security and Audit Compliance

4.2.3.12.1. Federal Security Compliance Requirements: The Vendor must ensure the IIS solution complies with applicable federal cybersecurity standards, including:

4.2.3.12.1.1. FedRAMP Authorization: The IIS solution must be hosted within at least a FedRAMP Moderate or higher authorized cloud environment. The IIS application itself is not required to hold a FedRAMP authorization. Vendors must provide proof that they can host the IIS solution within at least a FedRAMP Moderate or higher environment (e.g., existing FedRAMP-authorized cloud provider, current FedRAMP Moderate enclave, or executed agreement with a FedRAMP-authorized CSP). The Vendor must provide proof that the IIS solution is operating within at least a FedRAMP Moderate or higher environment prior to any data migration, onboarding, or system integration activities.

Yes. SSG confirms that *Casetivity*-IIS is hosted within Amazon Web Services (AWS), a FedRAMP-authorized cloud environment that meets FedRAMP Moderate or higher authorization requirements. AWS maintains government-grade cloud infrastructure designed to meet NIST 800-53 standards and federal cybersecurity requirements for protected health information.

SSG will provide proof that *Casetivity*-IIS is operating within this FedRAMP Moderate or higher environment prior to any data migration, onboarding, or system integration activities, as required by the State. This documentation will confirm that the cloud provider maintains FedRAMP Moderate or High authorization and 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.

The AWS hosting environment implements geographically distinct facilities with redundant power and cooling, role-based access controls with multi-factor authentication, AES-256

encryption at rest and TLS 1.3 in transit, continuous 24×7×365 monitoring and intrusion detection, and documented disaster recovery capabilities tested annually. The environment is HIPAA-eligible and maintains SOC 2 Type II attestations provided annually as supplemental evidence.

This FedRAMP-authorized hosting infrastructure ensures that *Casetivity*-IIS meets all mandatory federal security compliance requirements while supporting the State's privacy and IT governance standards throughout implementation and ongoing operations. SSG's single-tenant model requires dedicated infrastructure that creates additional expense for SSG compared to multi-tenant alternatives — a cost SSG absorbs because the data isolation and security controls it delivers are essential for a mission-critical statewide IIS. As an added benefit, this architecture enables SSG to grant authorized WVSIIS staff direct database access with Agency-controlled permissions, supporting West Virginia's data transparency and governance priorities.

4.2.3.12.1.2. 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).

Yes. All cryptographic modules used by *Casetivity*-IIS for data at rest and in transit are validated under NIST's Cryptographic Module Validation Program (CMVP) in accordance with FIPS 140-2 requirements.

Casetivity-IIS encrypts all data at rest using AES-256 encryption, implemented with FIPS 140-2 validated modules. For data in transit, the solution uses Transport Layer Security (TLS) protocols with cryptographic modules validated to FIPS 140-2 under NIST's CMVP. The system supports TLS 1.2 and TLS 1.3 at contract award and employs only approved cipher suites. SSG maintains the ability to implement newer TLS versions or configurations within 12 months of publication by NIST or CDC.

All IIS data exchanges, including connections to CDC's IZ Gateway, use TLS in accordance with the most current version of NIST SP 800-52 (Guidelines for the Selection, Configuration, and Use of TLS Implementations). SSG maintains compliance with evolving federal cybersecurity standards throughout the contract term and reports any changes to FedRAMP authorization, FIPS validation, or TLS support within 30 days.

This approach ensures that your immunization data remains protected with federally validated cryptographic controls at every stage—whether stored in the system or transmitted between authorized users and external systems—supporting your compliance obligations and protecting sensitive health information.

4.2.3.12.1.3. 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.

SSG maintains the ability to implement newer Transport Layer Security (TLS) versions or configurations within 12 months of publication by the National Institute of Standards and Technology (NIST) or the Centers for Disease Control and Prevention (CDC). This commitment is supported by SSG's secure software development lifecycle practices, change management processes, and continuous monitoring framework.

SSG's infrastructure is designed for rapid adaptation to evolving federal cybersecurity standards. The organization maintains documented secure development lifecycle practices aligned with NIST SP 800-218 (Secure Software Development Framework), which provides the foundation for implementing cryptographic and protocol updates. When NIST or CDC publishes new TLS versions or configuration guidance, SSG's vulnerability management program and compliance monitoring processes identify the requirement and initiate the implementation workflow.

SSG's change management process includes peer review, automated testing, and staged deployment to ensure new TLS configurations are implemented without service disruption. The organization performs Static Application Security Testing (SAST) scans integrated into the development pipeline for every code commit or build, and Dynamic Application Security Testing (DAST) scans at least quarterly and following any major release. This testing framework validates that new TLS implementations use cryptographic modules validated to Federal Information Processing Standards (FIPS) 140-2 or FIPS 140-3 under NIST's Cryptographic Module Validation Program and employ only approved cipher suites.

SSG's proven adaptability was demonstrated during the COVID-19 pandemic, when the organization delivered urgent configuration updates to support new reporting requirements and implement emerging HL7 profiles within compressed timelines—all without disruption to core registry services. This operational track record demonstrates SSG's capacity to operationalize complex federal directives under pressure.

SSG reports any changes to FedRAMP authorization, FIPS validation, or TLS support within 30 days, ensuring transparency and maintaining compliance with evolving federal cybersecurity standards throughout the contract term. This combination of technical capability, documented processes, operational experience, and compliance reporting confirms SSG's ability to implement newer TLS versions or configurations within the required 12-month timeframe.

4.2.3.12.1.4. 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.

Yes. SSG will 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.

SSG implements layered technical, administrative, and physical controls to enforce these commitments. The platform operates within hardened AWS VPC infrastructure protected by access control lists, intrusion detection and prevention systems, and end-to-end TLS and AES-256 encryption. All cryptographic modules used for data at rest and in transit are validated under NIST's Cryptographic Module Validation Program (CMVP). All data exchanges, including connections to CDC's IZ Gateway, use TLS in accordance with NIST SP 800-52, supporting TLS 1.2 and TLS 1.3 at minimum.

SSG conducts monthly vulnerability scans, applies automated patching, and maintains peer-reviewed change management processes. The incident response process is modeled on the NIST lifecycle and includes post-mortems and customer notification. Compliance automation dashboards monitor key security KPIs and ensure SSG consistently meets security objectives. Business continuity and disaster recovery plans, daily encrypted backups, and role-based access controls with annual reviews and multi-factor authentication further safeguard client data and maintain service resilience.

SSG will demonstrate the ability to implement newer TLS versions or configurations within 12 months of publication by NIST or CDC. Any changes to FedRAMP authorization, FIPS validation, or TLS support will be reported to the Agency within 30 days, ensuring transparency and continuous alignment with federal cybersecurity requirements throughout the contract term.

4.2.3.12.2. SOC 2 Type II Audit Report

4.2.3.12.2.1. The Vendor shall provide the State with an updated SOC 2 Type II audit report on an annual basis, no later than thirty (30) calendar days following the contract anniversary date, for the full duration of the contract term. Each report shall reflect an audit period ending no more than twelve (12) months prior to the date of submission. The State reserves the right to review, evaluate, and determine the adequacy and acceptability of the report. The State may, at its discretion, require the Vendor to furnish additional documentation,

clarification, or evidence of controls in the event of any material changes to the Vendor's hosting environment, operational processes, or security posture.

Yes. SSG will provide the State with an updated SOC 2 Type II audit report on an annual basis, no later than thirty (30) calendar days following the contract anniversary date, for the full duration of the contract term. Each report will reflect an audit period ending no more than twelve (12) months prior to the date of submission.

SSG maintains SOC 2 Type II certification as part of its commitment to security and operational excellence. The annual audit process ensures that SSG's controls related to security, availability, processing integrity, confidentiality, and privacy are independently verified and meet industry standards for protected health information systems. SSG provides this certification annually and supports the State's ability to review, evaluate, and determine the adequacy and acceptability of SSG's security posture.

The State retains the right to review each submitted report and may request additional documentation, clarification, or evidence of controls in the event of any material changes to SSG's hosting environment, operational processes, or security posture. SSG will respond to such requests in accordance with the contract terms and will ensure that all audit documentation reflects current operational practices and compliance with applicable federal and state cybersecurity standards.

This annual SOC 2 Type II reporting requirement is met in full and supports the State's ongoing oversight and risk management throughout the contract term.

4.2.3.12.2.2. 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.

Yes. SSG confirms that 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.

SSG's *Casetivity* platform maintains SOC 2 Type 2 certification and provides updated SOC 2 Type II audit reports on an annual basis. SSG hosts the solution in AWS data centers, which are SOC 2 Type II and FedRAMP certified, ensuring that the hosting provider adheres to rigorous security protocols and controls as required by industry standards. SSG undergoes regular audits and vulnerability assessments to ensure ongoing compliance with industry best practices.

SSG recognizes that while ISO/IEC 27001 certification demonstrates organizational security maturity, it serves only as supplemental documentation and does not replace the mandatory

SOC 2 Type II audit reporting requirement or compliance with U.S.-based data residency policies. SSG's compliance approach prioritizes the State's specified requirements and ensures that all data storage, transmission, and processing activities remain within U.S. borders in accordance with the State's data residency policy.

4.2.3.12.3. 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.

SSG understands and will comply with the State's requirements for annual third-party penetration testing, vulnerability management, remediation timelines, and reporting associated with the hosted *Casetivity*-IIS environment. SSG's cloud-enabled architecture incorporates security-focused operational practices including role-based access controls, encryption, security audits, disaster recovery protocols, incident response measures, and ongoing system maintenance activities designed to support a secure and resilient IIS environment.

4.2.3.12.4. 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:

4.2.3.12.4.1. 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.

SSG maintains a documented Secure Software Development Lifecycle (SSDLC) aligned with NIST SP 800-218 (Secure Software Development Framework) to ensure *Casetivity*-IIS is developed, maintained, and operated in accordance with federal cybersecurity standards. SSG maintains the SSDLC documentation throughout the contract term and provided to the Agency upon request.

SSG integrates security controls at every stage of the development lifecycle. The team performs Static Application Security Testing (SAST) scans integrated into the development pipeline for every code commit or build, and Dynamic Application Security Testing (DAST) scans at least quarterly and following any major release or production update. All identified vulnerabilities are tracked through a formal vulnerability management program, with critical and high-risk findings resolved within 30 calendar days unless otherwise approved by the Agency. SSG tracks and documents all third-party libraries and modules to ensure they remain updated and free of known critical vulnerabilities.

The development process follows a DevOps approach for application lifecycle management, combining agile sprint cycles with waterfall techniques at release milestones. At the conclusion of sprints within a release, SSG conducts robust system security testing, performance testing, data migration testing, disaster recovery testing, regression testing, and user acceptance testing. Secure code reviews and peer-reviewed change management processes ensure code quality and security before deployment. SSG implements continuous monitoring practices consistent with FedRAMP and NIST guidance, including automated vulnerability scanning and patching.

SSG conducts comprehensive system security assessments prior to go-live, aligned with HIPAA and NIST Cybersecurity Framework (CSF). The team performs vulnerability scanning, secure code reviews, penetration testing, and interconnection risk assessments for all environments. Remediation is tracked in a formal risk register with documented evidence of closure. Full security assessments are repeated every three years during maintenance and operations, with ad-hoc scans conducted following significant upgrades.

Third-party penetration testing of the hosted IIS environment is performed annually in compliance with NIST 800-53 standards. Detailed reports of findings and remediation actions are submitted to the Agency within 30 calendar days of test completion. All findings from SAST, DAST, and penetration testing are incorporated into the vulnerability management program with consistent remediation timelines.

These SSDLC practices ensure *Casetivity*-IIS is developed and maintained with security embedded throughout the lifecycle, protecting sensitive health information and maintaining compliance with federal cybersecurity standards.

4.2.3.12.4.2. 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.

Yes. SSG performs Static Application Security Testing (SAST) scans integrated into the development pipeline for every code commit or build, and Dynamic Application Security Testing (DAST) scans at least quarterly and following any major release or production update. SSG resolves all critical and high-risk findings within 30 calendar days, unless otherwise approved by the Agency.

SSG adheres to secure software development lifecycle (SSDLC) practices aligned with NIST SP 800-218 (Secure Software Development Framework). SAST scans are integrated directly into the development pipeline, ensuring that every code commit or build undergoes automated security analysis before advancing. This continuous scanning approach identifies vulnerabilities early in the development process, reducing risk and remediation costs.

DAST scans are performed at least quarterly and following any major release or production update to the IIS environment. These scans assess the running application for security weaknesses that may only be detectable during runtime, complementing the static analysis performed during development.

All findings from SAST and DAST scans are incorporated into SSG's documented vulnerability management program. SSG provides remediation plans for all identified vulnerabilities, with critical and high-risk findings resolved within 30 calendar days unless otherwise approved by the Agency. This remediation timeline is consistent with SSG's broader vulnerability management requirements and ensures that security issues are addressed promptly and systematically.

SSG tracks all defects and vulnerabilities in JIRA, providing full transparency and current reporting on the status of findings throughout the resolution process. This approach ensures accountability and enables coordinated response to security issues as they are identified.

SSG's SAST/DAST practices, combined with third-party penetration testing performed annually and continuous monitoring consistent with FedRAMP and NIST guidance, provide comprehensive security assurance throughout the software development lifecycle. This layered approach to application security testing ensures that *Casetivity*-IIS is developed, maintained, and operated in accordance with federal cybersecurity standards, meeting the requirement for integrated security testing with timely remediation of critical and high-risk findings.

4.2.3.12.4.3. 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.

Yes. SSG incorporates all findings from Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) into its vulnerability management program with remediation timelines consistent with Section 4.2.3.12.2. SSG conducts SAST scans integrated into the development pipeline for every code commit or build and performs DAST scans at least quarterly and following any major release or production update. All identified vulnerabilities are tracked within SSG's documented vulnerability management program, and the team provides remediation plans for all findings. Critical and high-risk vulnerabilities are resolved within 30 calendar days, unless otherwise approved by the Agency. SSG tracks remediation in a formal risk register with documented evidence of closure, ensuring full accountability and transparency throughout the vulnerability lifecycle. This integrated approach ensures that security testing findings are managed consistently with the same rigor applied to all vulnerability management activities, supporting the Agency's cybersecurity requirements and maintaining the security posture of *Casetivity*-IIS throughout its operational lifecycle.

4.2.3.12.4.4. 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.

Yes. SSG tracks and documents all third-party libraries and modules, ensuring they are updated and free of known critical vulnerabilities. This practice is integrated into SSG's secure software development lifecycle and vulnerability management program.

SSG maintains comprehensive documentation of all third-party components used in *Casetivity*-IIS. The vendor monitors these libraries and modules continuously to identify and remediate security risks before they can impact system operations. When critical vulnerabilities are identified in third-party components, SSG applies updates and patches according to established remediation timelines, with critical and high-risk findings resolved within 30 calendar days unless otherwise approved by the Agency.

This third-party component security management is supported by SSG's continuous monitoring practices, which align with FedRAMP and NIST guidance. The vendor performs Static Application Security Testing (SAST) scans integrated into the development pipeline for every code commit or build, and Dynamic Application Security Testing (DAST) scans at least quarterly and following any major release or production update. Findings from these scans are incorporated into SSG's vulnerability management program to ensure consistent tracking and remediation across all system components, including third-party libraries.

SSG's approach ensures that *Casetivity*-IIS remains secure and compliant with federal cybersecurity standards throughout the system lifecycle. By maintaining current, vulnerability-

free third-party components, SSG reduces security risk and supports the Agency's obligation to protect sensitive immunization and health information.

4.2.3.12.4.5. 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.

Yes. SSG implements continuous monitoring practices consistent with FedRAMP and NIST guidance, including automated code scanning and penetration testing at least annually.

SSG performs Static Application Security Testing (SAST) scans integrated into the development pipeline for every code commit or build, and Dynamic Application Security Testing (DAST) scans at least quarterly and following any major release or production update. The organization tracks and documents all third-party libraries and modules, ensuring they are updated and free of known critical vulnerabilities. SSG conducts penetration testing at least annually as part of its continuous monitoring program.

These practices are incorporated into SSG's vulnerability management program, with critical and high-risk findings resolved within 30 calendar days unless otherwise approved by the Agency. Monthly vulnerability scans and automated patching further support ongoing security posture management. All findings from SAST and DAST activities feed directly into remediation workflows with defined timelines aligned to risk severity.

SSG's continuous monitoring approach includes automated code scanning, regular vulnerability assessments, and compliance automation dashboards that enable the organization to monitor key security KPIs in real time. This layered approach ensures that *Casetivity*-IIS remains secure, resilient, and aligned with federal cybersecurity standards throughout the system lifecycle.

4.2.3.12.5. 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.

SSG hosts *Casetivity*-IIS in a FedRAMP Moderate-authorized cloud environment provided by Amazon Web Services (AWS). AWS maintains FedRAMP Moderate authorization, which meets the FedRAMP Moderate requirement specified in this solicitation. SSG will provide documentation confirming AWS' current FedRAMP authorization status upon request.

This hosting arrangement ensures that all Immunization Information System (IIS) data is stored, processed, and transmitted exclusively within U.S.-based data centers that meet federal cybersecurity standards. The FedRAMP-authorized environment provides the security controls, audit protocols, and compliance framework required for protected health information and immunization data management.

SSG will complete and submit the Vendor Attestation Form within 30 calendar days of contract execution, certifying cloud provider compliance with FedRAMP Moderate or High authorization, U.S.-based data residency requirements, and all applicable state and federal cybersecurity policies and standards as outlined in Section 4.2.3.12.6 of the solicitation.

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.

SSG hosts *Casetivity*-IIS exclusively within Amazon Web Services (AWS), a FedRAMP Moderate authorized cloud service provider that maintains U.S.-based data centers in compliance with federal government and West Virginia cybersecurity and data residency requirements. All IIS data—including backups, logs, and metadata—is stored and processed exclusively within data centers physically located in the continental United States. No data is transmitted, processed, or stored outside U.S. borders at any time, including during disaster recovery, failover, or support operations.

AWS provides HIPAA-eligible, government-grade cloud infrastructure designed to meet NIST 800-53 standards and federal security requirements. The hosting environment implements geographically distinct primary and failover facilities with redundant power and cooling, ensuring continuous availability while maintaining U.S.-based data residency. SSG's disaster recovery plan, tested annually, operates entirely within U.S.-based AWS regions to ensure compliance with data residency restrictions during all contingency scenarios.

The solution encrypts all data at rest using AES-256 encryption implemented with FIPS 140-2 validated cryptographic modules. Data in transit is protected using TLS 1.3 encryption in accordance with NIST SP 800-52 guidelines. These encryption standards apply to all data exchanges, including connections to CDC's IZ Gateway, and are maintained consistently across all U.S.-based data center operations.

SSG provides documentation verifying U.S.-based data residency and maintains compliance with applicable federal and state data protection laws and regulations. The solution operates within AWS's FedRAMP Moderate authorized environment, and SSG holds SOC 2 Type II and HIPAA attestations that are provided annually to support ongoing compliance verification. Continuous

monitoring, intrusion detection, and role-based access controls further ensure that data security and residency requirements are maintained throughout all system operations.

This architecture ensures that West Virginia's IIS data remains exclusively within U.S.-based infrastructure while meeting federal cybersecurity standards, state data residency requirements, and HIPAA compliance obligations.

4.2.3.12.5.3. Supports compliance with applicable Executive Branch and Office of Management Information Services (OMIS) Security Policies.

Yes. SSG hosts *Casetivity*-IIS within a FedRAMP Moderate or higher authorized cloud environment, ensuring compliance with applicable Executive Branch and Office of Management Information Services (OMIS) Security Policies. SSG's cloud infrastructure is built on hardened AWS VPC architecture protected by access control lists, intrusion detection and prevention systems, and end-to-end TLS and AES-256 encryption. This environment supports the security standards required by West Virginia's cybersecurity framework and federal guidelines.

SSG implements layered technical, administrative, and physical controls that align with OMIS requirements, including role-based access control with annual reviews, multi-factor authentication-protected VPNs, monthly vulnerability scans, automated patching, and peer-reviewed change management processes. The incident response process follows the NIST lifecycle and includes post-incident reviews and customer notification protocols consistent with state reporting requirements. Business continuity and disaster recovery plans, daily encrypted backups, and compliance automation dashboards ensure SSG meets recovery time objectives and monitors key security performance indicators.

SSG will complete and submit the required Vendor Attestation Form within 30 calendar days of contract execution, certifying compliance with U.S.-based data residency restrictions, SOC 2 Type II audit submission timelines, penetration testing and vulnerability remediation protocols, cloud provider compliance, and all applicable state and federal cybersecurity policies and standards. SSG's cloud provider documentation confirms FedRAMP Moderate or High authorization and exclusive U.S.-based data center operations, meeting West Virginia's data residency and transmission requirements. This approach ensures Casetivity-IIS operates within a secure, compliant environment that supports OMIS Security Policies and protects sensitive immunization data throughout the system lifecycle.

4.2.3.12.6. Vendor Attestation Form:

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:

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.

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.

Yes. SSG will complete and submit a Vendor Attestation Form within 30 calendar days of contract execution, certifying compliance with all required elements including U.S.-based data residency and transmission restrictions, SOC 2 Type II audit submission timelines, penetration testing and vulnerability remediation protocols, cloud provider compliance, and all applicable state and federal cybersecurity policies and privacy requirements.

SSG hosts *Casetivity*-IIS in AWS data centers located exclusively within the continental United States, ensuring full compliance with U.S.-based data residency requirements. All IIS data—including backups, logs, and metadata—remains within U.S. borders at all times, with no transmission, processing, or storage outside the United States during normal operations, disaster recovery, or support activities. SSG maintains SOC 2 Type 2 certification for the *Casetivity* platform and undergoes regular audits and vulnerability assessments to ensure ongoing compliance with industry best practices. AWS, as SSG's cloud provider, maintains both SOC 2 Type II and FedRAMP certification, meeting the highest standards of physical security and operational controls required for government systems.

SSG will provide updated SOC 2 Type II audit reports annually, no later than 30 calendar days following the contract anniversary date, with each report reflecting an audit period ending no more than 12 months prior to submission. The solution complies with all relevant data protection regulations through encryption of data in transit and at rest, role-based access control, multi-factor authentication, and continuous security monitoring. SSG will maintain

documentation of its incident response policy and plan aligned with NIST SP 800-61 and will follow the Agency's incident response procedures as specified in the contract.

The Vendor Attestation Form will confirm SSG's adherence to penetration testing protocols, vulnerability remediation timelines, and all applicable West Virginia Executive Branch and Office of Management Information Services security policies. SSG is prepared to provide updated attestations annually or upon any material changes to operations or hosting environment, subject to verification under the contract's audit and attestation requirements.

4.2.3.12.7. 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:

4.2.3.12.7.1. NIST Alignment: The Vendor's IR policy and plan must be aligned with the most current version of VIST SP 800-61 (*Computer Security Incident Handling Guide*) or successor publications.

SSG maintains a comprehensive Incident Response (IR) policy and plan aligned with NIST SP 800-61 (Computer Security Incident Handling Guide). The IR framework follows the NIST incident response lifecycle and includes detection, reporting, containment, eradication, recovery, and post-incident analysis. SSG tracks and manages all incidents in JIRA, ensuring consistent documentation and resolution tracking throughout the incident lifecycle.

The IR process incorporates layered technical, administrative, and physical controls to support rapid incident detection and response. These controls include role-based access with annual reviews and multi-factor authentication (MFA)-protected VPNs, hardened AWS Virtual Private Cloud (VPC) infrastructure protected by Access Control Lists (ACLs) and Intrusion Detection/Prevention Systems (IDS/IPS), end-to-end Transport Layer Security (TLS) and Advanced Encryption Standard (AES)-256 encryption, monthly vulnerability scans, automated patching, and peer-reviewed change management. The incident response process includes post-mortems and customer notification protocols to ensure transparency and continuous improvement.

SSG's IR policy emphasizes transparency, communication, and clarity to keep clients informed about the status of open incidents. The approach ensures consistent and effective management of information security incidents through robust tooling, dedicated resources, continuous monitoring, and proactive communication. Business continuity and disaster recovery plans

support the IR framework with daily encrypted backups and compliance automation dashboards that monitor key security Key Performance Indicators (KPIs).

SSG will work with the Agency to ensure the IR plan complements and integrates with the Agency's incident response procedures, ensuring coordinated detection, reporting, containment, eradication, and recovery. SSG commits to updating its IR policy and plan within six months of any NIST revision or federal mandate affecting incident response practices, and to submitting updated attestation forms annually or upon material changes to hosting environment, security posture, or compliance status. SSG will address any deficiencies identified during audits or attestations within 60 calendar days with written confirmation of remediation provided to the Agency.

4.2.3.12.7.2. 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.

Yes. SSG will update the IR policy and plan within 6 months of any NIST revision or federal mandate affecting incident response practices.

4.2.3.12.7.3. 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.

SSG's Incident Response (IR) plan is designed to complement and integrate seamlessly with the Agency's incident response procedures through a structured, collaborative approach that ensures coordinated detection, reporting, containment, eradication, and recovery.

- *Coordinated Detection and Monitoring:* SSG employs a robust suite of monitoring tools to continuously track system performance and detect potential issues early. This proactive monitoring enables the SSG team to identify and address concerns before they escalate into major disruptions. When an incident is detected, SSG immediately evaluates the incident's scope and potential impact to determine the most effective resolution path. If a cybersecurity threat is identified, SSG engages its Security Incident Response Plan to ensure appropriate technical and security protocols are activated.
- *Integrated Reporting and Communication:* SSG maintains clear communication with all critical partners throughout the incident lifecycle. Internally, updates are shared with the executive team and relevant personnel to ensure alignment on response activities. Externally, SSG's designated External Liaison manages client communications, providing regular status updates to those affected by the incident. SSG establishes a dedicated communication channel, typically via Microsoft Teams, for real-time coordination among team members and with Agency personnel. In cases of significant incidents, SSG activates established communication protocols to ensure timely and transparent updates to the Agency.

- *Coordinated Containment, Eradication, and Recovery:* SSG mobilizes internal and external resources, including Managed Service Providers (MSPs), and performs a risk assessment to prioritize recovery efforts. SSG's recovery strategy prioritizes restoration activities based on the assessed risks and potential operational impacts, ensuring that critical systems and functions are restored first. All incidents are tracked and managed in JIRA, providing full visibility and documentation throughout the resolution process.
- *Alignment and Integration:* SSG will work directly with the Agency to ensure the right end-to-end incident management process is in place that meets the Agency's specific needs for the Immunization Information System. This collaborative approach ensures that SSG's IR plan complements the Agency's incident response procedures, creating a unified response framework that supports coordinated detection, reporting, containment, eradication, and recovery across both organizations.

4.2.3.12.7.4. 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.

SSG acknowledges and accepts the Agency's requirement to conduct annual incident response exercises throughout the term of the Contract. SSG will conduct at least one annual incident response exercise, such as a tabletop exercise or simulated security incident, to evaluate the effectiveness of incident response procedures, communication protocols, and operational readiness. Following each exercise, SSG will prepare and provide the Agency with a summary report within 30 calendar days documenting the exercise objectives, results, lessons learned, identified improvement opportunities, and planned corrective actions.

4.2.3.12.7.5. Availability: The Vendor must make its IR policy and plan available to the Agency upon request and certify compliance annually.

SSG acknowledges and accepts the Agency's requirement to make its Incident Response (IR) Policy and Incident Response Plan available for Agency review upon request, subject to appropriate confidentiality and security protections. SSG will also provide annual certification that its Incident Response Policy and Plan remain current and that SSG continues to operate in accordance with its documented incident response procedures throughout the term of the Contract.

4.2.3.12.7.6. Continuous Improvement: The Vendor must incorporate lessons learned from incidents and exercises into its IR plan within 60 calendar days of identification.

SSG acknowledges and accepts the Agency's requirement for continuous improvement of its incident response program. SSG will evaluate lessons learned from security incidents, incident response activities, and annual incident response exercises and will incorporate applicable

updates into its Incident Response Plan within 60 calendar days of identifying improvement opportunities. Updates may include revisions to procedures, roles and responsibilities, communication protocols, response processes, or other operational controls to strengthen SSG's incident response capabilities and support ongoing readiness.

4.2.3.12.8. 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:

4.2.3.12.8.1. 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.

SSG acknowledges and accepts the Agency's requirement to provide evidence necessary to verify compliance throughout the term of the Contract. Upon the Agency's request, SSG will provide available system documentation, policies, configuration documentation, testing results, audit reports, and other reasonable evidence necessary to demonstrate compliance with contractual and technical requirements, at no additional cost to the Agency.

4.2.3.12.8.2. Timely Response: Provide requested evidence within 30 calendar days of the State's request, unless otherwise approved in writing by the Agency.

SSG acknowledges and accepts the Agency's requirement to provide requested compliance evidence in a timely manner. Unless otherwise approved in writing by the Agency, SSG will provide the requested documentation, policies, configurations, testing results, audit reports, or other requested evidence within 30 calendar days of the Agency's request.

4.2.3.12.8.3. 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.

SSG acknowledges and accepts the Agency's requirement for independent verification of security controls. Upon reasonable notice, SSG will cooperate with the Agency or its designated third-party auditor to facilitate independent verification activities, including technical assessments and, where applicable, coordinated site visits. Verification activities will be conducted in accordance with mutually agreed scheduling, applicable security procedures, and confidentiality requirements to protect the security of SSG's facilities, personnel, systems, and customer information while providing the Agency with the information necessary to verify compliance.

4.2.3.12.8.4. Ongoing Attestation: Complete and submit updated attestation forms annually, or upon material changes to the Vendor's hosting environment, security posture, or compliance status.

Yes. SSG will complete and submit updated attestation forms annually, or upon material changes to the hosting environment, security posture, or compliance status. This commitment ensures that the Agency maintains current visibility into SSG's compliance posture and operational controls throughout the contract term.

SSG provides SOC 2 Type II and HIPAA attestations annually as part of its standard audit and certification cycle. These attestations document SSG's adherence to security, availability, processing integrity, confidentiality, and privacy principles. When material changes occur—such as infrastructure updates, security control modifications, or shifts in compliance status—SSG proactively submits updated attestation forms to keep the Agency informed and aligned with current operational realities.

This annual attestation process integrates with SSG's broader compliance framework, which includes documented disaster recovery and contingency plans tested annually, monthly vulnerability scans, automated patching protocols, and incident response procedures modeled on the NIST lifecycle. The Agency retains the right to request updated attestations at any time, and SSG will respond within the timelines specified in the contract to support ongoing oversight and risk management.

SSG confirms full compliance with this requirement and will maintain transparent, timely attestation reporting throughout the partnership.

4.2.3.12.8.5. 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).

Yes. SSG confirms that audits and attestations will remain aligned with the most current versions of applicable federal and state cybersecurity standards, including NIST, FedRAMP, FIPS, and OMIS policies. SSG implements compliance automation dashboards to monitor key security KPIs and ensure continuous alignment with evolving standards. The company maintains layered technical, administrative, and physical controls that support ongoing compliance, including role-based access with annual reviews, hardened AWS VPC infrastructure, monthly vulnerability scans, automated patching, and an incident-response process modeled on the NIST lifecycle. SSG will update its incident response policy and plan within six months of any NIST revision or federal mandate affecting incident response practices, and will address any deficiencies identified during audits or attestations within 60 calendar days or as otherwise approved by the Agency, providing written confirmation of remediation. This commitment ensures that SSG's

security posture evolves in step with federal and state requirements, protecting client data and maintaining service resilience throughout the contract term.

4.2.3.12.8.6. 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.

Yes. SSG will 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. This commitment aligns with the Agency's security and compliance oversight requirements and ensures that SSG maintains continuous alignment with applicable federal and state cybersecurity standards, including NIST, FedRAMP, FIPS, and OMIS policies.

SSG's remediation process includes root cause diagnosis, corrective action planning, implementation of fixes, validation testing, and formal documentation of all remediation activities. The Agency will receive written confirmation upon completion of remediation, including evidence of corrective measures taken and verification that the deficiency has been resolved. If circumstances require an extension beyond the 60-day timeframe, SSG will work collaboratively with the Agency to establish an approved remediation schedule and provide regular status updates throughout the resolution process.

This remediation obligation applies to all audit and attestation activities, including SOC 2 Type II audits, penetration testing findings, vulnerability assessments, and compliance reviews. SSG's commitment to timely deficiency resolution supports the Agency's risk management objectives and ensures that *Casetivity*-IIS maintains the security posture required to protect immunization data and support public health operations.

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.

SSG confirms its full understanding and acceptance of the Agency's Acceptance Criteria. The Agency will issue written Acceptance of the IIS solution only after verifying that all functional, technical, security, interoperability, and performance requirements defined in the Solicitation

have been fully met. SSG acknowledges that no portion of the system will be considered Accepted until all Acceptance activities are completed and approved in writing by the Agency.

SSG's implementation methodology directly supports this requirement through a structured testing and sign-off process. SSG will continue to work in the System Integration Test Environment until the Agency signs off that the system meets the functional, systemic, security, and ADA requirements. This phase of testing is considered complete only when all previous tests have either passed—meaning any issues found are resolved through development work—or known issues are clearly documented by the requirement owner as having been determined acceptable as-is, whether permanently or temporarily. Once all testing is complete and issues are resolved, the Agency will provide formal email sign-off indicating that the release candidate is ready for deployment.

SSG's deployment process includes comprehensive validation before production release. The engineering team will not consider deployment complete until the system meets all functional requirements. SSG will monitor the system and provide necessary technical support after deployment to the production environment. The project team will review release activities and document an After-Action Review to capture lessons learned.

Upon successful conclusion of UAT and successful system deployment, the Agency will issue a letter of UAT Sign-off. SSG will ensure the security infrastructure and software is fully hardened and compliant with all security requirements, with Security Documentation describing all security measures taken. SSG will remediate all defects identified during Acceptance Testing.

SSG confirms that *Casetivity*-IIS will be deemed acceptable only when all conditions specified by the Agency have been met, and SSG will support the Agency through all Acceptance activities until written Notice of Acceptance is issued.

4.2.3.13.2. Acceptance Testing: The Vendor must support and participate in Agency-led Acceptance Testing, which includes but is not limited to:

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, HER 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

All defects identified during Acceptance Testing must be remediated by the Vendor at no additional cost to the Agency.

SSG confirms full support for and participation in Agency-led Acceptance Testing across all required testing activities. SSG's approach to Acceptance Testing is comprehensive, structured, and designed to ensure *Casetivity*-IIS meets all functional, technical, security, interoperability, and performance requirements before the Agency issues written Acceptance.

SSG will actively support the following Acceptance Testing activities:

- *Functional Testing of All Modules and Workflows:* SSG conducts thorough functional testing in the System Integration Test Environment to validate that all system functionality operates as specified. This includes testing all modules, workflows, and business processes to ensure they align with the Agency's approved Implementation Plan and solicitation requirements. SSG provides functional test results, automated test cases, and automated test results as deliverables during this phase.
- *Data Migration Validation:* SSG implements a phased data migration approach that includes rigorous validation at each stage. User Acceptance Testing includes end-to-end functional testing and data validation by exercising typical business process workflows. SSG analyzes migrated data, identifies data fix measures if discrepancies are found, and obtains critical partner sign-off before proceeding to production migration.
- *Interface and Interoperability Testing:* SSG validates that the transport layer between test sites and *Casetivity*-IIS is fully functional as part of onboarding and interoperability testing. The team conducts comprehensive interface testing to verify HL7 messaging, FHIR-based interfaces, IIS-to-IIS data exchange, Health Information Exchange (HIE) integrations, electronic health record (EHR) connectivity, and connectivity through the CDC IZ Gateway, as applicable. All required interfaces are tested to ensure they exchange data accurately, securely, and consistently with Agency-designated systems and meet all functional and interoperability requirements prior to production deployment.
- *Performance and Load Testing:* SSG conducts performance testing to confirm scalability under expected load and stress testing to assess stability at extreme loads. *Casetivity*-IIS is designed to support high transaction volumes and resource-intensive tasks without degrading performance, handling over 130,000 queries per hour and 35,000 vaccination messages per hour with sub-second response times. Follow-up performance testing cycles are conducted after data migration to ensure the system handles additional data without performance degradation.
- *Security and Access Control Verification:* SSG performs security testing including penetration and vulnerability assessments to validate that all security controls are implemented and operational. This includes authentication, authorization, audit logging, and compliance with Agency security standards. SSG ensures the security infrastructure

and software are fully hardened and compliant with all security requirements, providing Security Documentation that describes all security measures taken.

- *User Acceptance Testing (UAT) with Agency-Designated Staff:* SSG facilitates comprehensive User Acceptance Testing to determine whether the deployed system satisfies the acceptance criteria of the requirements owner and business users. SSG supports UAT by ensuring end users have test accounts, supporting end users with questions and triaging any feedback. Deliverables include a web-enabled issue reporting and tracking tool integrated with change control mechanisms, and updates to the solution including source code repository and system documentation. UAT testing continues until all tests have either passed or known issues are clearly documented by the requirement owner as acceptable.

All defects identified during Acceptance Testing will be remediated by SSG at no additional cost to the Agency. SSG uses a web-enabled issue reporting and tracking tool integrated with change control mechanisms to manage defect resolution efficiently. All test cases are traceable to requirements through the Traceability Matrix and require Agency approval before execution.

Based on the solicitation, West Virginia would like to run and execute UAT. So, unless directed otherwise, SSG will plan to be available each day during User Acceptance Testing (UAT), estimated to be at around an hour a day, to provide support with any questions that come up during UAT testing.

SSG will continue working through all testing phases until the Agency provides formal sign-off that the release candidate is ready to move to the production environment. Upon successful conclusion of UAT and system deployment, SSG supports the Agency's issuance of a written Notice of Acceptance, confirming that all Acceptance Criteria have been met and the system is ready for production use.

4.2.3.13.3. 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.

SSG confirms acceptance of all IIS Acceptance Criteria conditions as defined in Section 4.2.3.13 of the Solicitation. *Casetivity*-IIS will meet all specified acceptance requirements prior to the Agency's issuance of written Acceptance.

SSG will support and participate in all Agency-led Acceptance Testing activities, including functional testing of all modules and workflows, data migration validation, interface and interoperability testing for HL7, FHIR, IIS-to-IIS, HIE, and EHR connections, performance and load testing, security and access control verification, and user acceptance testing with Agency-designated staff. All defects identified during Acceptance Testing will be remediated at no additional cost to the Agency.

Casetivity-IIS will be deemed acceptable only when the following conditions are met:

- All system functionality is fully implemented as described in SSG's approved Implementation Plan and the requirements of the Solicitation
- All required interfaces are operational, exchanging data accurately and consistently with Agency-designated systems
- All defects classified as Critical or High severity are resolved, and no Medium or Low defects materially impact system operation or Agency workflows
- All documentation is delivered, including system architecture, configuration guides, user manuals, training materials, and administrative procedures
- All security controls are implemented and validated, including authentication, authorization, audit logging, and compliance with Agency security standards
- The system operates in the Agency's production environment without material errors for a mutually agreed-upon stabilization period

- SSG has met all contractual deliverables, including reporting, project management, and communication requirements

SSG will not invoice for implementation-related fees until the Agency issues a written Notice of Acceptance. Annual, recurring, subscription, hosting, or maintenance fees will not begin prior to Acceptance. Following Acceptance, SSG will invoice only for the prorated portion of annual fees corresponding to the remainder of the current contract year, calculated based on the number of days remaining following the date of Acceptance.

If the system fails to meet any Acceptance Criteria, SSG will correct all deficiencies identified in the Agency's Notice of Rejection at no additional cost and resubmit the system for Acceptance Testing. SSG acknowledges the Agency's right to repeat any portion of testing necessary to validate corrections.

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.

Yes. SSG confirms that it will not invoice for implementation-related fees until the Agency issues a written Notice of Acceptance, and that no annual, recurring, subscription, hosting, or maintenance fees will begin prior to Acceptance.

SSG's implementation approach aligns fully with the Agency's Acceptance Criteria requirements outlined in Section 4.2.3.13. During the Implementation Period, SSG will not assess, invoice, or otherwise charge the Agency for any fees, including annual licensing, subscription, hosting, maintenance, or support fees. Payment for implementation services will be tied exclusively to the successful completion of mutually agreed-upon implementation milestones established during initial planning sessions and incorporated into the approved Project Plan. No milestone payment will be due until the Agency has verified and approved completion of the corresponding milestone.

Final implementation payment will be made only upon the Agency's formal written Acceptance of the fully implemented *Casetivity*-IIS solution. This Acceptance will follow successful completion of all Acceptance activities, including User Acceptance Testing (UAT), operational validation of all required interfaces, resolution of all Critical and High severity defects, delivery

of all required documentation, validation of all security controls, and completion of the mutually agreed-upon stabilization period in the Agency's production environment.

Only upon issuance of the written Notice of Acceptance may SSG invoice for implementation-related fees. At that time, SSG will invoice only for the prorated portion of annual licensing, subscription, hosting, maintenance, or support fees corresponding to the remainder of the current contract year. Under no circumstances will SSG invoice for a full annual fee for a partial contract year. Proration will be calculated based on the number of days remaining in the contract year following the date of Acceptance.

This billing structure protects the Agency's investment by ensuring that all recurring fees are contingent upon successful system implementation, operational readiness, and formal Agency acceptance of the solution.

4.2.3.13.5. 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.

Yes. SSG confirms that if the system fails Acceptance Testing, SSG will correct all deficiencies at no additional cost to the Agency and resubmit the system for Acceptance Testing.

The project context explicitly states that 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.

SSG's approach ensures that all defects identified during Acceptance Testing are remediated at no additional cost to the Agency. SSG follows a structured defect resolution process that includes recreating reported issues, performing comprehensive testing to confirm resolution, conducting related tests to ensure fixes have not introduced new issues, and scheduling regression testing prior to the next release. This systematic approach ensures that corrected deficiencies are thoroughly validated before resubmission.

SSG will work with the Agency until full acceptance of the solution is achieved. This commitment extends through User Acceptance Testing and all subsequent validation activities required to meet the Acceptance Criteria defined in the Solicitation.

4.2.3.13.6. 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.

Yes. SSG confirms that upon the Agency's formal written Acceptance of the fully implemented IIS solution, SSG will invoice only for the prorated portion of annual licensing, subscription, hosting, maintenance, or support fees corresponding to the remainder of the current contract year. Under no circumstances will SSG invoice for a full annual fee for a partial contract year. Proration will be calculated based on the number of days remaining in the contract year following the date of Acceptance.

This approach ensures the Agency pays only for services actually rendered during the initial contract year, aligning billing precisely with system availability and operational use. Following completion of the prorated billing period, SSG will invoice for no more than twelve months of annual fees for any given billing period, billed either annually in advance or, subject to Agency approval, in quarterly installments. SSG will not invoice for any period beyond the next twelve months, nor for any period that has not yet commenced.

This billing structure supports transparent financial management, predictable budgeting, and equitable cost allocation tied directly to system acceptance and operational readiness.

4.2.3.13.7. 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 pilled 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.

Yes. SSG confirms that it will invoice for no more than twelve (12) months of annual fees per billing period. Annual licensing, subscription, hosting, maintenance, and support fees will be billed only in advance for the upcoming twelve-month period or, at SSG's option and subject to Agency approval, in quarterly installments billed in advance for the upcoming quarter. SSG will not invoice for multiple years of annual fees in a single lump-sum invoice, nor will SSG invoice for any period beyond the next twelve months or for any period that has not yet commenced.

This billing structure applies following completion of the prorated billing period that begins upon the Agency's formal written Acceptance of the fully implemented IIS solution. During that initial prorated period, SSG will invoice only for the prorated portion of annual fees corresponding to the remainder of the current contract year, calculated based on the number of days remaining in the contract year following the date of Acceptance.

SSG's invoicing practices align with the Agency's requirements for transparent, predictable annual fee management and ensure that the Agency is never billed for services beyond the authorized twelve-month advance billing period.

4.3 – Qualifications & Experience

4.3.1 Qualifications & Experience Information

4.3.1.1. 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.

Strategic Solutions Group (SSG) is a privately held software and consulting firm that has focused exclusively on public health and human services information systems for more than 23 years. SSG designs, develops, implements, hosts, and supports enterprise technology solutions that help government agencies manage critical programs, improve data quality, enhance interoperability, and support informed public health decision-making.

SSG, as a privately owned LLC, operates independently and serves exclusively government public health and human services agencies — with no private equity ownership, no obligation to maximize short-term shareholder returns, and no competing commercial priorities. In an IIS market where most (if not all) other viable solutions are either publicly traded or PE-owned, SSG's independent structure allows it to remain genuinely mission-driven: placing customer outcomes ahead of profit timelines, investing in R&D on a long-term basis, and making decisions guided by what is best for the public health programs it serves. This independence — combined with a 100% project implementation success rate over more than 23 years — reflects the kind of long-term partnership orientation that West Virginia's statewide immunization program deserves.

SSG is the developer of the *Casetivity* platform, a configurable suite of public health and human services solutions used by state agencies to support immunization programs, disease surveillance, early intervention services, environmental health programs, clinical decision support, health information exchange, and other mission-critical public sector initiatives. Unlike firms that primarily provide consulting services around third-party products, SSG delivers both the software platform and the implementation, operational, and support services required to ensure long-term project success.

A cornerstone of SSG's experience is the design, development, implementation, and ongoing operation of statewide public health systems. Most notably, SSG designed, developed, implemented, and continues to operate the Massachusetts Immunization Information System (MIIS), the Commonwealth's statewide IIS. Originally implemented in 2006, MIIS has remained in continuous production operation for approximately 19 years and continues to support immunization management, provider participation, interoperability, vaccine inventory

management, clinical decision support, reporting, and public health analytics. SSG is also currently implementing *Casetivity*-IIS for the Wisconsin Department of Health Services.

Over the past two decades, SSG has successfully delivered more than 100 technology projects for government agencies and maintains a 100 percent implementation success rate. Every project undertaken by SSG has successfully reached production and continues to support operational public health programs. SSG currently operates multiple production instances of the *Casetivity* platform across several states, serving millions of records and thousands of users through secure, cloud-hosted Software as a Service (SaaS) environments.

SSG provides end-to-end services throughout the project lifecycle, including project management, business analysis, solution architecture, software development, interoperability, data migration, testing, training, cloud operations, cybersecurity, maintenance, and customer support. This combination of deep public health domain expertise, proven technology platforms, and long-term operational experience enables SSG to successfully deliver and support complex information systems for government health and human services agencies.

SSG may be the only independently owned organization remaining in the IIS market.

23 years. 100+ government projects. 100% implementation success rate. Every client SSG has ever implemented for continues to operate their system today.

4.3.1.2. 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.

SSG does not have a parent corporation or any subsidiaries.

SSG's company information is as follows:

- Address: 1329 Highland Ave, Needham, MA 02492
- Phone: 781-400-1322
- Fax: 781-644-7460
- FEIN: 80-0298804
- Website: https://www.ssg-llc.com
- Email: sales@ssg-llc.com

4.3.1.3. Organization and Structure: The Vendor should provide an overview of its organization 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.

Strategic Solutions Group (SSG) is a privately held software and consulting firm focused exclusively on public health and human services information systems. For more than 23 years, SSG has designed, developed, implemented, and supported enterprise solutions that help government agencies manage critical public health programs and data.

SSG operates using a matrix organizational model designed to promote customer focus, subject matter expertise, operational accountability, and long-term solution stewardship. This structure combines vertically aligned delivery divisions with horizontally aligned functional practices and shared services teams. Together, these groups provide the expertise, governance, and operational support necessary to successfully implement and operate complex public health systems such as *Casetivity*-IIS.

Delivery Divisions

SSG organizes project delivery through dedicated business divisions aligned to specific public health domains, including Immunization, Disease Surveillance, Early Intervention, and other public health solution areas. Each division is responsible for solution delivery, customer engagement, product evolution, and long-term operational success within its respective domain.

The Immunization Division is responsible for the delivery, support, and continued enhancement of *Casetivity*-IIS. This division includes project managers, business analysts, technical resources, and delivery teams with specialized expertise in immunization program operations, interoperability, public health reporting, vaccine management, and IIS implementation.

This organizational approach enables SSG to maintain deep domain expertise while providing clients with dedicated teams that understand the unique business, technical, and regulatory requirements associated with immunization information systems.

Functional Practices

Supporting the delivery divisions are cross-functional practices that develop and maintain expertise across key disciplines including Product Support, Business Analysis, and Solution

Architecture. These practices establish standards, promote knowledge sharing, support career development, and ensure consistent delivery quality across all projects.

This model allows SSG to maintain specialized expertise while ensuring that each project benefits from proven methodologies, best practices, and experienced personnel.

Shared Services

SSG maintains centralized shared services teams that support all delivery divisions. These include:

- Product Management
- Internal Technology and Security
- Business Development

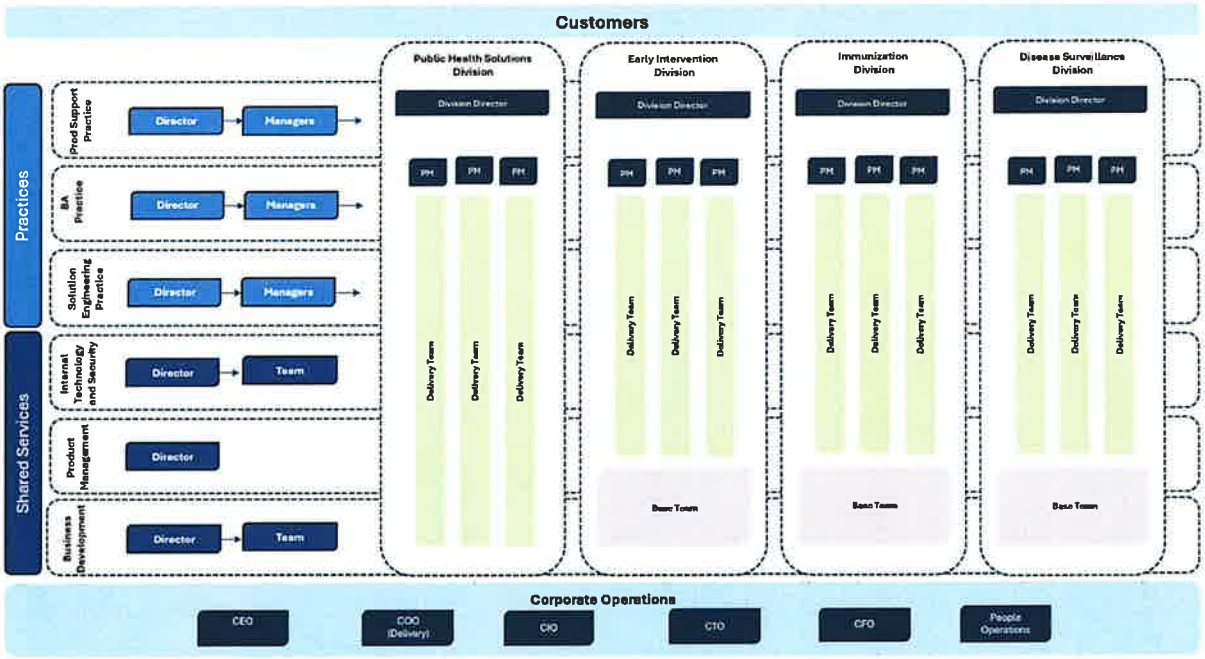
These groups provide enterprise governance, product strategy, cybersecurity oversight, infrastructure support, and organizational leadership across all solution areas.

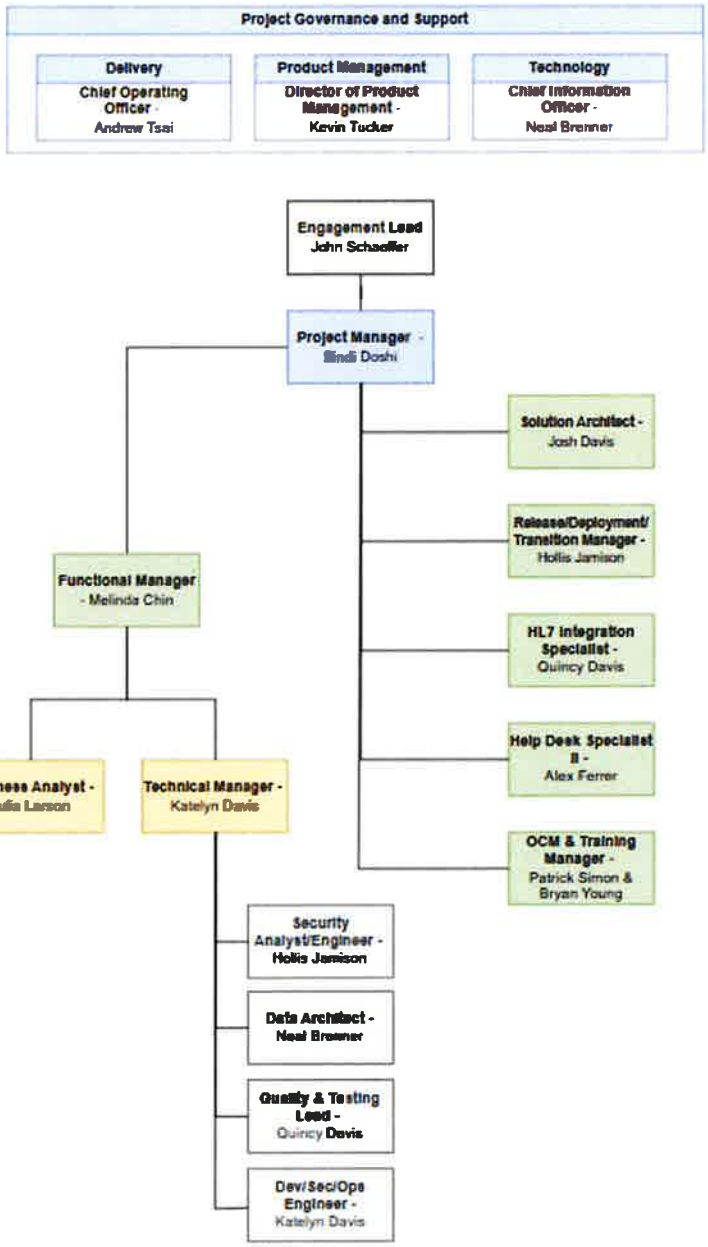
Operational Relationships Supporting the Proposed IIS Solution

For the West Virginia IIS project, the Immunization Division will serve as the primary delivery organization and will be supported by SSG's functional practices and shared services teams. Project management, business analysis, solution architecture, interoperability, data migration, testing, training, security, and operational support resources will work collaboratively throughout implementation and ongoing operations.

Executive leadership, product management, and technology leadership provide project governance and strategic oversight, while the dedicated IIS project team is responsible for day-to-day delivery activities. This structure provides clear accountability, direct access to decision-makers, efficient communication channels, and long-term continuity throughout the lifecycle of the system.

The organizational charts included with this proposal illustrate both SSG's enterprise organizational structure and the proposed project organization for delivery of *Casetivity*-IIS.


Customers
Practices
Prod Support Practice
Director
Managers
BA Practice
Director
Managers
Solution Engineering Practice
Director
Managers
Shared Services
Internal Technology and Security
Director
Team
Product Management
Director
Business Development
Director
Team
Public Health Solutions Division
Division Director
PM
PM
PM
Delivery Team
Delivery Team
Delivery Team
Early Intervention Division
Division Director
PM
PM
PM
Delivery Team
Delivery Team
Delivery Team
Immunization Division
Division Director
PM
PM
PM
Delivery Team
Delivery Team
Delivery Team
Disease Surveillance Division
Division Director
PM
PM
PM
Delivery Team
Delivery Team
Delivery Team
Corporate Operations
CEO
COO (Delivery)
CIO
CTO
CFO
People Operations


Project Governance and Support
Delivery
Chief Operating Officer - Andrew Tsai
Product Management
Director of Product Management - Kevin Tucker
Technology
Chief Information Officer - Neal Brenner
Engagement Lead John Schaeffer
Project Manager - Bindi Doshi
Solution Architect - Josh Davis
Release/Deployment/ Transition Manager - Hollis Jamison
HL7 Integration Specialist - Quincy Davis
Help Desk Specialist II - Alex Ferrer
OCM & Training Manager - Patrick Simon & Bryan Young
Functional Manager - Melinda Chin
Business Analyst - Julie Larson
Technical Manager - Katelyn Davis
Security Analyst/Engineer - Hollis Jamison
Data Architect - Neal Brenner
Quality & Testing Lead - Quincy Davis
Dev/Sec/Ops Engineer - Katelyn Davis

4.3.1.4. 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.

SSG operates from its headquarters and maintains a distributed workforce throughout the United States to support state immunization information system implementations and operations. Help desk staff and technical personnel are physically located throughout the U.S., enabling SSG to provide localized support when desired by clients. All staff members supporting the contract—including help desk personnel, technical teams, and implementation specialists—are full-time SSG employees or employees provided through subcontractor partnerships, and all are based within the United States.

SSG does not operate any overseas locations, and no overseas facilities will be used to support the contract. All data storage, processing, and transmission occur exclusively within data centers physically located in the continental United States. SSG's infrastructure design ensures that no State or Federal data is stored on servers or systems outside U.S. borders at any time, including during disaster recovery, failover, or support operations. This U.S.-based data residency requirement is maintained across all operational activities, including backups, logs, metadata storage, and all phases of system support.

SSG's distributed U.S.-based workforce model supports collaboration across consortium states while maintaining dedicated resources for each client. This structure enables SSG to scale support during surge periods, provide localized assistance when requested, and ensure continuity of operations through geographically distributed teams—all while maintaining strict compliance with federal and state data protection requirements and U.S.-based data residency mandates.

4.3.1.5. 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.

Reference 1

Project: Massachusetts Department of Public Health (MDPH) – Massachusetts Immunization Information System (MIIS)

Contact: Tricia Charles, Immunization Information System Director
Phone: (617) 645-9547
Email: tricia.charles@mass.gov

SSG designed, developed, implemented, and continues to operate and enhance the Massachusetts Immunization Information System (MIIS), the Commonwealth's statewide immunization registry. Originally implemented by SSG in 2006, MIIS has remained in continuous production operation for approximately 19 years and continues to receive ongoing enhancements, maintenance, and operational support from SSG.

MIIS serves as the Commonwealth's centralized immunization registry and supports statewide immunization management, provider participation, vaccine inventory management, interoperability with healthcare organizations, clinical decision support, reporting, and public health analytics.

The primary goals of the project were to provide a comprehensive statewide immunization information system, improve immunization data quality and accessibility, support provider reporting requirements, and enhance public health decision-making. SSG was responsible for the complete system lifecycle, including requirements analysis, system design, application development, implementation, interoperability, ongoing enhancements, maintenance, and operational services. Most recently, SSG implemented a public-facing portal that allows individuals to access and verify immunization records and submit record update requests.

Over the past five years, SSG has delivered multiple major enhancements that have significantly expanded MIIS capabilities beyond routine system operations. Notable recent initiatives include: becoming the first jurisdiction in the nation to implement full outbound integration with the CDC's VTrckS API (Phase 3), enabling real-time exchange of provider, inventory, ordering, returns, and wastage data; implementing a comprehensive Temperature Excursion

management workflow to automate vaccine storage and handling processes; introducing a secure in-system Message Center for direct communication between the jurisdiction and provider organizations; and expanding advanced immunization coverage reporting to provide more flexible, granular population health analysis.

As of the most recent reporting period, MIIS maintains more than 10.8 million unique patient records, supports 5,185 onboarded provider sites with 4,376 live in production — including 804 Vaccines for Children (VFC)-enrolled providers — and has processed more than 123 million immunization records, including nearly 99 million records exchanged through real-time HL7 messaging and more than 235 million bidirectional HL7 query/response (QBP/RSP) transactions. SSG continues to provide hosting, maintenance, modernization, Customer Care (production support), and ongoing enhancements while maintaining uninterrupted statewide operations.

The system has been in continuous production operation under SSG management since 2006, with ongoing modernization and enhancement activity throughout — including significant platform and capability expansion within the past five years.

Reference 2

Project: Wisconsin Department of Health Services – Immunization Registry

Contact: Amy Bittrich, Public Health Systems Section Manager
Phone: (608) 261-6857
Email: Amy.Bittrich@dhs.wisconsin.gov

SSG is currently implementing Wisconsin's next-generation statewide Immunization Information System (IIS) using SSG's existing *Casetivity*-IIS solution. The project does not involve building a new IIS from scratch. Rather, SSG is configuring and implementing the established *Casetivity*-IIS platform to meet Wisconsin's jurisdiction-specific requirements, workflows, business rules, and operational needs. The project's goal is to replace Wisconsin's existing Immunization Registry with a modern IIS that supports the State's statewide immunization program and provides a sustainable platform for future needs.

SSG's responsibilities include business and technical requirements analysis, solution architecture, *Casetivity*-IIS configuration, system integration and interoperability, data conversion planning, testing, project management, training, and implementation planning. The solution supports the core capabilities required of a statewide IIS, including immunization record management, interoperability and data exchange, provider onboarding, vaccine management, reporting, and public health program administration.

The project began in January 2026 following contract signing, with initial implementation and go-live targeted for March 2027. The project is currently in active implementation and therefore

is not yet in production operation. Once implemented, Wisconsin will operate its statewide IIS on SSG's *Casetivity*-IIS solution.

Reference 3

Project: Florida Department of Health – Early Steps Data System

Contact: Maryanne Marchese, Project Manager
Phone: (800) 218-0001
Email: Maryanne.Marchese@flhealth.gov

SSG designed, developed, and implemented Florida's statewide Early Steps Data System using the *Casetivity*-EI platform. The project's goal was to provide Florida with a modern statewide data system supporting its Early Intervention program and federal Part C reporting needs. The implementation supports one of the largest state Early Intervention programs in the country and demonstrates SSG's ability to deliver a complex, statewide public health and human services platform from requirements and design through implementation and ongoing operations.

SSG's responsibilities included business and technical requirements analysis, solution design, application development and configuration, system implementation, testing, project management, and training. The system supports statewide Early Intervention program operations and Part C reporting. Following implementation, SSG continues to provide system maintenance, operational support, and continuous enhancements.

The project began in November 2022, and the Early Steps Data System successfully went live statewide in April 2026, transitioning users and data from the legacy system to the new solution. The system has been in production operation since April 2026 and is now in ongoing support, maintenance, and enhancement.

4.3.2 Mandatory Qualification/Experience Requirements

4.3.2.1. The Vendor must demonstrate organization 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.

SSG has more than 23 years of experience delivering enterprise public health information systems and extensive experience designing, implementing, operating, and enhancing Immunization Information Systems (IIS). As demonstrated by two of the three projects provided as references in Section 4.3.1.5, SSG brings both long-term operational experience with a statewide IIS and current experience implementing a next-generation statewide IIS.

Most notably, SSG designed, developed, implemented, and continues to operate the Massachusetts Immunization Information System (MIIS), the Commonwealth's statewide IIS. Originally implemented by SSG in 2006, MIIS has remained in continuous production operation for approximately 19 years and supports immunization management, provider participation, vaccine inventory management, clinical decision support, interoperability, public access services, reporting, and public health analytics. SSG remains responsible for ongoing enhancements, maintenance, operational support, and modernization of the system, now using *Casetivity*-IIS. This ongoing work demonstrates SSG's IIS experience within the five years preceding this solicitation while also demonstrating the long-term sustainability of an IIS designed and implemented by SSG.

SSG is also currently implementing Wisconsin's next-generation statewide IIS using SSG's existing *Casetivity*-IIS solution. Rather than developing a new IIS from scratch, SSG is configuring and implementing the established *Casetivity*-IIS platform to meet Wisconsin's jurisdiction-specific requirements, workflows, business rules, and operational needs. The engagement includes business and technical requirements analysis, solution architecture, configuration, system integration and interoperability, data conversion planning, testing, project management, training, and implementation planning. This current project demonstrates SSG's recent, directly relevant experience implementing a modern statewide IIS and supporting complex immunization workflows, interoperability, provider onboarding, vaccine management, reporting, and public health program administration.

Collaboration is central to SSG's approach. We have worked with federal agencies, national organizations, state governments, and data exchange networks to ensure our solutions are interoperable and standards compliant. The following lists just some of the organizations that we have collaborated with or performed project work for:

- CDC: Collaboration on IIS Functional Standards, case definitions, and disease surveillance reporting.
- AIRA: Active Platinum Corporate Partner; MIIS achieved validation in all five content areas.
- AIM: Active Gold Corporate Alliance Member
- Data Exchange Networks: Implementations with IZ Gateway, VTrckS, vital records systems, EHR vendors, and health information exchanges (e.g., Mass HIway).
- Local and State Partners: Extensive work onboarding providers, schools, and local health departments, including training and user support.

This history demonstrates SSG's ability to coordinate effectively across jurisdictions, national standards bodies, and third-party systems to deliver interoperable solutions.

SSG currently operates multiple production instances of the *Casetivity* platform across several states, serving millions of records and thousands of users. Each customer environment is independently deployed and managed using dedicated infrastructure and data partitioning. SSG has more than a decade of experience providing secure, fully managed Software as a Service (SaaS) solutions for public health agencies.

Across its portfolio, SSG has successfully delivered more than 100 public sector technology projects and maintains a 100 percent implementation success rate. Every project undertaken by SSG has successfully achieved production and continues to support operational public health programs. In addition to IIS implementations, SSG has designed, implemented, and supported large-scale public health systems including disease surveillance systems, health information exchanges, vital records systems, clinical decision support systems, electronic laboratory reporting systems, and other mission-critical public health applications.

SSG's solutions are designed to support applicable federal and state requirements, industry interoperability standards, accessibility requirements, security controls, and public health reporting obligations. Through its successful implementation and long-term operation of

statewide IIS and other enterprise public health platforms, SSG has demonstrated the organizational experience, technical expertise, and operational maturity required to meet the goals and requirements of this RFP.

SSG

1329 Highland Avenue | Needham, MA 02492

www.ssg-llc.com