APPENDIX A. ADDITIONAL INFORMATION

In this section, CNSI is providing other pertinent information that is supporting or supplementary data which would substantiate our experience, expertise, and capability to provide the required services, as well as the capability of our proposed solution. This information includes tables, screenshots, architectural diagrams and other graphics, and supporting text.

A.6.1 Overall Requirements [SOW, Section 5.1]

The evoBrix PMIS supports the processes identified in the MITA's Provider Management business process area that will position AHCCCS to meet its objectives, including:

- Online web capabilities for all users including providers. The solution offers the unique Provider portal that allows providers to access many services 24 hours a day, 7 days a week (24x7x365). The portal enables providers to enter new enrollment applications and maintain their provider data.
- User-friendly, rules-based structure to support provider enrollment and reenrollment policies.
- Excellent audit trail features identifying who initiated the change, what changed, when the change was requested, who approved or denied the change, and when was it was approved or denied.
- Outstanding filtering and inquiry capabilities allowing authorized users to search for and retrieve provider information based on user-supplied search criteria.
- Compliance with and use of the National Provider Identifier (NPI) for provider enrollment and automatic assignment of atypical provider IDs for providers who are not eligible for NPIs.
- Fully service-oriented platform with a seamless integration of industry leading COTS products for letter generation, content management, reporting, and enterprise service bus to support the file exchange process.

Overall, evoBrix PMIS module benefits AHCCCS by modernizing and streamlining the many paper and manual processes used in the legacy environment while substantially increasing the ability to respond to provider requests and improve customer service. Figure A.6.1-1 shows the overall evoBrix PMIS business architecture. This figure depicts a summary of the functions available to providers and business operations staff, as well as the various enrollment types supported in the solution. This figure also shows the integration with external systems, evoBrix application security, and COTS products. The evoBrix PMIS module interacts with external systems through an automated communication channel using real-time web-services and file exchange process.

This page intentionally left blank.

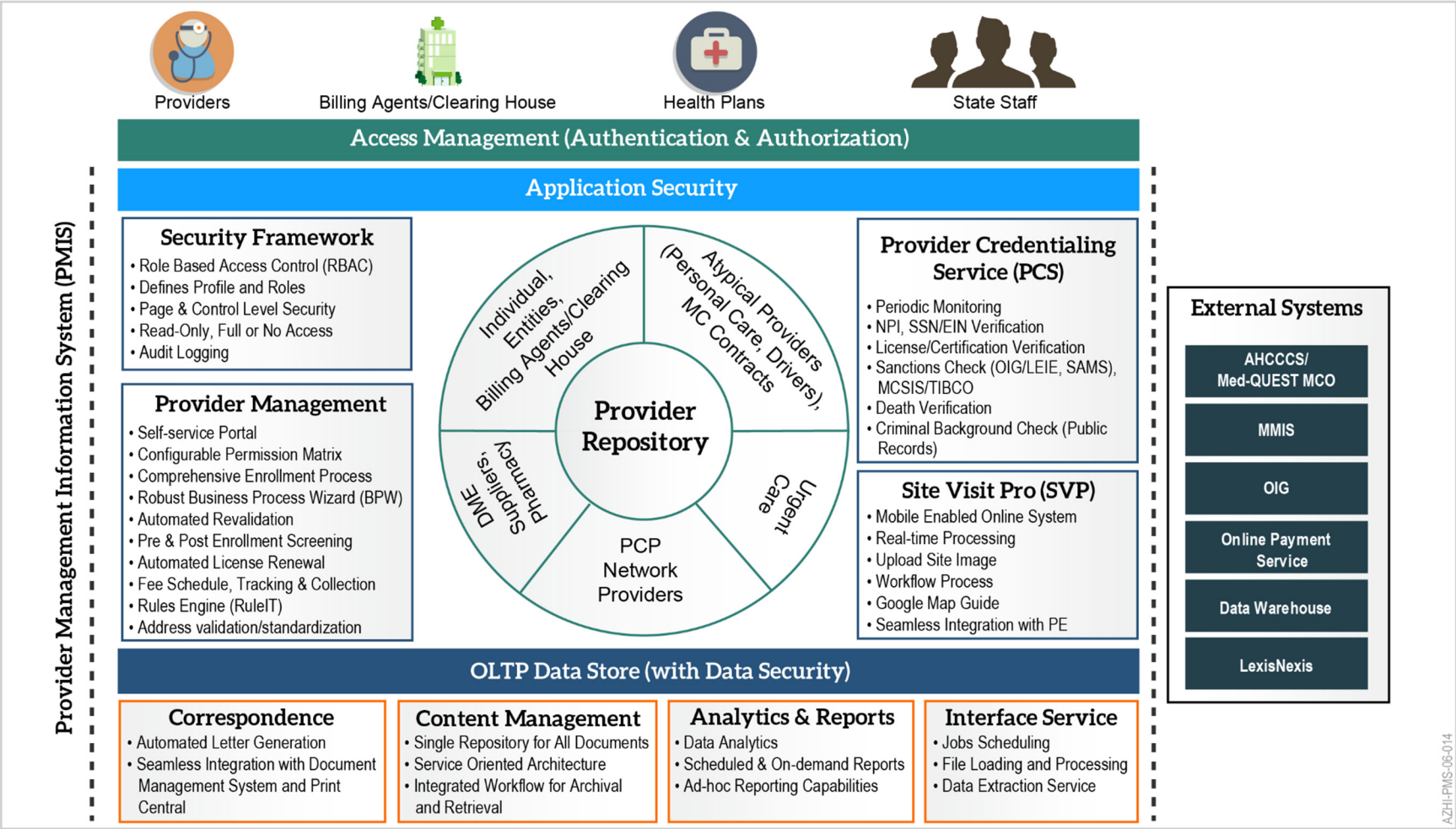


Figure A.6.1-1. evoBrix PMIS Business Architecture. This figure depicts a summary of the functions available to providers and business operations staff, as well as the various enrollment types supported in the solution.

This page intentionally left blank.

evoBrix PMIS has built-in functionality to allow new user registrations for both providers and State-authorized users, a workflow feature to route new user registrations to authorized State staff for their review, a feature to enforce a password reset policy, functionality to actively monitor user accounts for prolonged period of inactivity for automated locking of those accounts, and functionality to maintain demographic information of all users. The evoBrix PMIS solution also provides functionality that allows State staff to request for security profiles based on their job duties.

evoBrix PMIS offers a configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data. Authenticated access and role-based access control (RBAC) enforces security in the evoBrix PMIS module. The security framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy. The Security Framework supports role-based security and limits access to users by domain and user ID. evoBrix maintains three independent, secure access methods for the provider enrollment business area. The method of access depends on the status and type of user. The first type is a provider who has no previous relationship with AHCCCS and is applying for the first time. The second type of user is a provider who has a prior active relationship with the AHCCCS and who wants to initiate a new enrollment. The third type of user is a business operations worker. Business operations workers may have responsibility for processing enrollment applications submitted online, reviewing submitted applications and rendering an approval or denial decision, or providing support to enrolling providers.

The provider enrollment process is supported by a Business Process Wizard (BPW) that guides the provider through the process. Business rules are housed in the decision management framework called RuleIT which governs the sequence of the enrollment steps and the content collected. The business rules prevent submission of the enrollment application until the information content and validity has reached the AHCCCS-acceptable level. The system communicates the process deficiencies and missing information in online screens in real time before allowing the provider to move to the next step in the enrollment process.

The evoBrix PMIS solution supports both new enrollments and enrollment modifications. The new enrollment application, once submitted by the provider, will be reviewed and approved by the provider enrollment unit. The solution also provides the ability for providers to perform updates to the enrollment information using the web portal, which will be forwarded to the provider unit for review and approval. The BPW uses AHCCCS-specific rules configured using the RuleIT rules engine to designate steps as required or optional, dynamically depending on data entered by the provider for a given enrollment type. The wizard validation rules are based on the enrollment type and include validation of data, such as NPI. For additional detail on RuleIT, please refer 6.4 Other System Requirements under 6.4.3 Separate Business Rules Engine. The evoBrix PMIS solution highlights are listed below into features and benefits:

Key Features:

- Configure enrollment process workflow per state-defined criteria
- Perform enrollment process electronically
- Define industry standard provider types, specialties and sub specialties; associate standard and non-standard taxonomies through a comprehensive Permission Matrix
- View/Upload attachments for uploading the supporting documentation such as copy of license, copy of any certifications with the enrollment application
- Track fingerprinting based on the provider risk category
- Support submission and processing of provider appeals and grievances including service requests tracking
- Collect enrollment fee for the institutional providers via online payment service
- Accept electronic forms, supporting documents/attachments

Figure A.6.1-2 shows provider enrollment statistics of CNSI's previous implementations of the Provider Enrollment system.

	Michigan	Illinois	Washington	Utah
Enrolled Provider Volume	170,000	250,000	198,000	25,000

Figure A.6.1-2. Enrolled Provider Volume in CNSI's Previous Implementations. We have provider volume ranging from 25,000 to 250,000 across the four states we have worked with.

Provider Credentialing Service (PCS). CNSI's PCS platform, in partnership with LexisNexis, will integrate with the AHCCCS/Med-QUEST-approved credentialing solution to provide full compliance with the ACA Provider Enrollment Screening requirements. The PCS solution is comprised of pre- and post-enrollment screening processes that integrate the system with a real-time credentialing service. This one-stop solution provides improved automation and reduced manual intervention. Pre-enrollment screening results are available in real time within PCS web pages for the provider enrollment specialist to review and make appropriate decisions regarding whether to approve or deny the enrollment application.

The solution is flexible for the provider enrollment specialist to perform the screening process on an on-demand basis using online PCS web pages anytime during enrollment application or modification review. The solution performs periodic screening of providers using LexisNexis credentialing service and AHCCCS-approved screening solution and applies the business rules defined by the State Medicaid program. The PCS solution provides ability to track screening results to meet audit requirements for the following screening criteria:

- State/Federal Death Verification
- General Services Administration (GSA) Exclusion list (EPLS/SAM)
- License Board Sanctions
- NPI Verification
- SSN, EIN/TIN Verification
- National Council for Prescription Drug Programs (NCPDP) Verification
- License/Certification Verification
- DEA, CLIA, Board Certification Verification with American Board of Medical Specialties
- Criminal History and Sex Offense check

Figure A.6.1-3 shows the various components in the PCS architecture, including real-time and batch services integration.

CNSI's PCS has a web Interface that provides a user-friendly GUI for viewing screening results in a tabular layout. Any screening that requires attention is flagged for users so they can check for more details before deciding.

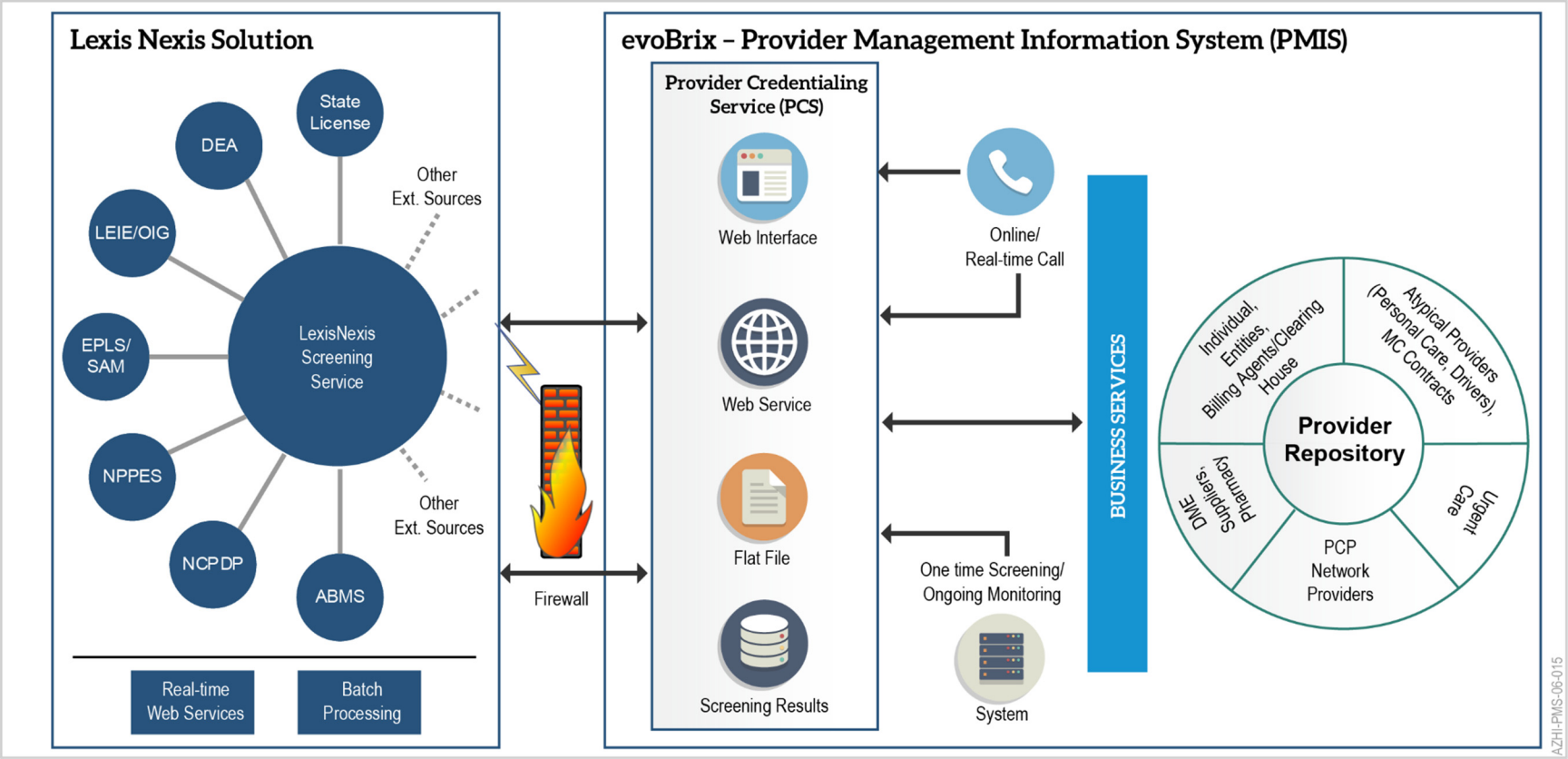


Figure A.6.1-3. Provider Credentialing Service Solution Overview. evoBrix PMIS integrates with LexisNexis.

This page intentionally left blank.

SiteVisitPro (SVP). CNSI's SiteVisitPro (SVP) solution is a portable application which the business operations staff can take with them directly to provider sites to perform unannounced site visits. The application is mobile-enabled for tablets, eliminating the need for paper forms. It supports organizations in performing site visits using real-time provider information directly from the Medicaid Provider Enrollment system, eliminating redundant data entry. SVP assists in the identification of fraudulent providers by capturing specific information about the provider's practice. SVP can be accessed from anywhere with a wireless connection. This application:

- Streamlines site visit processing using a real-time system, eliminating paper
- Eliminates periods of no activity on the site visits through alerts to the appropriate business operations staff
- Decreases the time it takes to approve or reject a provider's application for enrollment
- Eliminates redundant data entry and manual updates to the Medicaid Provider Enrollment system

The SVP common features as follows:

- Allows an administrator to balance workloads by assigning site visits to the business operations staff
- Provides scheduling capabilities and allows the business operations staff to see the scheduled site visits in a calendar
- Displays a map and provides directions to site visit locations
- Retrieves and displays provider demographic details in real time from the Medicaid Provider Enrollment system
- Captures specific information that is relevant to the provider's specialty
- Stores location images captured during the site visit
- Tracks the status of the site visit from scheduling to completion and maintains history
- Alerts the business operations staff when specific actions need to be taken
- Sends systematic notification of the site visit results to the Medicaid Provider Enrollment system

Figure A.6.1-4 shows the various components in the SVP architecture, including the integration of the Provider Enrollment system.

This page intentionally left blank.

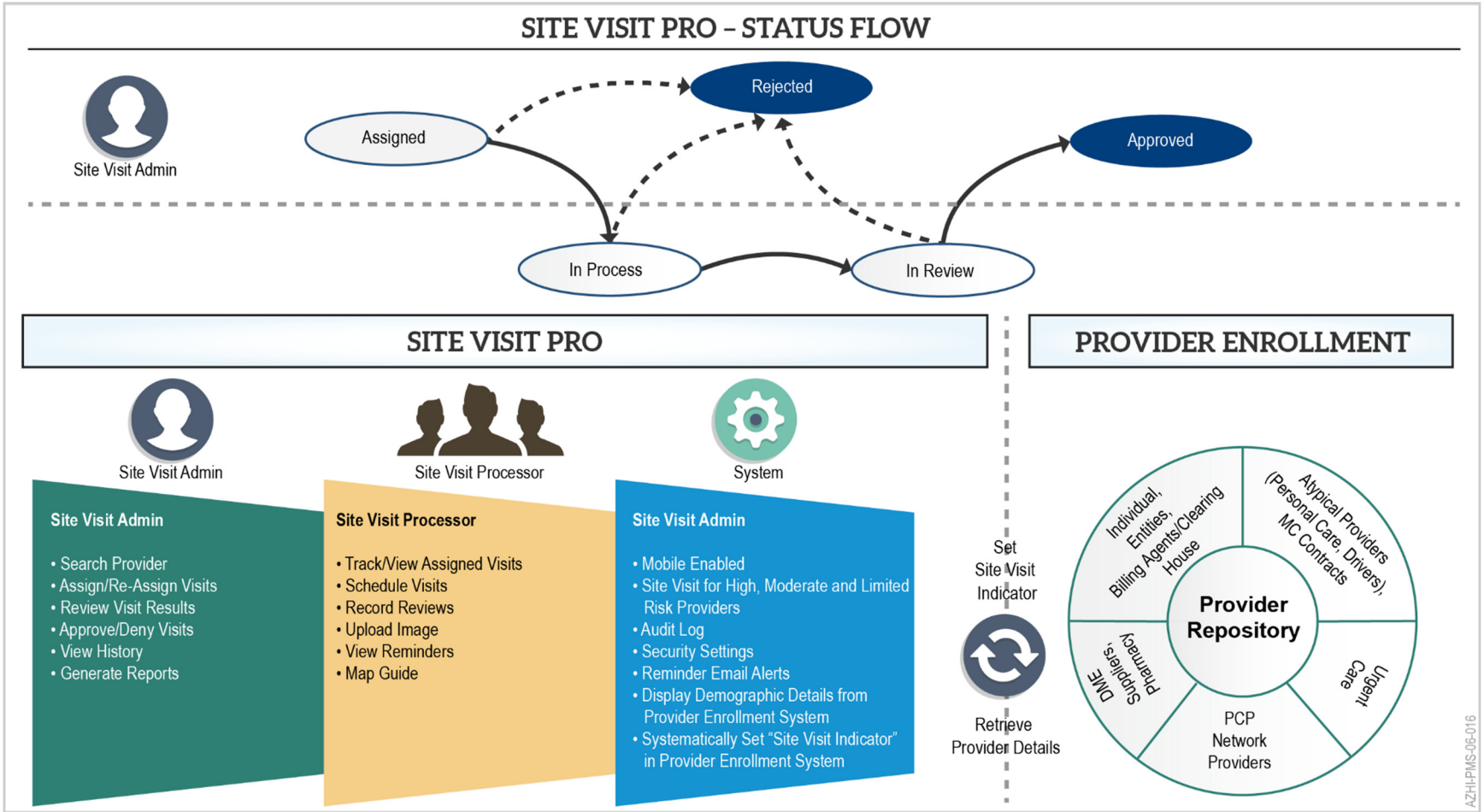


Figure A.6.1-4. Site Visit Pro. This diagram illustrates the overall SVP architecture and real-time integration with Provider Enrollment system.

This page intentionally left blank.

A.6.1.1 COTS Solution [SOW, Section 5.1.1]

Figure A.6.1-5 describes the different components of configuration and customization of evoBrix solution.

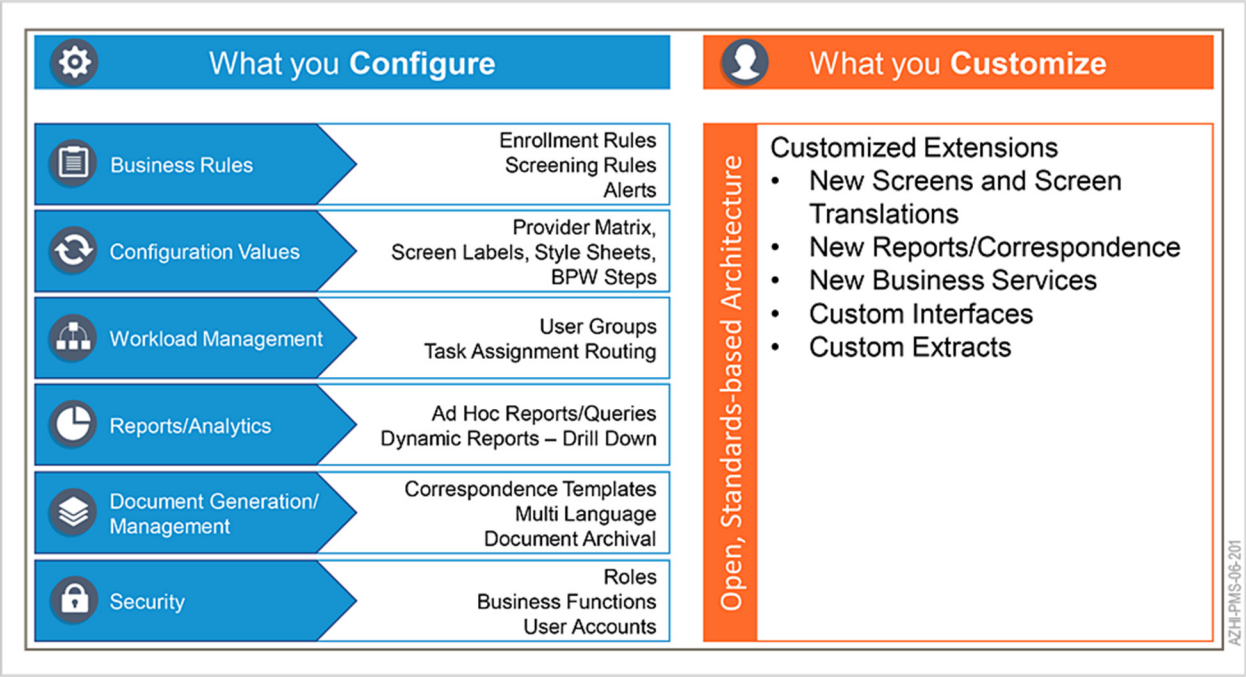


Figure A.6.1-5. evoBrix Configuration Vs Customization. Shows different components of configuration and customization of evoBrix solution.

A.6.1.2 Receipt of Provider Applications [SOW, Section 5.1.2]

The evoBrix PMIS collects the provider's demographic information in the Basic Information screen which is the first step of the enrollment process wizard, as shown in Figure A.6.1-6. After the provider basic information is successfully saved, evoBrix PMIS generates a unique application number, as shown in Figure A.6.1-6, and sends an email notification to the provider. The providers use the number as reference which allows them to track, resume and submit the enrollment application through self-service portal.

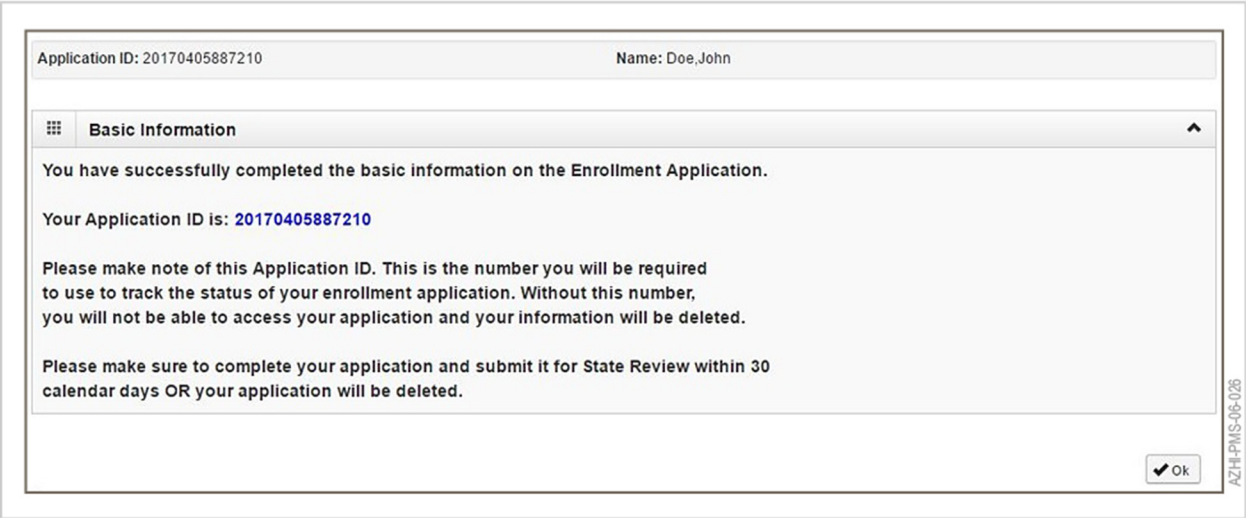


Figure A.6.1-6. Application ID generation. After basic information is successfully completed system generates an Application ID for tracking of the application by providers.

Provider Revalidation. The evoBrix PMIS solution offers a streamlined, configurable process for automated provider revalidation according to State requirements. evoBrix PMIS sends automated revalidation notices based configurable business rules to begin the revalidation process for each provider. The providers will have at least 30 days (configurable option) from the date of their revalidation letter to complete the revalidation process. The providers are required to revalidate all the steps in the enrollment by completing each step that are listed in the BPW screen.

The evoBrix PMIS also sends automated revalidation reminder notices for each provider 90 days and 30 days prior to the due date. evoBrix PMIS terminates enrollments automatically and sends termination notices for the providers who do not complete revalidation within 30 days. The 30-day revalidation period, 90-day and 30-day reminder notice periods are configurable based on State's policy. evoBrix PMIS provides ability to configure a five-year revalidation interval by Risk Category (High, Moderate, and Low) or by Provider Type/Specialty.

As part of the revalidation process, evoBrix PMIS solution automatically dis-enrolls/end-dates the provider eligibility upon failure to revalidate, or renew any mandatory Certifications or Licenses which are required to meet Federal and State Policies and Regulations. evoBrix PMIS sends termination notice to providers upon termination of the provider eligibility. The termination process can be configured based on State-approved processes and procedures.

A.6.1.3 Collecting and Maintaining Provider Data [SOW, Section 5.1.3]

Figure A.6.1-7 shows some of the evoBrix PMIS datasets that support other module functions.

Type of Provider Data	Intended Use for Supporting Other Module Functions in the AHCCCS/Med-QUEST Medicaid enterprise
Provider Edits - ■ Eligibility ■ Taxonomy ■ Provider Type / Specialty	Service Authorization and Claims/Encounter processing business functions
Provider Flags / Indicators ■ Stop Payment Flag ■ Valid EIN / TIN Flag ■ Valid SSN Flag ■ Valid NPI Flag ■ W9 Indicator ■ Warrant Suppress Indicator	Payment processing business functions
Provider datasets ■ Enrollment details ■ Demographic details ■ Specialty / Sub-specialty details ■ License / Certification details ■ Revalidation details	Dashboard and Reporting functions

Figure A.6.1-7. Provider data to support other module functions. The evoBrix PMIS solution collects and maintains provider data to support an array of module functions such as claims/encounters processing, service authorizations, and dashboard/reporting functions.

A.6.1.4 Backup, Recovery, and Refresh Functionality [SOW, Section 5.1.5]

CNSI's backup and recovery approach is based on using the following tools:

- Oracle Database Backup Service: All the systems are backed up using Oracle's Database Backup Service and Oracle Cloud Infrastructure Object Storage and Archive Storage Service. All data running

in the environment is backed up in its native format. This cloud service automatically replicates data objects across multiple fault domains for high durability and it is actively monitored for data integrity and availability. All data stored in the object and archive storage is encrypted at rest, by default, using the AES 256 encryption algorithm.

- Oracle Cloud Infrastructure Object Storage– Storage for both structured and unstructured data including backups supported by enterprise-class data protection, resilience, and elastic scalability.
- Oracle Cloud Infrastructure Archive Storage– Storage for infrequently accessed data with enterprise-grade security, resilience, and elastic scalability

- Oracle Recovery Manager (RMAN): This tool is used to configure and backup the Oracle databases to local and offsite locations. RMAN Backup includes Oracle RMAN Compression and Encryption features to ensure that backups, which are stored in offsite locations, are also secured.

A.6.1.5 User Prompts and Guidance [SOW, Section 5.1.6]

Figure A.6.1-8 shows the Upload Document step that gives the ability for the provider to upload documents as part of the enrollment BPW process wizard.

Figure A.6.1-8. Upload Document. This gives the ability for the provider to upload documents as part of the enrollment BPW process wizard.

A.6.1.6 Cloud-based Technology [SOW, Section 5.1.9]

There are two ways by which expansion happens in CNSI's private cloud:

Horizontal Expansion – Cloud Services. CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type to be added or removed quickly. This flexibility is because all infrastructure components are either built using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or SaaS services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in CNSI's private cloud can be subscribed to or cancelled, on an ad hoc basis, using the "Pay as you go" subscription model. Oracle Compute Cloud Service forms the backbone of the IaaS layer within our solution. The virtual machine instances that are deployed by the Oracle Compute Cloud service provides the necessary low-latency, highly-available and fault-tolerant infrastructure required to run the application software components. Both IaaS and PaaS services leverage the same cloud-optimized hardware, firmware, software stack, and networking infrastructure to deliver unrivaled performance and strong isolation. For example, if AHCCCS has a requirement to install and configure a security or compliance tool for a short period of time:

- CNSI creates a new VM with a specific number of cores using the IaaS Service – "Oracle Compute Classic Cloud Service"
- Allocates the necessary SAN space for the VM, that was created earlier, using the Oracle Cloud Block Storage IaaS Service
- The VM is then backed up regularly using Oracle Cloud Backup Service and the backups are stored using Oracle Cloud's Object Storage Service

- All the above services are billed using “Pay as you go” subscription model on an hourly basis
- Once the security or compliance task is over, the above services are then cancelled.

Vertical Expansion – Cloud Bursting. CNSI’s hosting platform also supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes. Any additional capacity used is charged on an hourly basis and billed monthly in arrears (“Pay as You Go” model).

For example, if the current database server has four cores allocated and you are running a monthly job that requires additional computing power, then the cloud bursting feature will add additional cores to the database server, to meet the additional demand. This additional capacity used is charged on an hourly basis and billed monthly in arrears (“Pay as You Go” model).

A.6.1.7 Virtualized Environment for Hosting and Executing [SOW, Section 5.1.10]

CNSI's proposed cloud-based solution is hosted in the Oracle Government Cloud. It includes hardware and software components built using either Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or Software as a Service (SaaS) Cloud services and these can be re-hosted upon request.

- Oracle PaaS and SaaS services are designed to manage the Database layer, Service Oriented architecture (SOA) and Enterprise Service Bus (ESB) Integration Layer, Application Servers, Storage and Network. It includes the highest level of automation and powerful template capabilities are available to enable infrastructure as code and DevOps processes
- Oracle IaaS services are designed to manage Application virtual machines. It leverages the best-in-class Oracle virtualization technologies to logically partition physical servers, leading to a lower total cost of ownership. It also supports microservices and cloud-native application deployment with Docker and Containers

Since these cloud services are subscribed on a monthly basis, any transition to a AHCCCS/Med-Quest data center can be easily handled, once these subscriptions are cancelled at the end of their contract period.

- The databases can be exported using the standard backup tools such as Oracle Data Pump and Oracle Recovery Manager (RMAN)
- The application code can be redeployed in the Application server setup at the AHCCCS/Med-Quest data center.
- All other COTS products can be reinstalled in AHCCCS/Med-Quest data center and then data can be migrated using the standards backup tools.

A.6.1.8 Prompts for Provider Participation Agreement Affirmation [SOW, Section 5.1.11]

As part of the enrollment process, the provider is prompted to accept the terms and conditions of the Provider Participation Agreement, and then submit the enrollment. as shown in Figure A.6.1-9, after which a confirmation message is displayed, as shown in Figure A.6.1-10.

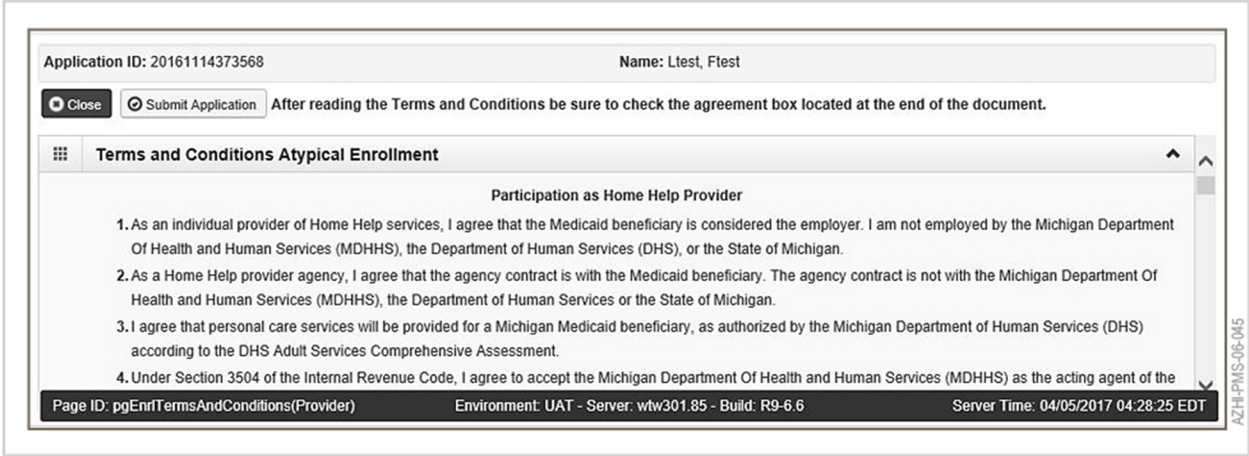


Figure A.6.1-9. Terms and Conditions. The provider will need to accept the terms and conditions and click on Submit Application to finish the enrollment.

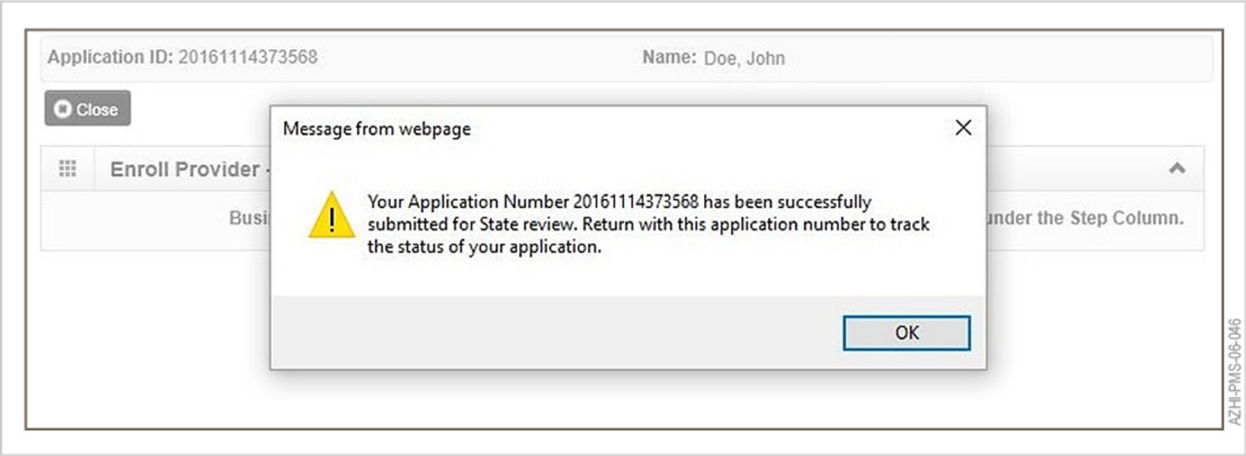


Figure A.6.1-10. Enrollment Submission Confirmation. Once the enrollment submission is completed the system displays confirmation message.

A.6.1.9 Detailed Descriptions of Virtualized Environments [SOW, Section 5.1.12]

The classification of Infrastructure components and their equivalent Cloud Services are specified in Figure A.6.1-11.

Infrastructure Components	Cloud Service Type	Cloud Service
Database	PaaS	Oracle Database Cloud Service (DBCS)
Virtual Machines (VM)	IaaS	Oracle Compute Classic Cloud Service
Application Server	PaaS	Oracle Java Cloud Service (JCS)
Integration Platform	PaaS	Oracle Service Oriented Architecture Cloud Service (SOA CS)
Storage	PaaS	Oracle Cloud Block Storage
Backup Storage	PaaS	Oracle Cloud Object Storage
Backup Service	PaaS	Oracle Cloud Backup Service

Infrastructure Components	Cloud Service Type	Cloud Service
Provider Screening	SaaS	Lexis Nexis Screening
Provider Fee Collection	SaaS	First Data Fee Collection Service
Identity Management	PaaS	Oracle Identity Cloud Service
Security Suite	PaaS	Oracle Management Cloud

Figure A.6.1-11. Infrastructure components and its equivalent Cloud Services. This classification maps how each infrastructure component is subscribed as IaaS, PaaS, or SaaS services.

An overview of the various PaaS, IaaS, encryption and security services that form the building blocks of CNSI's evoBrix PMIS solution is illustrated in Figure A.6.1-12. Using this infrastructure framework, AHCCCS/Med-QUEST can create the virtualized environments necessary to house and operate the system in a selected Data Center.

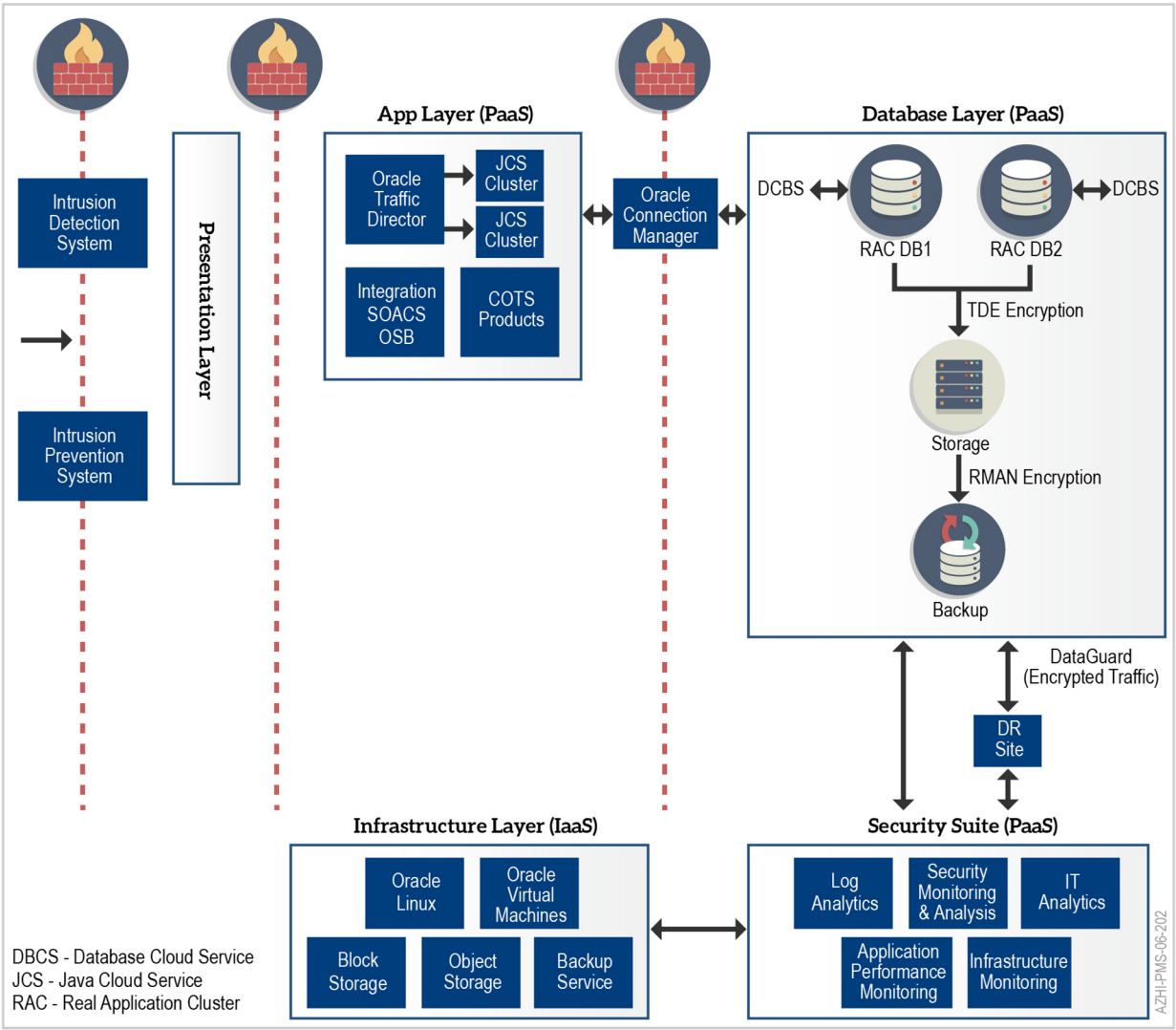


Figure A.6.1-12. Hosting Platform Overview. Oracle Cloud's hosting platform, types of IaaS, PaaS, security and encryption services reflect the secure platform CNSI offers the State.

A.6.1.10 Meeting Software and Hardware Requirements [SOW, Section 5.1.13]

Hosted in the cloud, all infrastructure components are built using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or SaaS services, thereby creating a highly flexible and elastic environment. This elasticity and scalability allow for both short-term capacity spikes as well as long-term growth as needs evolve, as shown below.

- Vertical Scalability –CNSI's hosting platform supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes.
- Horizontal Scalability –CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type, to be added or removed quickly. This flexibility is because all infrastructure components are build using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or SaaS services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in Team CNSI's private cloud can be subscribed or cancelled to, on an ad-hoc basis, using the "Pay as you go" subscription model.

Since the evoBrix solution is based on COTS products, we use versions of software that are currently supported under standards maintenance agreements and generally available during the life of the contract.

- Upgradeability: All infrastructure components (hardware and software) are built using either Traditional perpetual based licensing or they are subscribed as Cloud Services. These licenses are maintained throughout the period of the contract. Since these infrastructure components are fully licensed along with maintenance support, we will receive new version upgrades and patches from the respective vendors, whenever they are available.
- Scalability: CNSI's PMIS solution provides application-level as well as infrastructure-level scalability capabilities to support business growth. CNSI's hosting platform is elastic and scalable to allow for both short-term capacity spikes as well as long-term growth as needs evolve whose key capabilities include:
    - Vertical Scalability –CNSI's hosting platform supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes.
    - Horizontal Scalability –CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type, to be added or removed quickly. This flexibility is because all infrastructure components are build using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or SaaS services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in Team CNSI's private cloud can be subscribed or cancelled to, on an ad-hoc basis, using the "Pay as you go" subscription model.
    - Provisioning –CNSI's hosting platform are in highly available and scalable configurations that can be rapidly provisioned and ready for use in minutes.

Supported Software versions: CNSI will receive new version upgrades and patches from the respective vendors, whenever they are available. These patches and upgrades are applied during the approved maintenance windows, thus making sure that we always run the supported and compatible version of software during the life of the contract.

A.6.1.11 Web-based Solution [SOW, Section 5.1.14]

CNSI's evoBrix web portal, comprised of the state and operations user portal that can be used by internal staff and a provider portal used by provider communities, is developed with W3C web-based standards. The rich user interface is designed to work on the most commonly-used internet browsers, as shown in Figure A.6.1-13. Web portals are designed with a UI framework that has different tiers for business logic and content representation. It also has a responsive UI to show different layouts on various device sizes (e.g., tablets and smart phones). This makes the portals more scalable and robust. The user interface complies with usability standards such as Section 508 subpart B Section 1194.21 - an amendment to the United States Workforce Rehabilitation Act.

Browser Name	Version	Platform	HTML Only Web Client	Notes
Apple Safari	9+ up to 10	Mac OS X	Yes	New browser version upgrades will be tested for compatibility and released for end user utilization
Firefox	20+ up to 51.0	Mac OS X Windows	Yes	New browser version upgrades will be tested for compatibility and released for end user utilization
Google Chrome	26+ up to 56.0	Mac OS X Windows	Yes	New browser version upgrades will be tested for compatibility and released for end user utilization
Microsoft Edge	25.0	Windows	Yes	New browser version upgrades will be tested for compatibility and released for end user utilization
Microsoft Internet Explorer	9+ up to 11.839	Windows	Yes	New browser version upgrades will be tested for compatibility and released for end user utilization

Figure A.6.1-13. evoBrix Browser Support. evoBrix is a web centric solution and supports various standard browsers.

The Cognos reports portal is accessed through a standard set of browsers, as shown in Figure A.6.1-14.

Browser Name	Version	Platform	HTML Only Web Client	Compatibility Mode*	Notes
Firefox	45 up to 51.0	Windows	Yes	N/A	New browser version upgrades will be tested for compatibility and released for end user utilization **Specific Limitations**: 1. Add to bookmarks function not available for Reports
Google Chrome	41 up to 56.0	Windows	Yes	N/A	New browser version upgrades will be tested for compatibility and released for end user utilization **Specific Limitations**: 1. Add to bookmarks function not available 2. Launching of Query Studio, Analysis Studio, Report Studio, Event Studio, Drill-through definitions are not available
Microsoft Internet Explorer	10+ up to 11.839	Windows	Yes	ON (host domain should be added to compatibility settings)	New browser version upgrades will be tested for compatibility and released for end user utilization

** **Compatibility Mode** feature of the web browser which is applicable only for Microsoft Internet Explorer (IE) in version 8 and later. When ON/active, Compatibility View forces IE to display the webpage in Quirks mode as if the page were being viewed in earlier versions.*

Figure A.6.1-14. Cognos Reports Browser Support. Cognos Reports portal is a web centric solution and supports various standard browsers.

A.6.1.12 System Architecture Document [SOW, Section 5.1.15]

CNSI proposes evoBrix, a Modular Medicaid Platform, to serve as the Provider Management System solution. CNSI's evoBrix is fully backed by its solid track record of enabling the states of Michigan and Illinois to successfully run provider management functions in a multi-vendor implementation environment. evoBrix leverages a comprehensive set of previously certified components and federally compliant functional modules. As an early adopter of CMS' modularity vision, CNSI's evoBrix is cloud- and SOA-enabled, positioning it as the most advanced Medicaid platform in the market.

Key highlights of the evoBrix modular and MITA-aligned platform include:

- Functionally rich evoBrix PMIS which is based on the CMS-certified modules in the state of Michigan and Washington
- Modular and extensible technical architecture that utilizes configuration capabilities, including a rules engine, to enable Provider Management System (PSM) to quickly and cost-effectively adapt to the changing environment of Medicaid
- As a MITA-aligned solution, evoBrix will enable PSM to demonstrate overall alignment to the CMS technology vision and adherence to CMS standards and guidance, thereby fully realizing the business benefits resulting from such compliance
- Individual solution components are Service Oriented Architecture (SOA)-based and loosely coupled to each other, enabling a high level of reuse and interoperability within the system
- As a fully scalable and automated solution, intrinsically designed for high availability, evoBrix offers a low-risk solution, maximizes business and system performance, and reduces the complexity and cost of operations and maintenance while providing the ability to scale up to business growth
- Flexibility to modify business rules to support business and policy changes with minimal involvement of developers, greatly improving time-to-market of business requirements

CNSI understands AHCCCS desire to have a functionally rich business solution supported by a highly flexible and scalable technical architecture. As a MITA-aligned solution, evoBrix will assist PSM as a solution that enables the state to receive favorable treatment for Federal matching funds for implementation and ongoing maintenance. The modular architecture will provide the state with flexible procurement options to leverage the best fit solution.

Technical Architecture View of the Proposed Solution. CNSI's proposed solution, was engineered from the ground up based on service-oriented architecture principles, wherein business and functions are available as services across various architecture layers, promoting reuse and interoperability in an enterprise integration environment. As shown in Figure A.6.1-15, the evoBrix technical architecture view depicts a layered architecture comprising accessibility services; integration services; technical, configuration, and monitoring services; data and reporting services; and COTS services which operate in a highly secure and interoperable technical environment.

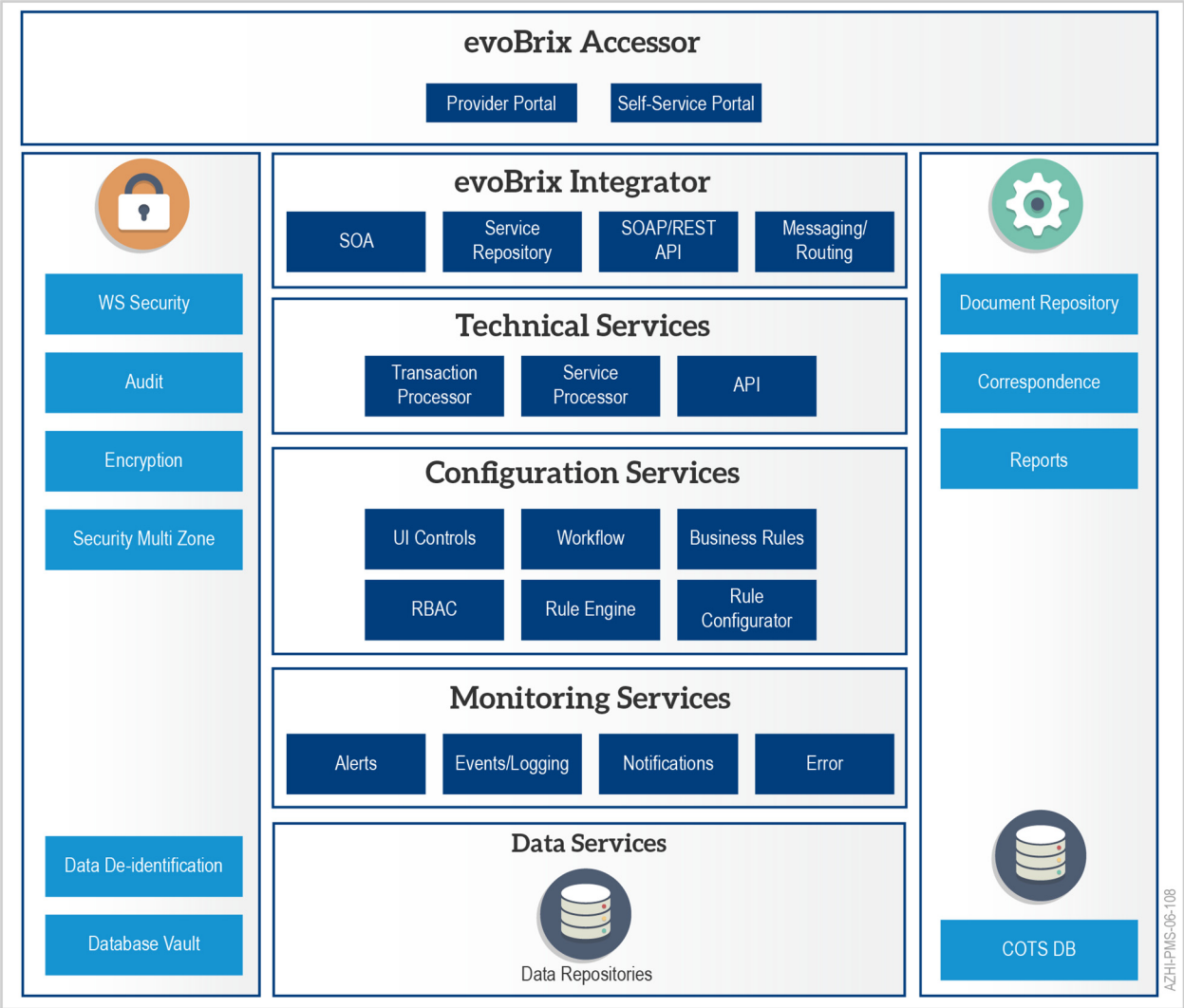


Figure A.6.1-15. High-level Technical Architecture of evoBrix. This shows the alignment of architecture layers with the MITA technical architecture.

The technical architecture capabilities of the proposed solution will allow for interoperability between the evoBrix solution and the other modules in the AHCCCS enterprise environment. The technical architecture and design of the solution adopts service-oriented principles for modularity and interoperability, and the core technology components are distributed across various architecture layers as depicted in the following exhibit. Service orientation, interoperability, reuse, and extendibility are foundational to the proposed technical architecture as can be evident from the constructs of the architecture layers. The key service layers and their role as part of the technical architecture are shown in Figure A.6.1-16.

Services	Service Description
Accessibility Services	■ Includes services that enable user access to various users of the solution via web portals and mobile devices ■ Responsive UI technology for multi-device, multi-browser support ■ Compliant to web and ADA standards ■ Multi-channel support including web, mobile, Computer Telephony Interface (CTI)
Integration Services	Set of Integration services, Integration gateway, and SOA mediator for enabling service oriented

Services	Service Description
	integration between PMIS and other systems in the AHCCCS Enterprise environment through the system integrator.
Technical Services	Set of services leveraged across the evoBrix modules that ensure standardization and reuse of key technology functions in the areas of configuration services, processing services, technical COTS services, and monitoring services.
Security Services	Includes a core security framework responsible for application security, including authentication, authorization based on RBAC, application data security, audits, and other security controls.
Data Services	Enterprise data repository services that facilitate secure storage and efficient retrieval of enterprise data. Includes highly secure data security components and services.
Reporting & Analytics Services	Includes reporting services and advanced analytics services which can be leveraged across the system.

Figure A.6.1-16. evoBrix Service Layers. evoBrix service layers encapsulate a modular and integrated solution stack.

A.6.1.13 Master Data [SOW, Section 5.1.6]

The evoBrix PMIS solution's Logical data model is a detailed pictorial representation of various functional requirements independent of database management systems. It provides an in-depth overview of various entities and attributes. The model is a culmination of the best practices based out of MMIS implementations across multiple States. Figure A.6.1-17 shows a sample logical data model for a subset of the Cloud evoBrix PMIS solution's Provider Enrollment business area.

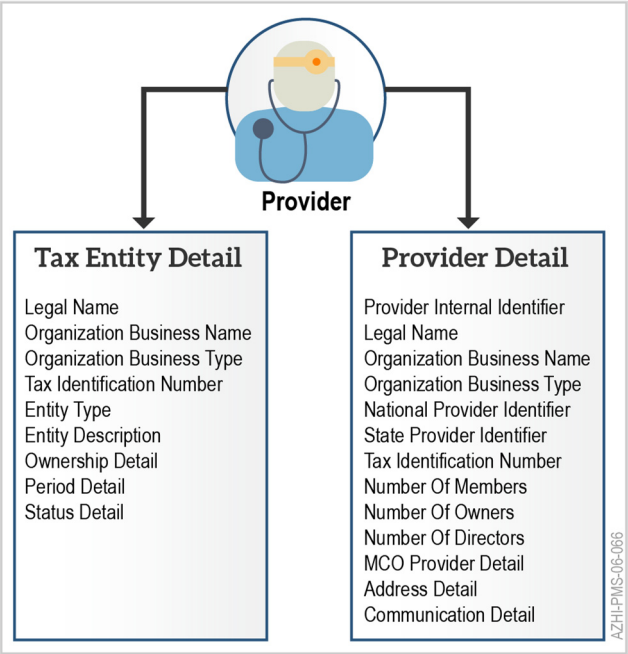


Figure A.6.1-17. The evoBrix Provider Enrollment – Logical Data Model. The evoBrix Logical data model was designed and refined using the best practices learned from MMIS implementations across multiple tenants.

A.6.1.14 Central Repository [SOW, Section 5.1.17]

The evoBrix PMIS solution repository is comprised of different types of data as noted below:

- Master Data – Data used for reference such as list of providers and taxonomy.
- Transactional Data – Data generated as result of transactions such as provider enrollment and provider maintenance.
- Configuration Data – Data that manage the day-to-day functioning of the evoBrix PMIS solution such as restriction rules.
- Access Control Data – Data regarding the list of users who can access the evoBrix PMIS system, their roles, and privileges.

The evoBrix PMIS solution also maintains a failover server with all the above-mentioned data replicated in real time. All evoBrix PMIS solution data stored in these two centralized databases never get transferred to off-shore locations. Any data used for development and analytical purposes is deidentified which is key for ensuring data privacy, confidentiality, and data protection.

A.6.1.15 E-Signatures [SOW, Section 5.1.19]

The Provider Agreement signature page automatically populates the logged in Provider first and last name along with the system date which cannot be modified by the user. The evoBrix PMIS solution ensures that the electronic signature is unique to the person using it, is capable of reliable verification and the not to allow any alteration or deletion of the electronically signed record without invalidating.

CNSI's evoBrix PMIS provides the audit tracking and transaction history capabilities of the electronic signature solution which includes the First Name, Last Name and date of signature. This builds a comprehensive audit trail with the date and login user details that each signature was applied on a Provider Agreement. The audit trail contains a unique identifier, that can be used to look up a record in our database that shows who signed a document and when. Figure A.6.1-18 shows the consent and electronic signature confirmation on the Provider Agreement screen during enrollment submission.

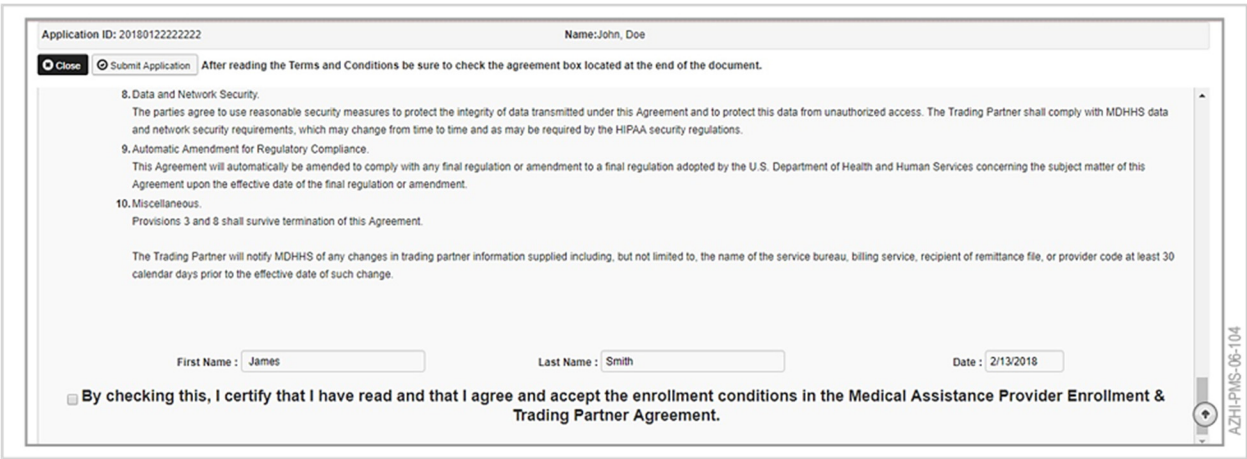


Figure A.6.1-18. Electronic Signature Page. Provider enrollment submission process requires consent and sign electronically to ensure that provider agreement is accepted by the enrolling provider.

Digital Signature

Digital signature implementation will use a private key to generate a digital signature; Each signatory possesses a private and public key pair. Public keys may be known by the public; private keys are kept secret. Anyone can verify the signature by employing the signatory's public key. However only the user that possesses the private key can perform signature generation. The digital signature algorithm allows an entity to authenticate the integrity of signed data and the identity of the signatory.

A.6.1.16 Consistency with CMS Technical Reference Architecture (TRA) [SOW, Section 5.1.22]

Key Capabilities of the Technical Solution

Figure A.6.1-19 highlights and communicates the key features and related benefits of the proposed AHCCCS solution. AHCCCS will greatly benefit from the proven, innovative evoBrix solution, as it aligns well with AHCCCS' vision to create a modular Medicaid solution focused on business outcomes.

Features and Capabilities	Benefits
Modularity	Maximizes flexible procurement options supported by Modularity Eliminates vendor lock-in
Interoperability	Enhanced interoperability allows for increased information exchange among trading partners and other agencies
Configurability	Rules-based architecture enables changes to business rules through configuration

Features and Capabilities	Benefits
Accessibility	Ensure enterprise-wide access to services through various access channels
Adaptability and Extensibility	Agility to adapt to changes in AHCCCS business and regulatory environment Modules are highly configurable to support evolving business needs with the portfolio of business and technical services
Security	Secured access to information, information exchange, secure communication, protection of privacy, and data security
Scalability	Scale up functional and technical capacity based on business demands Support business growth
Alignment to Industry Standards	Leverage business process improvement opportunities through MITA business process maturity

Figure A.6.1-19. Key Features. Illustrates CNSI's proposed Technical Solution's features and their benefits to the State.

A.6.2 Documentation and Certification [SOW, Section 5.2]

Not applicable

A.6.3 Regulatory System Compliance Requirements [SOW, Section 5.3]

A.6.3.1 Section 508 and W3C Compliance Reports [SOW, Section 5.3.2]

The browser version range listed in Figure A.6.3-1 indicates the minimum versions for those browsers that have been tested for compatibility with the evoBrix application.

Browser Name	Compatibility Tested Versions
Apple Safari	9 or higher
Firefox	20 or higher
Google Chrome	26 or higher
Microsoft Edge	25 or higher
Microsoft Internet Explorer	9 or higher
Otello Opera	49 or higher

Figure A.6.3-1.Compatibility with Browsers. evoBrix PMIS is developed with W3C web-based standards and is designed to work on Safari, Firefox, Chrome, Edge, Internet Explorer and Opera browsers.

W3C Standards. CNSI's proposed evoBrix PMIS solution is compliant with W3C's technical specifications and standards as shown in Figure A.6.3-2.

Specs/Stds	CNSI evoBrix PMIS
Browser Support	evoBrix PMIS is designed to work on Safari, Firefox, Chrome, Edge, Internet Explorer, and Opera browsers. CNSI will coordinate with AHCCCS and perform compatibility testing for any new browser versions released in the future. Please see Appendix A, section A.6.3.1, for a listing of browser versions that have been tested for compatibility with the evoBrix application.
Web Design	CNSI's Accessibility layer technology components include HTML5, CSS3, Angular JS, and other interactive

Specs/Stds	CNSI evoBrix PMIS
	UI technologies to enable a fully responsive UI framework that can be accessed by a variety of devices.
Web of Devices	CNSI staff use our innovative mobile enabled application, SiteVisitPro (SVP) to plan, conduct, and maintain site visits. SVP is designed for use with tablets to enable our business operations staff to provide site visit updates on a real-time basis to support the enrollment process. Additionally, the portal is designed with a UI framework that has different tiers for business logic and content representation, and has Responsive UI to show different layouts on various device sizes (e.g., tablets and smart phones). It is designed and developed to be robust and highly scalable, as it is accessible through the public internet where multiple users may access it at any given time.
Web Architecture	By using Java 2 Platform, Enterprise Edition (J2EE) web architecture for evoBrix platform, the only software required on a user's computer is the internet browser as our application is being accessed through web browser complying with the principles of HTTP and URI technologies. As modern desktop, laptop, and tablet computers universally support web browsers, there is no reason to install client-side software, plugins, or framework. Use of fully browser based applications results in efficiencies for all since don't need to upgrade client hardware or software to match the AZ/HI system requirements.
XML Technology	CNSI's solution architecture supports standard content formats such as documents, XML, JSON, EDI for user- and machine-readable and -understandable content. CNSI's evoBrix PMIS solution utilizes evoBrix Integrator for supporting all the integration needs of the solution. evoBrix Integrator supports XML as a messaging format to ensure interoperability. The use of Web services supports a standards-based XML data exchange to enable interoperability between the system and other external applications to consume the data and interact with the system.
Web Services	CNSI's evoBrix Integrator OSB solution leverages ESB features within the SOA framework to integrate disparate systems effectively. The proposed solution is capable of handling common industry standard service requests such as SOAP and REST API's which leverages WSDL specifications for data exchange. This supports web-services-based information exchange for real-time integration capabilities.

Figure A.6.3-2. Meeting W3C Requirements.

A.6.3.2 Automated Provider Enrollment Screening/Monitoring Processes and Tools [SOW, Section 5.3.5]

Figure A.6.3-3 shows the various components in the PCS architecture, including real-time and batch services.

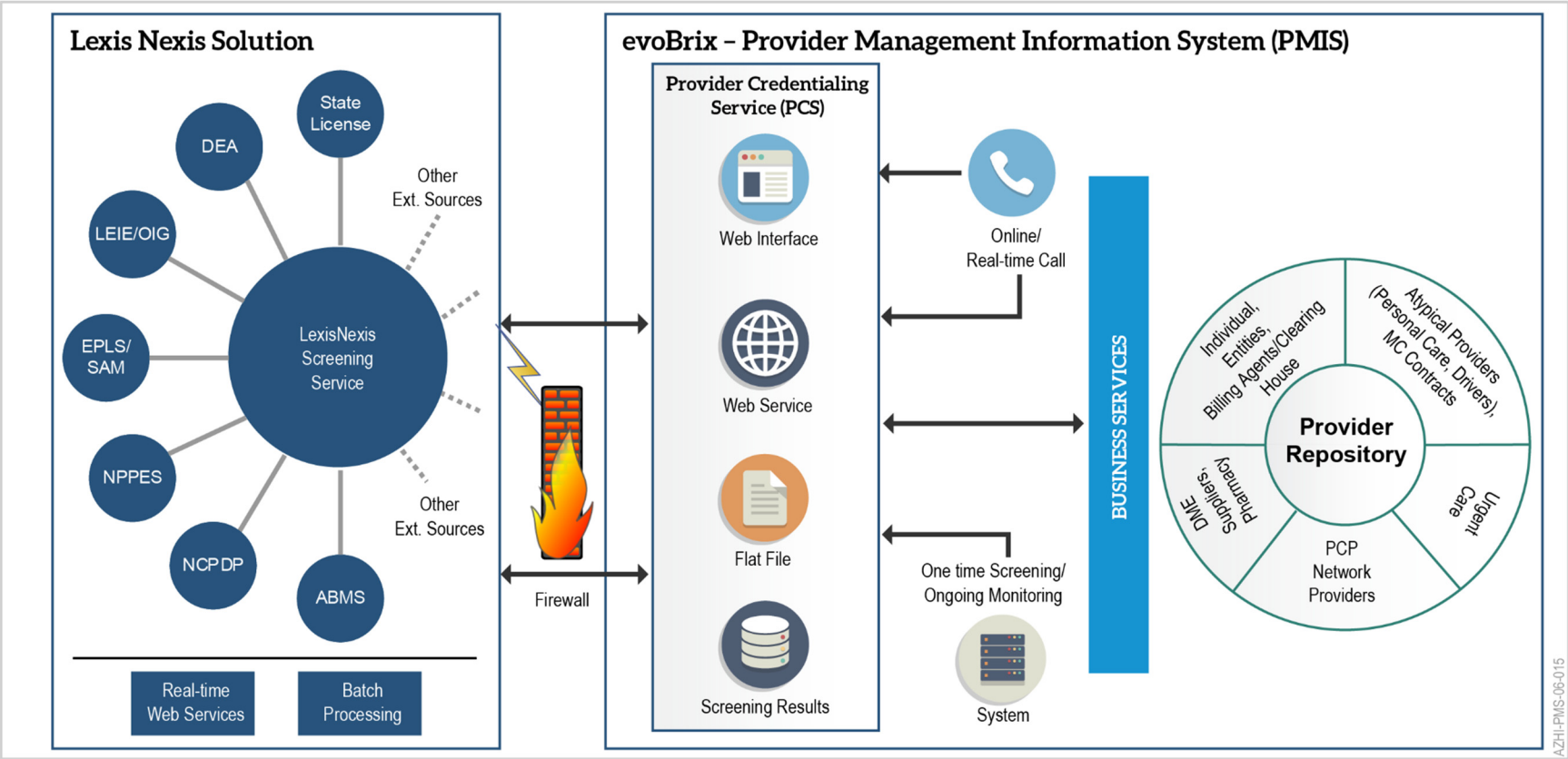


Figure A.6.3-3. Provider Credentialing Service Solution Overview. evoBrix PMIS integrates with LexisNexis and the AHCCCS/Med-QUEST approved CVO system.

This page intentionally left blank.

A.6.3.3 Compliance with CMS Harmonized Security and Privacy Framework [SOW, Section 5.3.12]

Figure A.6.3-4 provides an overview on how our solution is compliant with CMS Harmonized Security and Privacy Framework controls.

Control Name	Key Compliance Factors
Security Controls	Compliance with security controls that commensurate with the data sensitivity and encryption.
Identify and Access Management	Identify Proofing & Authorization
Managed Services Computing	Data Encryption Solutions, Data protection/audit Methods and Infrastructure Monitoring Framework
Data Encryption	Data Encryption at Rest and Data Encryption in Transit
Audit Trails	Data protection and Audit Methods
Business Continuity	Disaster Recovery Process
Compliance Oversight	Risk Assessment and Management, Penetration Testing and Continuous Monitoring and Reporting
Privacy	Accessibility, Data Integrity and Accountability
Systems and Data Classification	FIPS Publication 199 and FIPS Publication 200

Figure A.6.3-4. Harmonized Security and Privacy Framework. Key compliance factors of CNSI's evoBrix PMIS solution with respect to Harmonized Security and Privacy Framework controls.

A.6.3.4 Conformation to ITIL v3 Standards [SOW, Section 5.3.13]

Figure A.6.3-5 provides a visual description of our operations management strategy. It describes our ITIL-based operations management focus areas, key elements of our strategy, and the expected results and benefits.

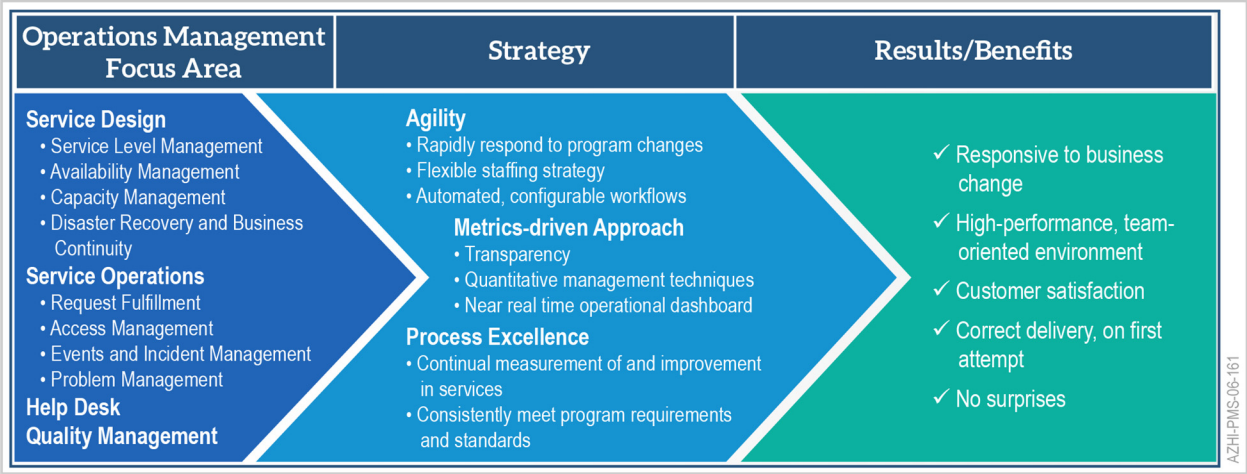


Figure A.6.3-5. CNSI's Operations Management Strategy. CNSI's operations management strategy helps AHCCCS/Med-QUEST achieve goals and objectives for the Medicaid enterprise.

A.6.4 Other System Architecture Requirements [SOW, Section 5.4]

A.6.4.1 Business Process Management and Workflow Technologies [SOW, Section 5.4.1]

CNSI's evoBrix PMIS is an automated and improved business process with a full range of online, real-time data entry, screening, and inquiry features, including expedited provider application processing. Based on the needs of AHCCCS/Med-QUEST, PMIS system allows the decision management framework includes features that allow authorized users to perform the following activities:

- Define State-specific Provider Types, specialty and subspecialty combinations
- Configure mandatory, optional, and conditionally mandatory enrollment and re-enrollment data requirements by provider Enrollment Type, Applicant Type, specialty and mode of claims submission method
- Define and configure credentialing and re-credentialing rules for each unique provider type and specialty combination

In evoBrix PMIS, business rules for provider management use the following tools to cover three broad areas:

- Credentialing Matrix – To define specific credentials, such as licensing, required by the successful applicant for each defined enrollment type or specialty and subspecialty combination
- Rule Composer – To define the enrollment steps needed for each category of enrollment
- Permissions Matrix – Permissions matrix allows to configure and maintain a cross walk of provider types with specialty, sub-specialty and other attributes. Authorized users can view this matrix through application screen as shown in Figure A.6.4-1. Authorized administrative users are allowed to maintain the permission matrix.

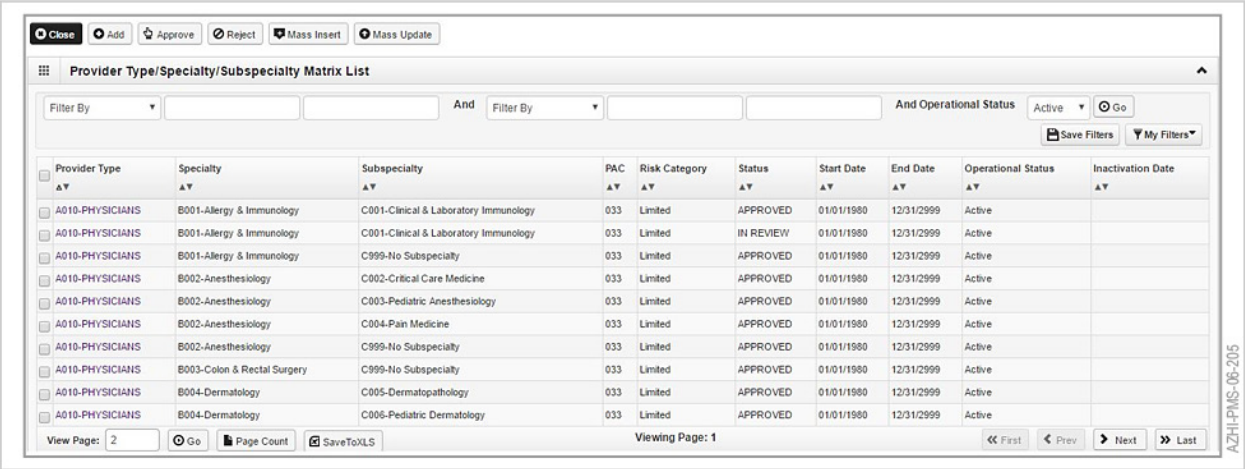


Figure A.6.4-1. Permissions Matrix. The AHCCCS solution allows to specify the specialty and sub-specialty cross walk with provider types.

- Business Process Wizard (BPW) – The PMIS supports interactive online enrollment application, which provides structured, online screens with a business process wizard (BPW) for provider enrollment. The wizard guides the provider through the step-by-step enrollment process. The BPWs are configured to the State's standards and fully support State-specific credentialing rules. As the provider proceeds through the application, the wizard marks each step as required or optional, and shows which steps have been completed. The provider enrollment BPW is configurable for different enrollment types. Figure A.6.4-2 shows an example of the BPW for a newly-initiated enrollment with the individual enrollment type.

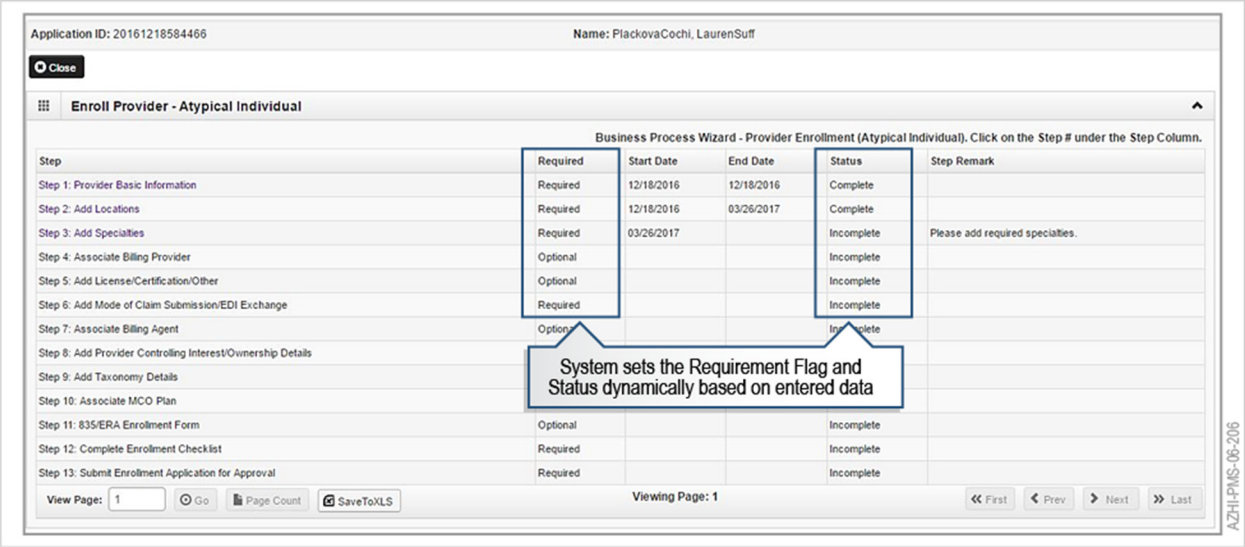


Figure A.6.4-2. Provider Enrollment Business Process Wizard. AHCCCS solution wizard guides the enrolling provider through all steps of the enrollment process.

Workflow Features

Real-time Configuration

The evoBrix PMIS workflow engine processes work queues in real time, assigns tasks, sends notifications, and provides escalation to management and/or supervisors. State-authorized users will receive notification messages to their “My Inbox” section and will be able to navigate directly to the applications that need action. evoBrix PMIS online screens provide users the ability to modify any existing rule and allow applications to be routed to another business unit/owner. New rules can be defined at any point, allowing additional enrollments to be assigned to the right business units or owners. evoBrix PMIS workflow rules can be configured using online screens as shown in Figure A.6.4-3 and Figure A.6.4-4. State-authorized users are able to maintain and modify rules based on business process requirements. The evoBrix PMIS screens present users with a visual representation of all workflow rules and how they are being used throughout the system. Using online screens, State-authorized users are also able to view pending applications and re-route them to another business unit or owner.

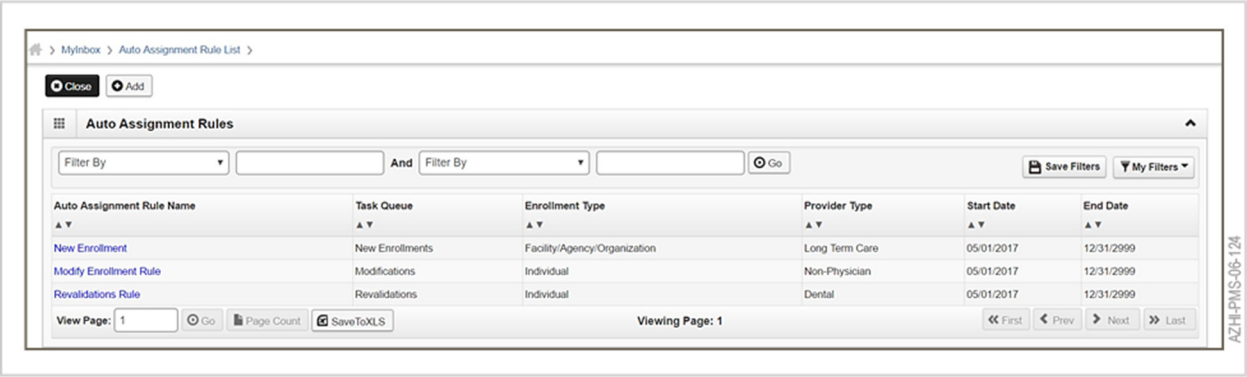


Figure A.6.4-3. Auto Assignment Rules Screen. This screen allows business users to define/modify the workflow process for New Provider Enrollment applications.

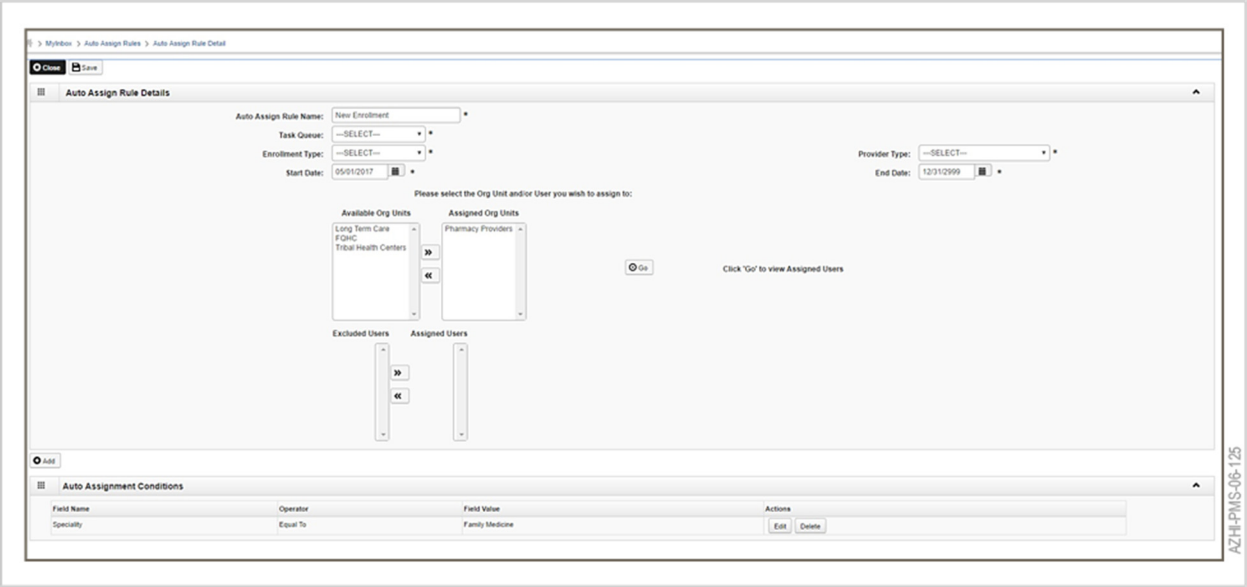


Figure A.6.4-4. Auto Assignment Rule Details Screen. This screen allows business users to assign Organization Units to a workflow process.

The evoBrix PMIS Workflow screens allow configuration of user assignments to work queues/locations based on attributes such as Enrollment Type, Provider Type, Specialties. These configurable screens support the business logic embedded in the rules. These can be maintained by the administrator in real time and support distributions of work based on workloads. evoBrix work management configuration screens support supervisory operations for the management of workflow including:

- Assignments/re-assignments
- Work allocation and load balancing
- Approval for work assignments and work deliverables via a tiered approach
- Ability to take necessary action or provide notification when corrective action is needed
- Intelligent work distribution and re-distribution based on work type, worker skill, priority, and age of work

The evoBrix PMIS Workflow screens present users with a visual representation of all workflow rules and how they are used throughout the system. Using online screens, Provider Enrollment staff can also view pending applications and re-route them to another business unit or owner. Figure A.6.4-5 shows the screen through which administrative users can monitor and manage runtime workflow process executions.

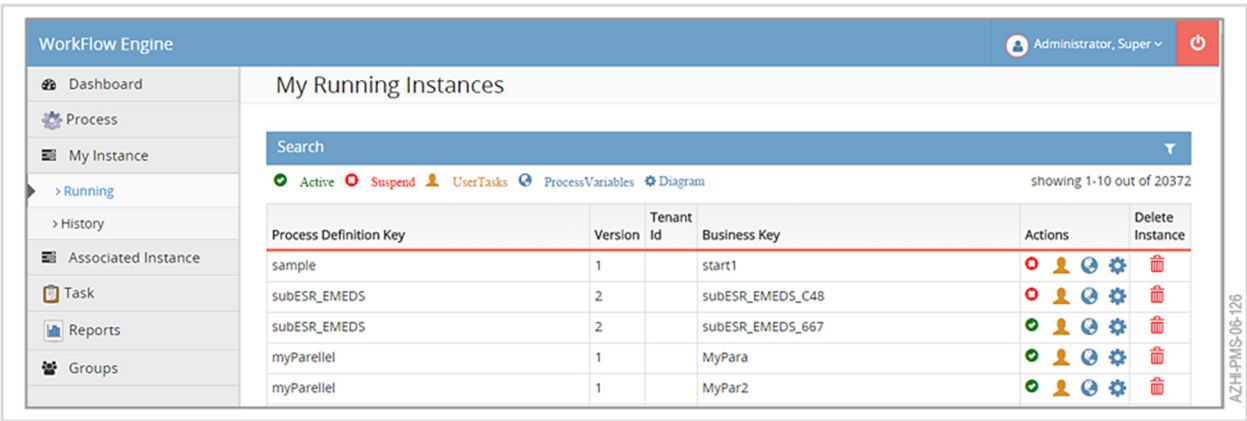


Figure A.6.4-5. Process Flow Monitoring. This screen allows administrative users to monitor and manage runtime executions of process flows.

CNSI's workflow solution provides the ability to view alerts and/or reminders by user and by work-type. State staff receive notification messages in their "My Reminders" section, as shown in Figure A.6.4-6, and can navigate directly to the item that needs action. The access to the content can be configured using evoBrix PMIS RBAC security.

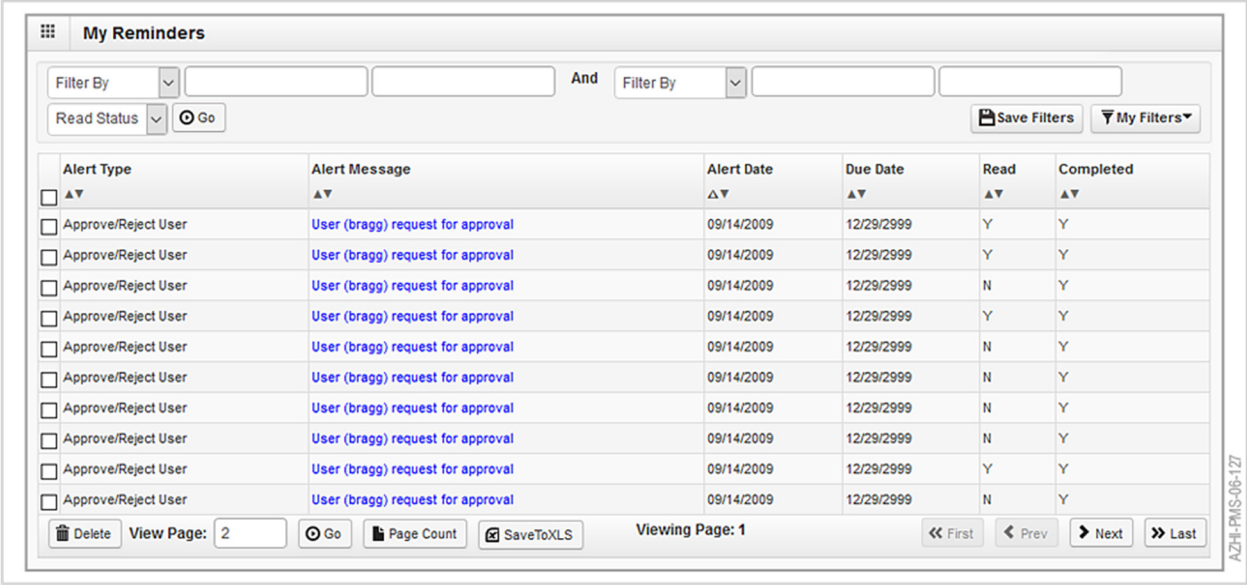


Figure A.6.4-6. Inbox View. This panel presents a list of alerts or messages for a specific user.

Figure A.6.4-7 shows the view of the task list assigned to a user for their action.

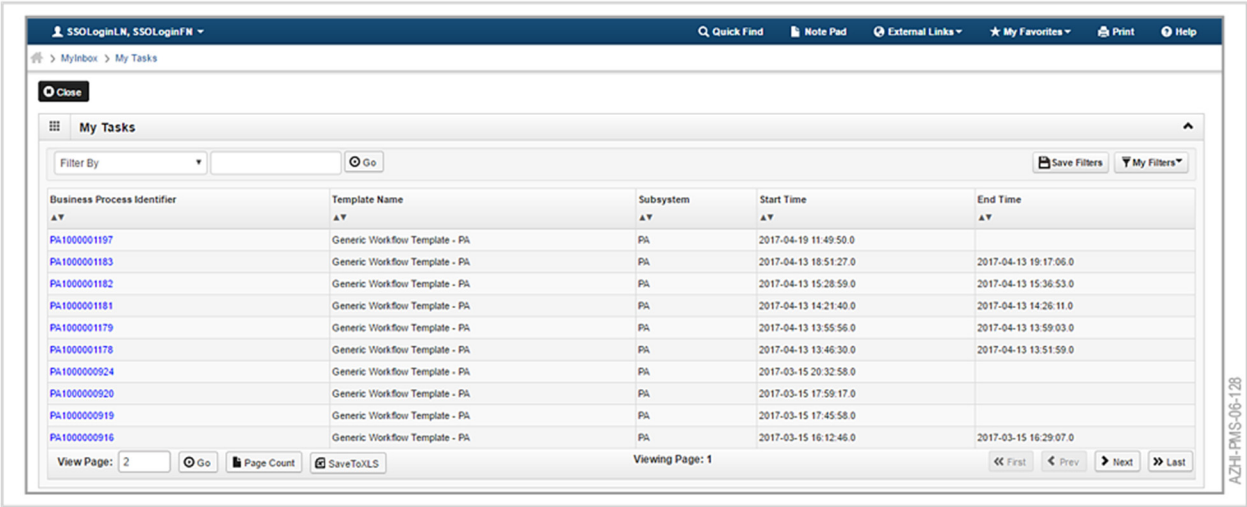


Figure A.6.4-7. Tasks View. This panel presents a list of tasks that are assigned to a specific user.

CNSI's workflow solution runtime engine uses industry standard Business Process Model and Notation (BPMN) 2.0 for configuring workflow. Figure A.6.4-8 shows a sample process flow depicted using BPMN.

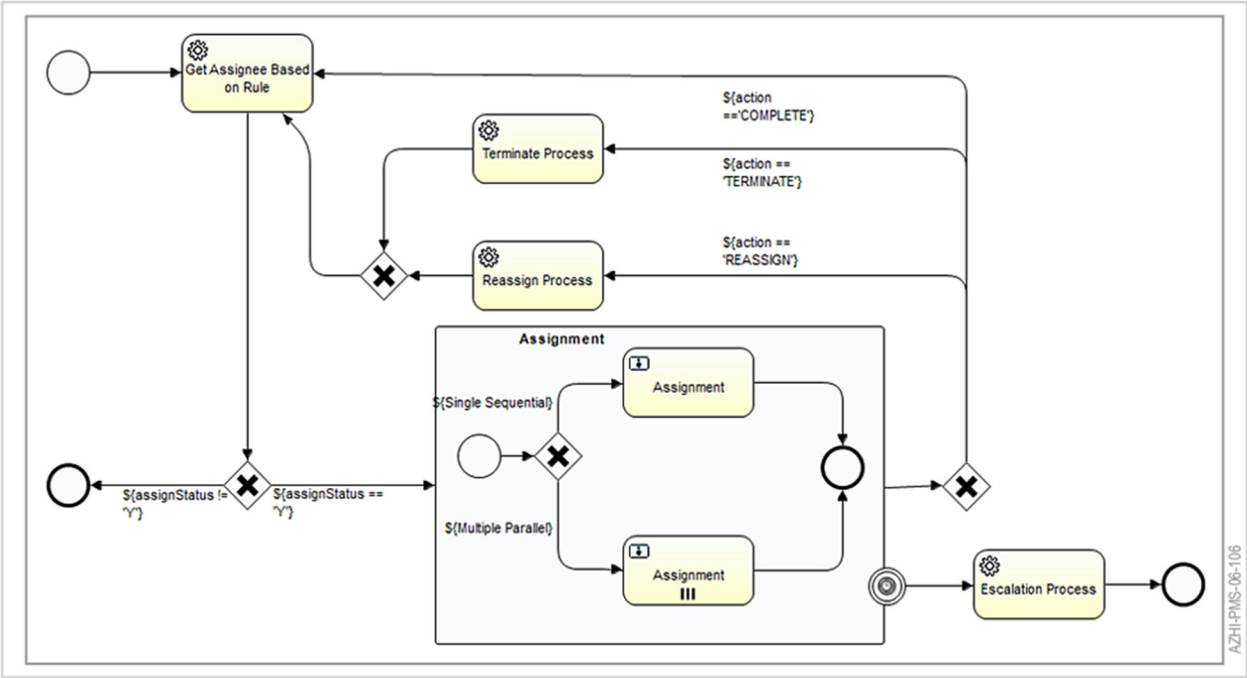


Figure A.6.4-8. BPMN Notation Usage. A sample process flow using BPMN.

For instance, provider enrollment applications can be forwarded to specific Organization Units or to a specific user within a group. Different combinations of enrollment types/provider types and specialties can be configured to route the enrollment applications to departments specialized in that area.

CNSI's workflow solution supports work queues. Data and documents can be routed across worker's queue and through web services across different solutions or applications.

Figure A.6.4-9 shows a reassignment of an open task from one worker's queue to another.

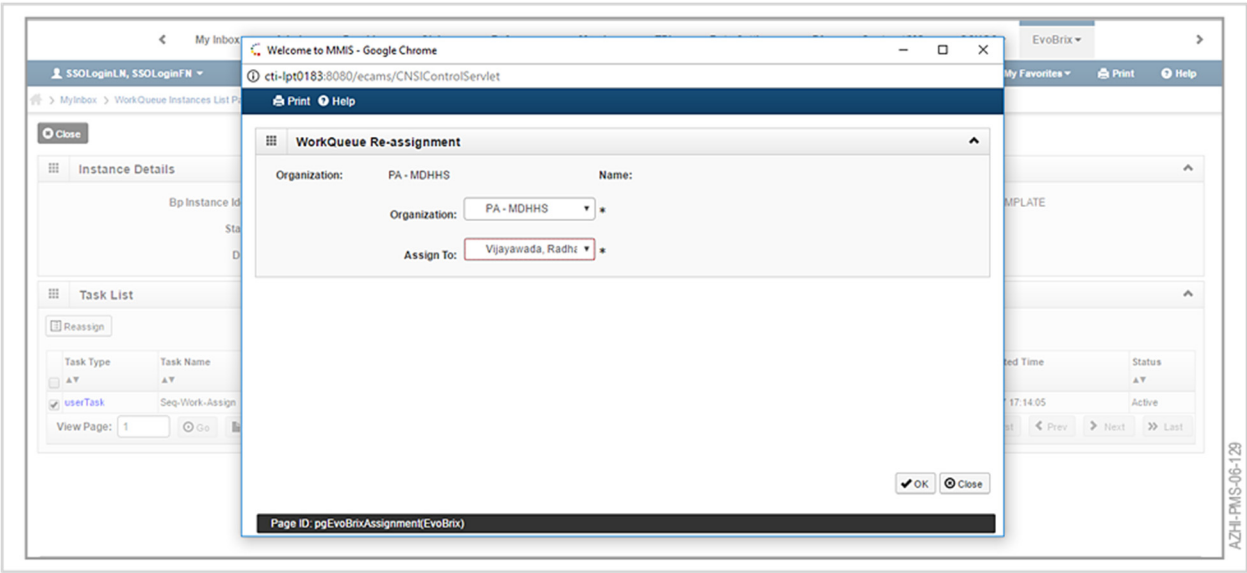


Figure A.6.4-9. The evoBrix Workflow - Task Reassignment Screen. Tasks can be reassigned from one worker queue to another through this screen.

CNSI's integrated workflow management solution supports the State desire for improved automation, reduced manual intervention, configurable work routing, and task management. This helps reduce time

for the overall completion of a process as well as reducing potential errors caused by human interaction. The evoBrix PMIS Workflow solution comes with table-driven configurable rules, task routing, assignment, and tracking capabilities. This makes processes more efficient, compliant, agile, and visible by ensuring that every process step is explicitly defined, monitored over time, and optimized for maximum productivity. CNSI's workflow solution will ensure compliance with state defined processes.

A.6.4.2 Separate Business Rules Engine [SOW, Section 5.4.3]

The flexible and comprehensive RuleIT Rule Composer allows authorized users to define the enrollment rules for each provider enrollment type and specialty. An enrollment type is a predefined general category of provider. Authorized users will use the Rules Composer to define each step of the enrollment process and the data elements required to complete that step for each enrollment type. The business rules developed using RuleIT are deployed to providers and business operations staff in the form of Business Process Wizards (BPWs) that govern the enrollment and maintenance activities for each type of enrollment. Once all the business rules are defined, the authorized State user will use the Rules Composer to organize the enrollment path for each type of enrollment.

RuleIT Composer provides a user name and password screen to authenticate users before they are allowed access to the application. Administration of RuleIT users is available to authorized security administrators through online screens. Users can be added and removed and their appropriate privileges can be assigned through this interface, so it does not pose a risk of unauthorized data access. Figure A.6.4-10 shows the Rule IT Composer login screen.

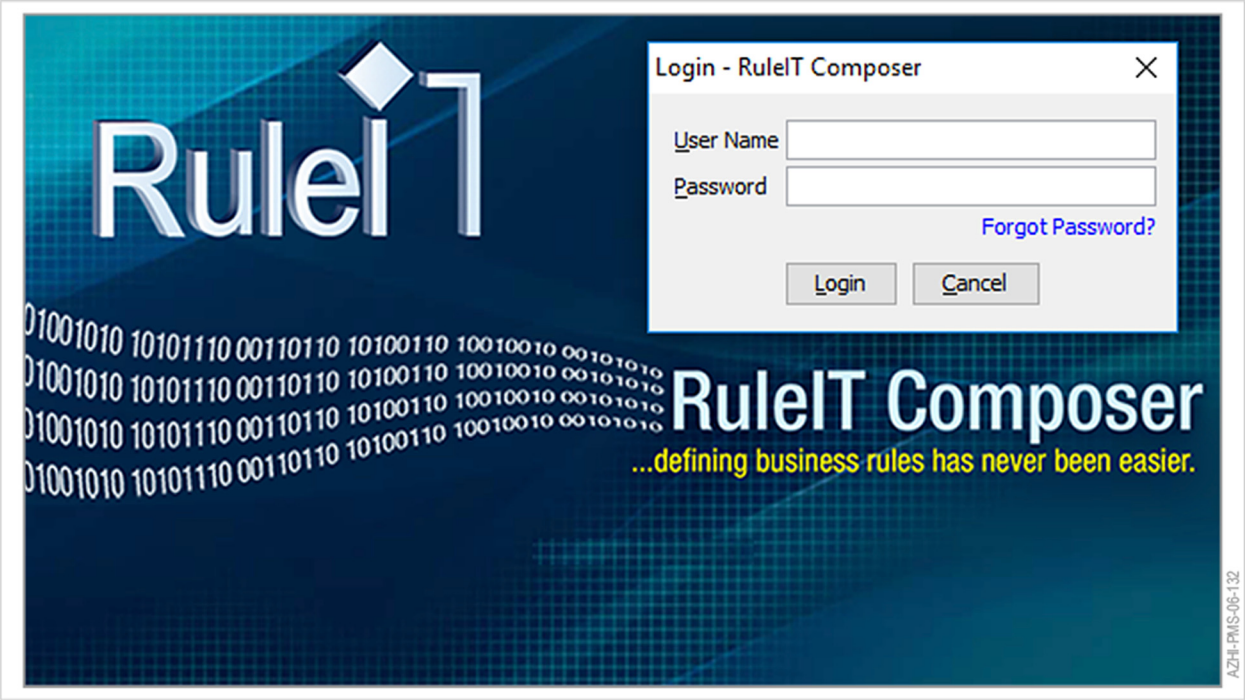


Figure A.6.4-10. RuleIT Composer Login Screen. RuleIT supports well-tested and audited authentication and authorization security measures.

The RuleIT Composer component is built on the Java platform, and is a graphical user interface (GUI) used for creating, editing, exporting, importing, and searching rules in a repository, as shown Figure A.6.4-11. It also provides the capability to document the rule and the option to make the rule change time-sensitive for claim processing. RuleIT Composer also allows users to navigate all the rules and search within the rules based on user-selected criteria. These features enable designated Department users to apply or disable rules quickly and without programmer intervention.

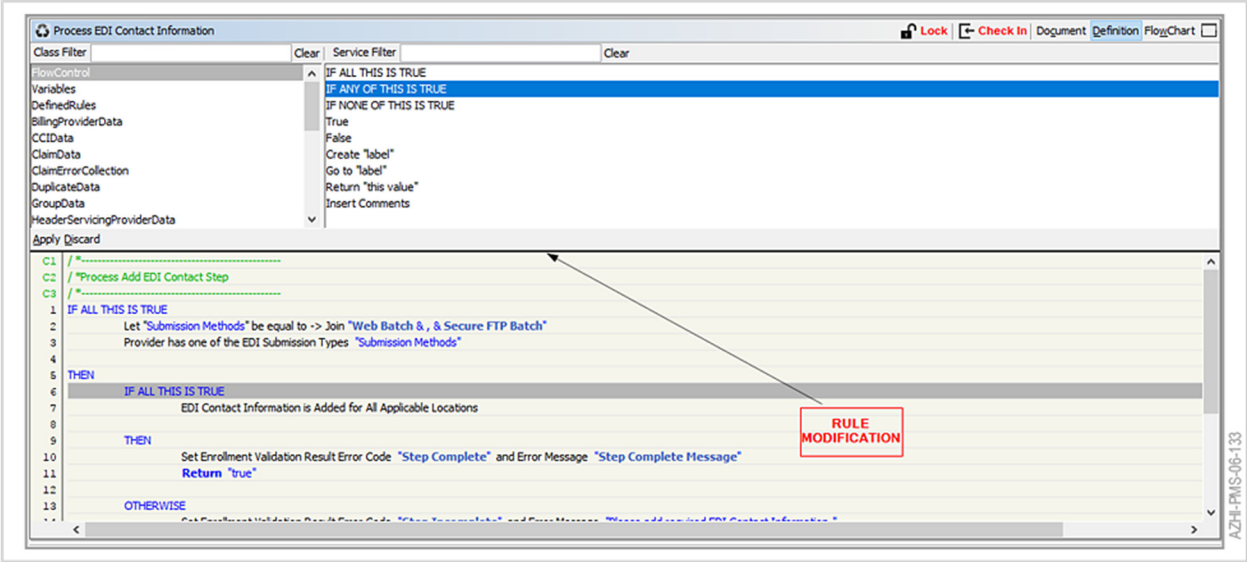


Figure A.6.4-11. RuleIT Composer Rules Editing Screen. RuleIT's user-friendly GUI facilitates rules maintenance without coding changes.

CNSI has honed a balanced approach to manage the implementation of business rules via online configuration-driven tables and declarative English-like rules syntax in the rules engine. RuleIT Composer allows subject matter experts or technical resources to write natural language business rules. These rules are human-readable, as shown in Figure A.6.4-12.

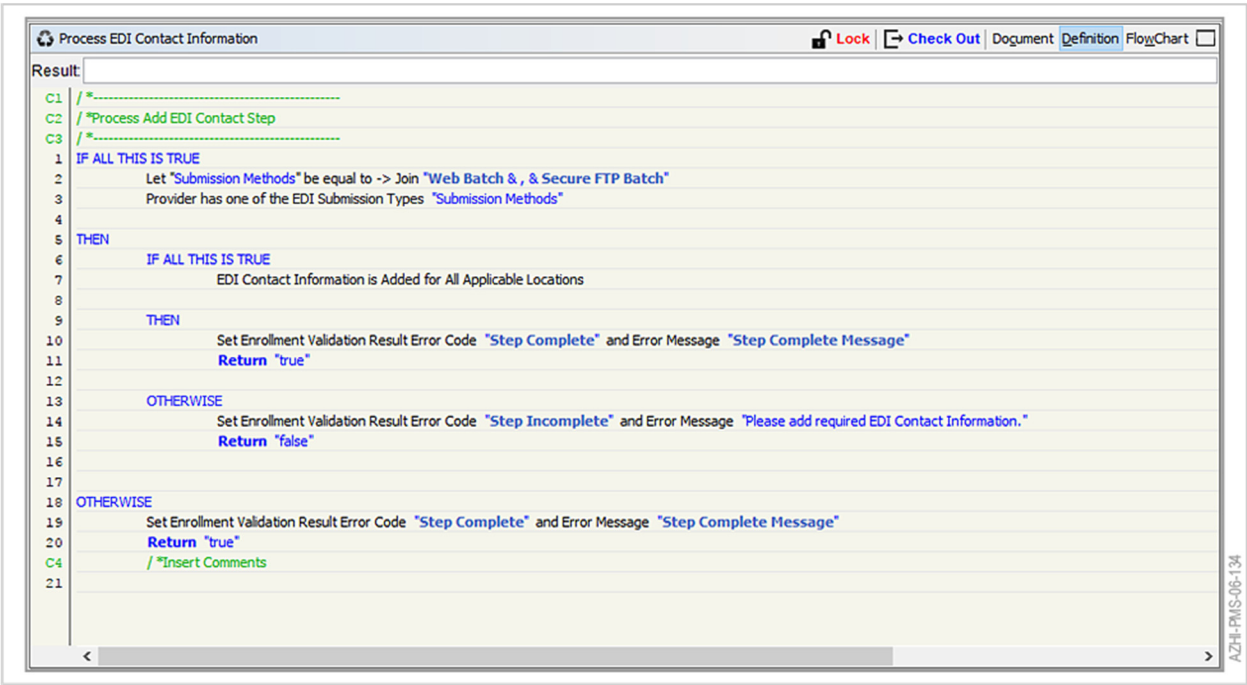


Figure A.6.4-12. RuleIT Composer Rules Screen. RuleIT provides an intuitive English-like user interface and a decision tree model of implementation.

The flexible and comprehensive RuleIT Rule Composer allows authorized users to define the enrollment rules for each provider enrollment type and specialty. An enrollment type is a predefined general category of provider. Authorized users will use the Rules Composer to define each step of the enrollment process and the data elements required to complete that step for each enrollment type. The business rules developed using RuleIT are deployed to providers and business operations staff in the form of Business

Process Wizards (BPWs) that govern the enrollment and maintenance activities for each type of enrollment. Once all the business rules are defined, the authorized State user will use the Rules Composer to organize the enrollment path for each type of enrollment.

The evoBrix PMIS leverages RuleIT, a rules engine based on industry standards and built specifically to address the Medicaid program. The RuleIT Composer shown in Figure A.6.4-13 is the component of RuleIT used to add, modify, or remove/retire rules in the rules engine repository. The exhibit highlights some of the key features of this tool and shows a sample rule syntax.

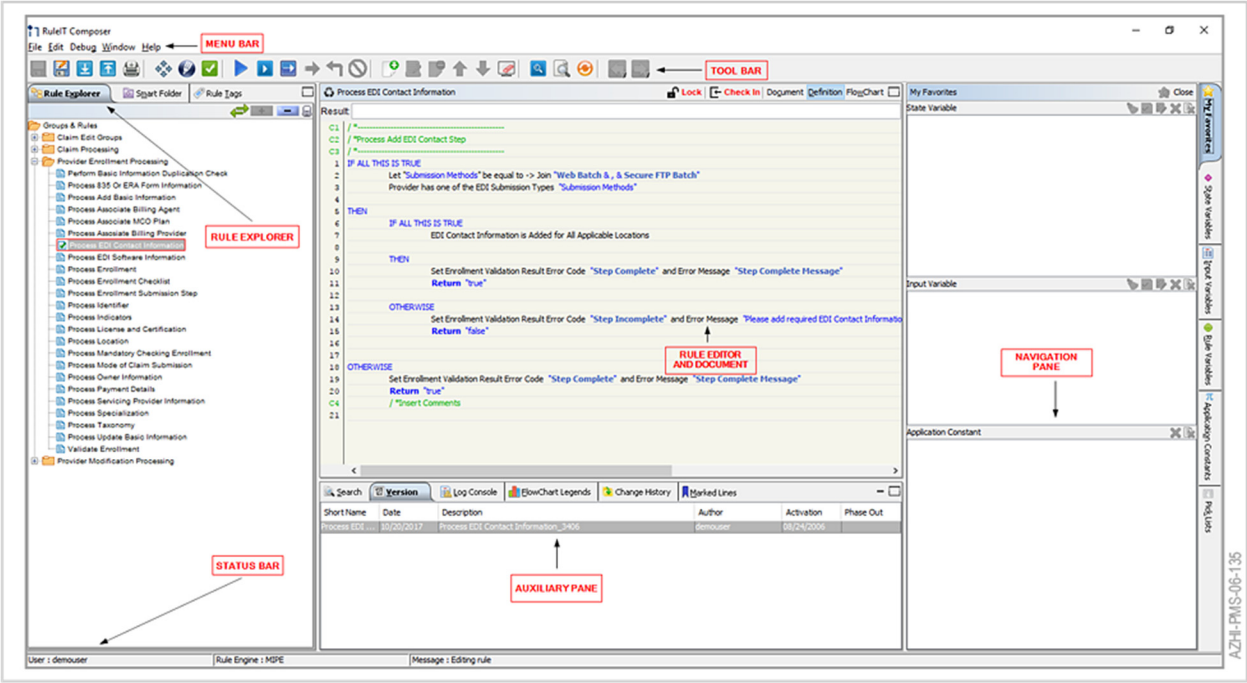


Figure A.6.4-13. RuleIT Composer. RuleIT Composer has a user-friendly interface that makes it easy to use.

Using RuleIT Composer, users can modify the rules for the change in business variable values and application constants. After the rule modification, rule validation can be checked as shown in Figure A.6.4-14. Rules are developed in the development environment and promoted to higher environments such as test, user acceptance, and production using the RuleIT Migrator. The rules migration process is performed during the scheduled deployment window and will not impact production rules engine availability and operations.

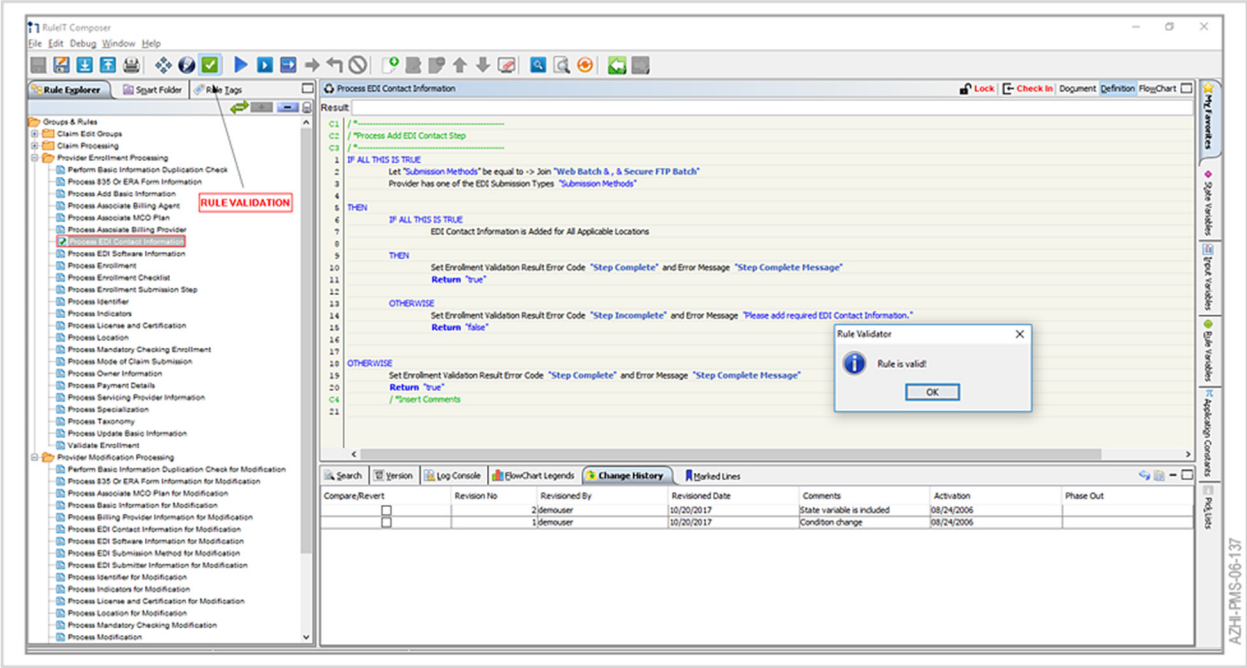


Figure A.6.4-14. RuleIT Composer Rules Validation Screen. RuleIT allows users to easy access to validate the rules.

The table-driven Permissions Matrix changes are tied to effective date ranges and will not disrupt the rules implementation in production. Authorized State staff can use an evoBrix PMIS feature called “Mass Update” to apply the Permission Matrix changes to all impacted providers at the same time.

Rules change history is maintained and the users would be able to roll back to the previous versions when required, as shown in Figure A.6.4-15. Rules are developed in the development environment and promoted to higher environments such as test, user acceptance, and production using the RuleIT Migrator. The rules migration process is performed during the scheduled deployment window and will not impact production rules engine availability and operations.

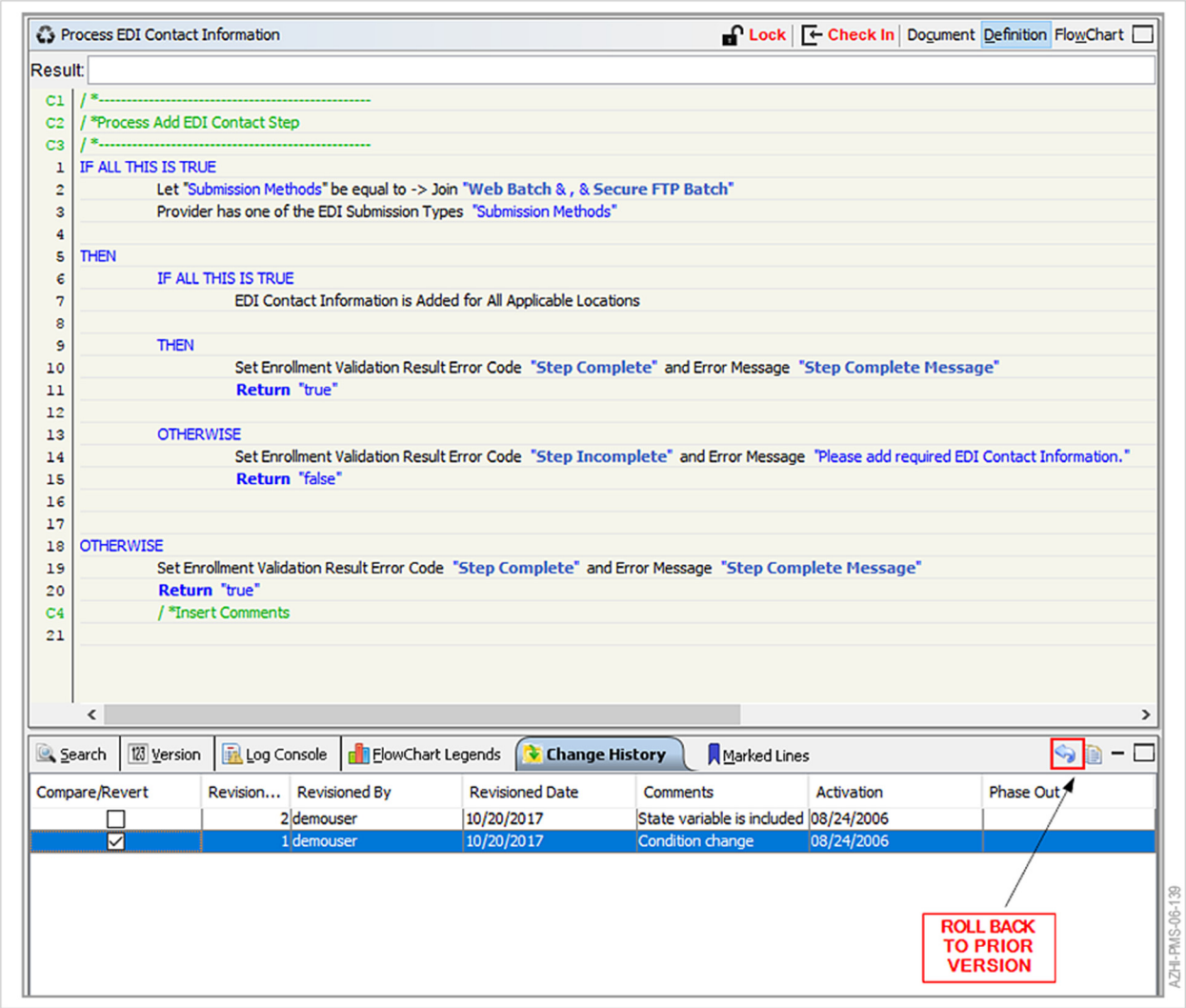


Figure A.6.4-15. RuleIT Composer Change History Screen. RuleIT allows users to roll back changes and retrieve older versions of the rule.

RuleIT offers the flexibility to create and integrate customized rules specific to the Department's needs and can accommodate changes to existing rules. The flexibility and increased productivity that RuleIT offers will reduce the time it takes to build, test, and implement complex rules. RuleIT Composer provides the option to retire rules, which can be useful when rules must be retired based on policy changes. Figure A.6.4-16 shows the screen used for retiring a rule.

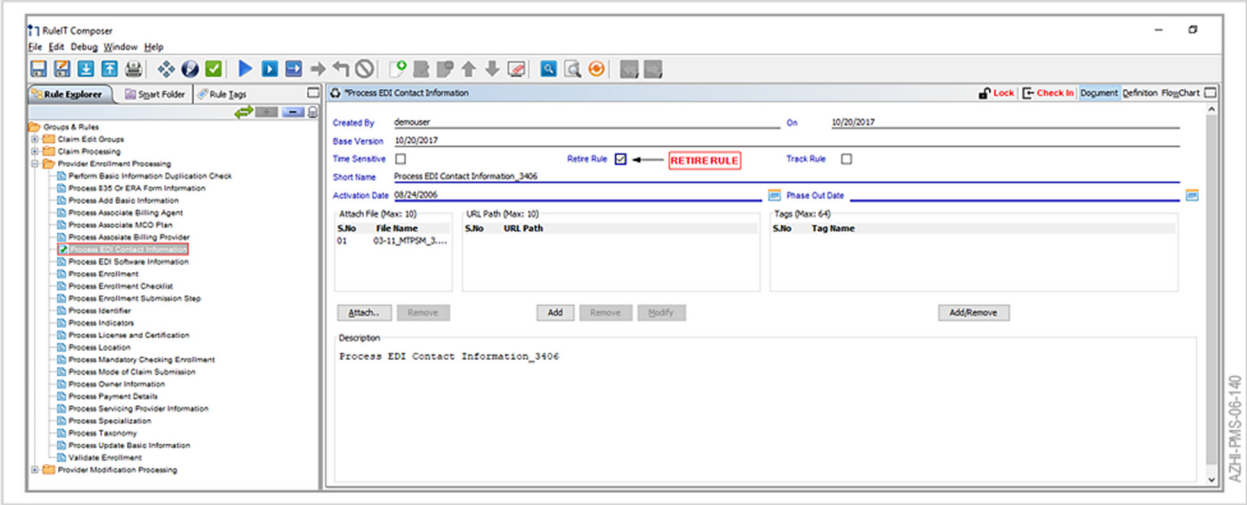


Figure A.6.4-16. RuleIT Composer Retire Rule Configuration Screen. RuleIT supports retiring rules through an easy configuration screen.

CNSI uses the Web services framework to integrate with other components. The architecture provides for a set of tools and infrastructure services to support the management of integration with other components in the enterprise using SOA principles. RuleIT Processor can be exposed as a service to external components using a Web services wrapper. When exposed as a webservice, the rules can be consumed by external enterprise application using SOA integration methodologies.

CNSI maintains a fully-integrated testing environment that contains production data to allow authorized users to perform “what-if testing.” This environment will mimic the production setup and can be refreshed with the current production data to support impact analysis of “what-if” scenarios. The before and after outcomes can be compared and results of the comparison can be published to State staff and designated project resources. Further, RuleIT Evaluator, a component of RuleIT, enables users to test business rules by creating scenarios based on various rules inputs and perform “what-if testing,” which aids in understanding the impact and analyzing outcomes of the changes. This is illustrated in Figure A.6.4-17.

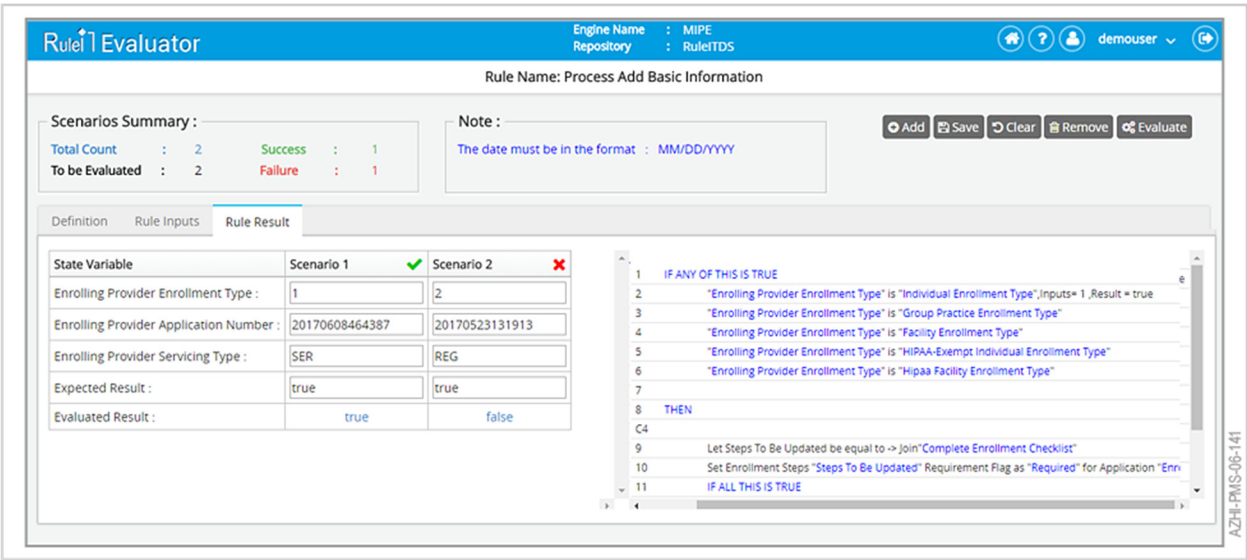


Figure A.6.4-17. RuleIT Evaluator screen. RuleIT Evaluator performs rules testing to understand the before and after outcomes and supports what-if scenario testing.

The graphical representation of the business rules flow is presented using the RuleIT Modeler is shown in Figure A.6.4-18. The business rules flow could be altered using the modeling elements, and the user would be able to publish the rule and view the rule definition as English-like syntax.

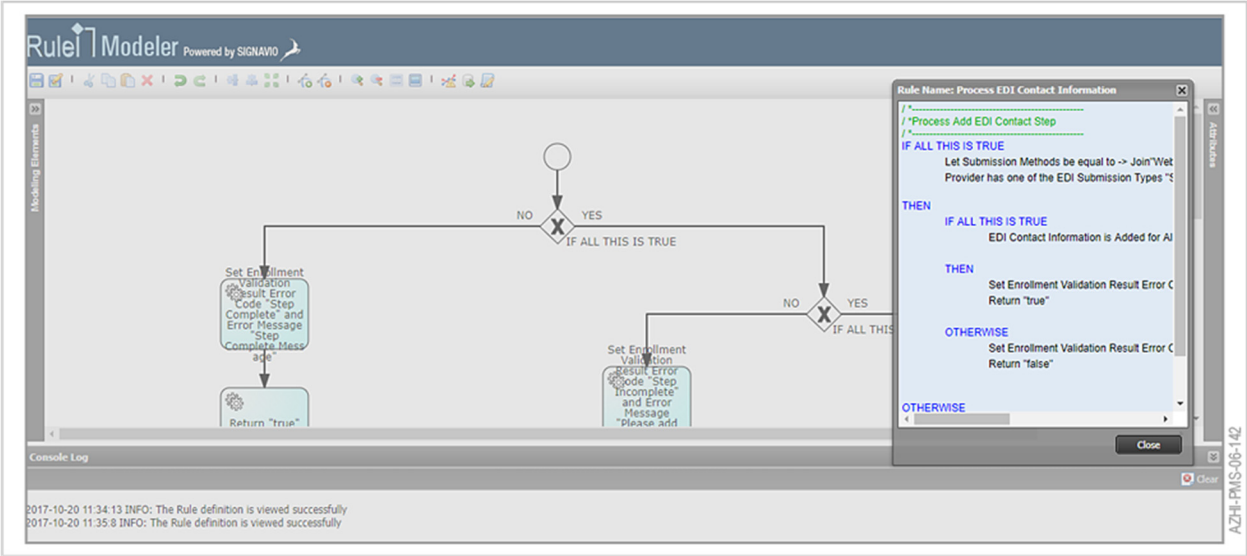


Figure A.6.4-18. RuleIT Modeler Screen. RuleIT Modeler provides a graphical representation of the rules flows.

A.6.4.3 Errors and Exception Conditions [SOW, Section 5.4.5]

CNSI's Cloud evoBrix solution utilizes generic frameworks and codes to handle business functions widely used within the system. For example, a generic model framework referred to as Message Management Framework (MMF) is used to maintain and interact with application to generate messages and correspondences. MMF addresses the need to streamline application and system messaging by following a universal framework across various modules in the evoBrix PMIS solution. This is a multi-tenant, multi-language compliant framework that dynamically builds messages based on configurable pre-defined parameters stored in the MMF configuration data mart. This approach helps messages and parameters to be easily configured without having to alter the program code. Figure 19 shows the nomenclature that is used to drive the configuration of messages in the evoBrix PMIS solution using the Message Management Framework.

Various message categories are handled by MMF including, but not limited to:

- Application Message - Warning/errors related to the application screens or operations
    - Services Validation Message
    - Persistence Validation Message
    - Message Encrypt Validation Message
- Security Message - Authentication/ unauthorized access related messages
    - Authentication Validation Message
    - Application Access Validation Message
    - Unauthorized Access Validation Message
    - Validation Message - Any generic validation that doesn't conform to a specific function
    - Tenant Validation Message
    - Login Validation Message
- Other Generic Messages

As shown below CNSI's evoBrix framework intelligently handles all Error and Exception conditions and displays it in a meaningful way to the User.

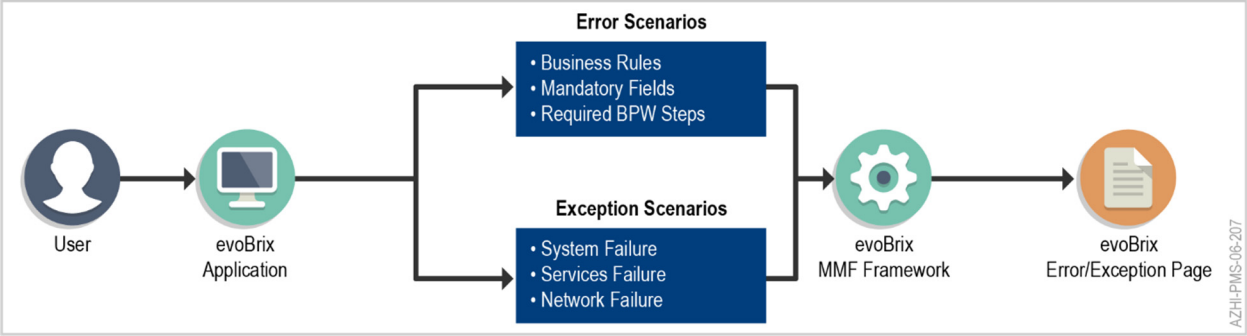


Figure A.6.4-19. Error and Exception Conditions Handling. evoBrix PMIS distinguishes between errors and exception conditions.

A.6.4.4 Deployment of System Components in Cloud Computing Environments [SOW, Section 5.4.6]

CNSI's knowledge and understanding of building, testing, and successful integration of various modules to provide the requisite services provided by an MMIS is based on its Washington and Michigan implementations that are certified by CMS, coupled with adherence to the industry best practices by following the ITIL-aligned Configuration Management (CM) policies, processes, and procedures. As shown in Figure A.6.4-20, this provides a framework to avoid any unauthorized changes, manage the baselines to support multiple environments, and provide traceability and auditing for all CIs throughout the lifecycle of the AHCCCS/Med-QUEST solution. This practice has enabled us to deploy our Solution as needed. Our recent implementations as part of CHAMPS into the State of Michigan's Private Cloud and our Demo environments hosted in Oracle Public Cloud are a living testimony to our practice and maturity of the deployment processes.

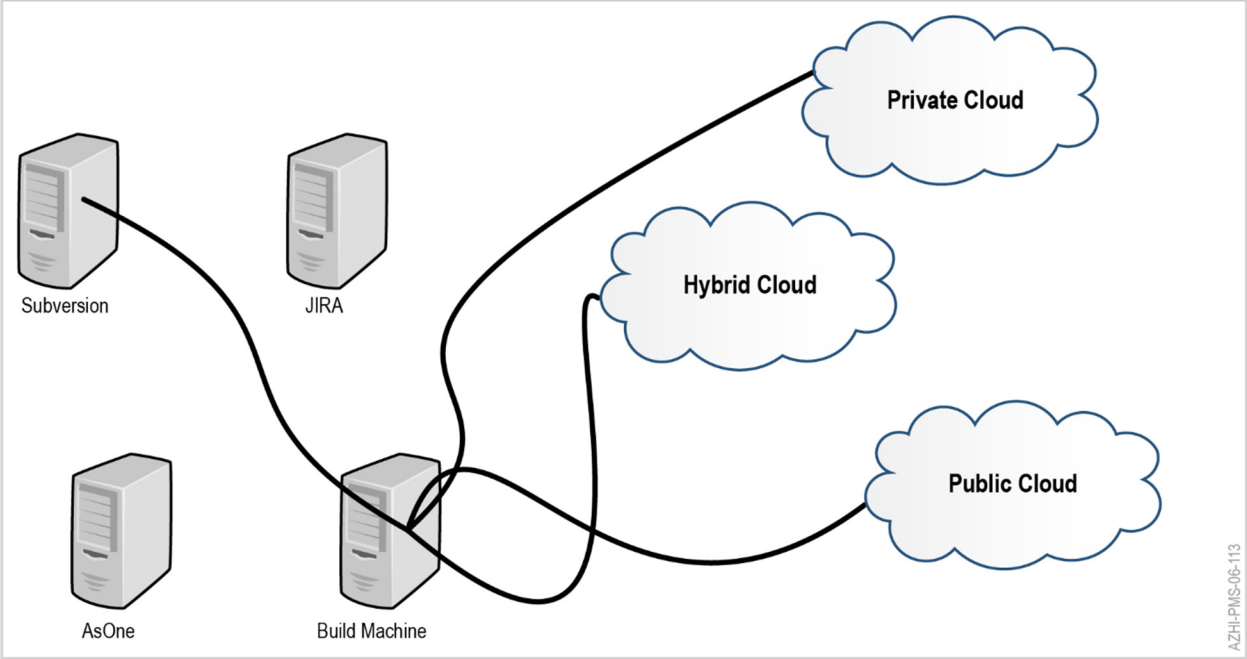


Figure A.6.4-20. Flexibility of Solution deployment to Private Cloud, Public Cloud or a Hybrid Model. CNSI's Release and Deployment model allows the packaging of code in a central repository and its deployment to any cloud ecosystem.

The ITIL framework defines several processes and functional groups and their relationship with a CM system. New Systems Team members are encouraged to obtain ITIL certifications while existing members already have or are on track towards obtaining ITIL foundation level certifications at a minimum to maintain alignment with the latest standards. Figure A.6.4-21 illustrates how the different functional groups feed and obtain data from the CM-maintained system.

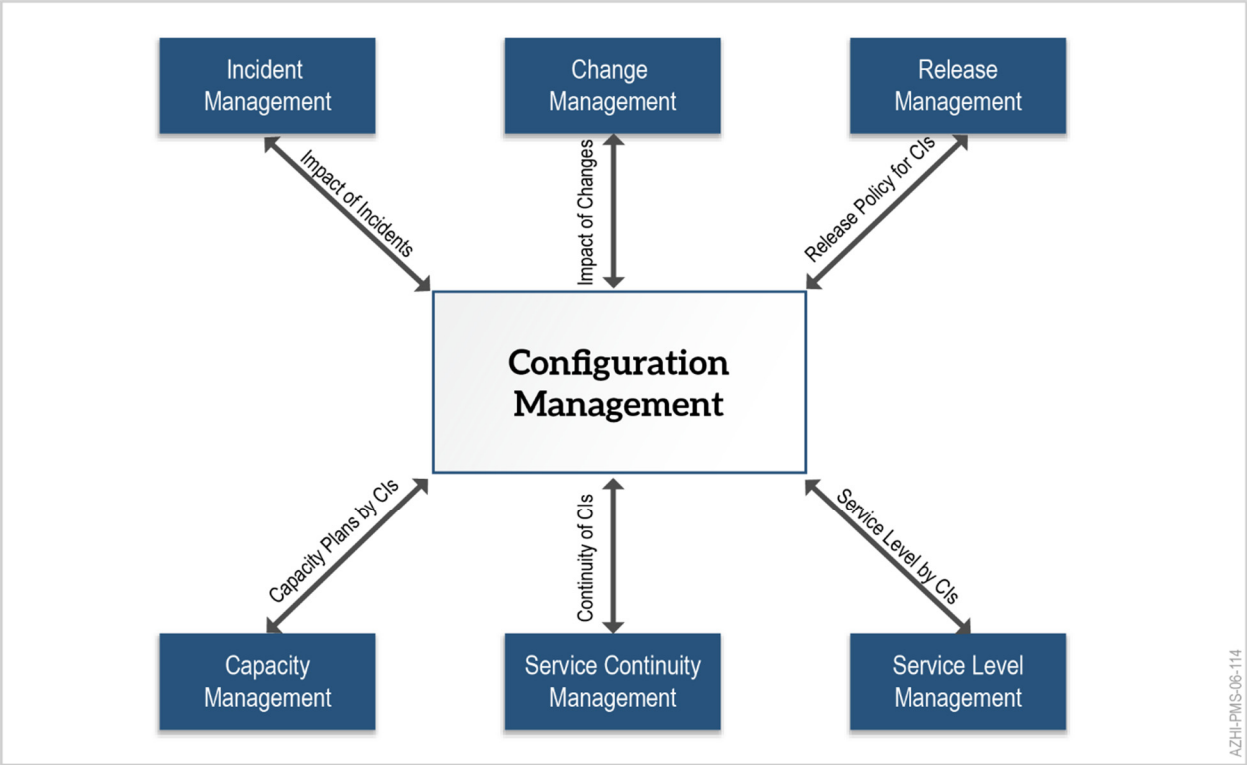


Figure A.6.4-21. Configuration Management as part of ITIL Framework. CNSI's approach to Configuration Management provides a holistic view across all ITIL service areas.

A brief description of all the various ITIL Process areas interacting with the Configuration Management process area is listed in Figure A.6.4-22.

ITIL Process Area	Brief Description
Incident Management	Incident Identification, Incident logging, Categorization and Prioritization, Resolution, Closure and Communication to all the stakeholders at a high-level.
Change Management	Planning and Tracking a change to a Configuration Item to meet the defined business requirements at a high level
Release Management	Planning, Preparing, Scheduling, and Deployment/Distribution of a release content to meet the business requirements. Controls and Checks defined as part of Configuration and Change Management guide the Release activities
Capacity Management	Ensuring that the IT infrastructure can provide IT services at the agreed Service Levels in the most efficient and optimum manner feasible
Service Continuity Management	Managing risks that might adversely affect the performance of IT Services disrupting business continuity
Service Level Management	Designing, Monitoring and Reporting on the service levels to make sure that agreed to Service Level Agreements are being met

ITIL Process Area	Brief Description
Configuration Management	Tracking all of the individual configuration items that would contribute towards building and maintaining an IT solution to meet the defined business requirements

Figure A.6.4-22. ITIL Process Areas. Brief description of each process area that interact with Configuration Management.

CNSI's Software Configuration Management (SCM) methodology is based upon the following terms:

- Configuration Item (CI): Defined as any artifact that needs to be managed to deliver an IT service; it can be a hardware artifact, source code artifact, software artifact, document or an IT service.
- Baseline: Defined as a snapshot of the CI or set of CIs frozen and recorded at a point of time; it can be used to restore an IT service to a given state should something go wrong or as a reference point for any change that might be required.

Figure A.6.4-23 summarizes the tools that will be used for each of the ITIL Process areas.

ITIL	Tools
Incident Management	Open Ticket Request System (OTRS)
Change Management/Configuration Management	As-One/JIRA/ iTOP
Release Management	Subversion/JIRA/As-One/MW Ops Portal
Capacity Management	HealthBeat
Service Continuity Management	HealthBeat/SLA Monitoring
Service Level Management	HealthBeat/SLA Monitoring

Figure A.6.4-23. Implementation tools by ITIL Process Areas. CMDB by each ITIL area is listed.

A.6.4.5 Storage Requirement Capacity Estimates [SOW, Section 5.4.7]

CNSI's evoBrix PMIS solution is highly scalable and supports multiple environments starting from Development to Production. Every environment mentioned below supports concurrent sessions and applications necessary to perform parallel concurrent processing. The environment topology along with the purpose and capacity estimates for Storage Area Network (SAN) and Network Attached Storage (NAS) is listed in Figure A.6.4-24.

Zone	Environment	SAN Reqts (in GB)	NAS Reqts (in GB)	Purpose of the Environment
Build	Build & Deploy	3250		This environment contains Applications, Tools, and Utilities that are required to perform Build, Deploy, Versioning, Modelling, Design, IDE, and Development functions.
Development/Test/ Stage/DR	Development	2550		Used for Development purposes. Contains de-identified data. No PHI/PII data is present here.
	System Test	2550		Used for Unit testing and System Testing purposes by CNSI's testing team to support operational releases. Contains de-identified data.
	UAT	2550		User Acceptance Testing is performed here by business users to support Operational Releases.

Zone	Environment	SAN Reqts (in GB)	NAS Reqts (in GB)	Purpose of the Environment
	Regression	2550		This is a Production Patch Environment and it support Emergency Operational Releases.
	Conversion	950	500	This environment is used for Data Conversion activities.
	Training/Outreach	2550		This environment is used for Training purposes ("Train the trainer").
	Disaster Recovery/ Performance	10800	10300	Standby Environment that will become active during a disaster. When not active, this environment will become the Performance test environment and load test is performed in this environment before go-live and every major release.
Production	Production	6900	10300	Production environment.

Figure A.6.4-24. Environment Topology. List of all environments in CNSI's evoBrix PMIS solution along with their capacity estimates for storage requirements

A.6.4.6 Support for SOA- and ESB-based System [SOW, Section 5.4.8]

The evoBrix's ISR solution, as shown in Figure A.6.4-25, uses an enterprise class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations.

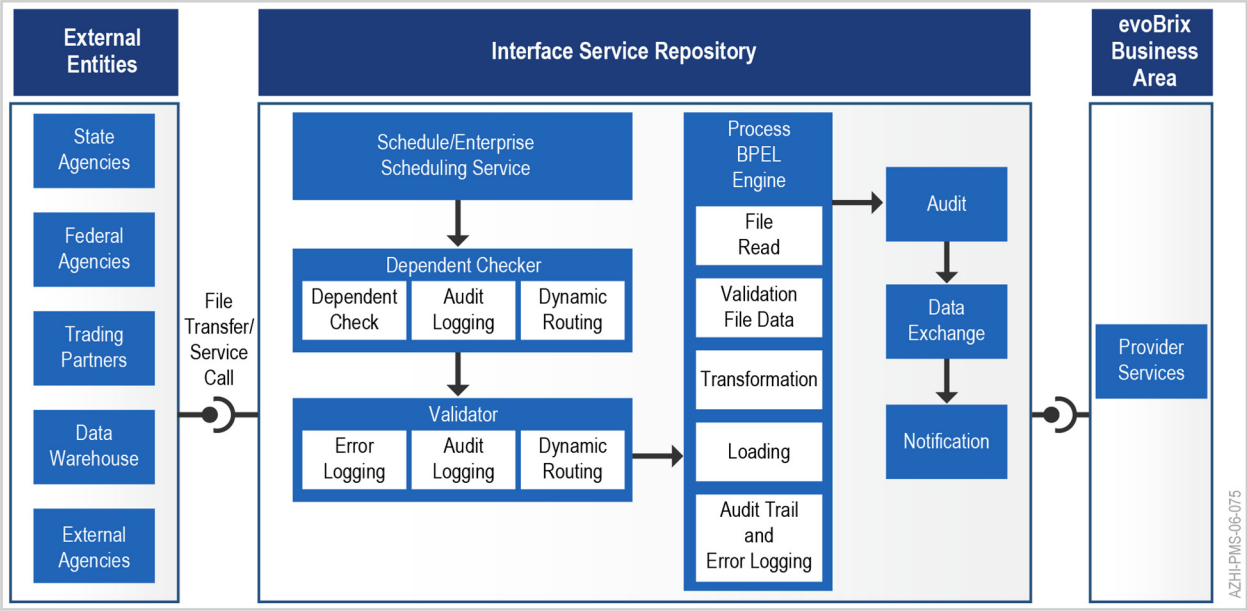


Figure A.6.4-25.The evoBrix ISR Solution.

A.6.4.7 Changes to Licensed Software [SOW, Section 5.4.13]

Following types of Configuration Items (CIs) are defined for the overall System. The criteria for configuration identification include the following:

- The item will be used by one or more groups
- The item is expected to change over time due to defects logged or enhancements

- The item is either dependent on another item or triggers a change in other items because of a change in this one
- The item is critical to the project

Figure A.6.4-26 lists the various types of CIs that exist on the project.

Type of CI	Description
Source Code	Project source code
Status Records	Records in JIRA or As-One providing a snapshot of the CI status
Document	Documents created as part of project activities
Hardware	Servers and routers that help implement the project activities

Figure A.6.4-26. Types of CIs. Lists the types of CIs that will be tracked for the entirety of AHCCCS solution.

Each CI is stored in its respective Configuration Management Database (CMDB) as shown Figure A.6.4-27, which lists the applicable CMDB for each of the CIs in the system. Any change to a CI generates an audit trail.

Name	Type of CI	Repository	Configuration Control Trigger
Java, JSP, XML, JS, PL/SQL, SQL, CSS, HTML, Images	Source code	Subversion	Initiation of the project
Source Code Defects/Enhancement Requests	Status Records	JIRA	Submission to State
Formal Document Deliverables, as defined in the Project Work Plan	Document	As-One	Submission to the State
Servers, Routers, Switches	Document	iTOP/Wiki	Initiation of the Project
Non-Contract Deliverables, as defined in the Project Work Plan	Document	As-One	Approval by Delivery Manager/Director

Figure A.6.4-27. Items Under Configuration Management. Lists each type of CI, repository where it will be stored and the phase that the CI will be placed under configuration control.

A.6.4.8 Plans/Procedures for Meeting Audit/Compliance Requirements [SOW, Section 5.4.14]

Figure A.6.4-28 shows a sample table of contents produced through CNSI's certification planning process.

Table of Contents

1. Introduction 1
1.1 Document Purpose 1
1.2 Document Organization 1
1.3 Reference to Other Documents 2
1.4 Audience 2
2. Certification Overview and Assumptions 7
2.1 Certification Definition 7
2.2 Relationship between Certification Plan and MECT 8
2.3 Roles and Responsibilities 8
3. Certification Approach and Methodology 9
3.1 Draft and Final Certification Plan 9
3.2 The Process 9
3.2.1 Initial Assessment 9
3.2.1.1 Identification of SCI Certification Stakeholders 9
3.2.1.2 CHAMPS to MITA Crosswalk Evaluation 10
3.2.1.3 Initiating Preemptive Remedation for SCI Phase 11
3.2.2 Activities During SCI 12
3.2.2.1 Managing Crosswalk Updates 12
3.2.2.2 Managing Certification Checklist Reevaluation 13
3.2.2.3 Pre-implementation Certification Readiness Review 14
3.2.2.4 Establish the Certification Evidence Repository 15
3.2.3 Preparation for formal Certification Request 16
3.2.3.1 Identify Critical Success Factors 16
3.2.3.2 Commission Certification Team 17
3.2.3.3 Construct Initial Certification Schedule 17
3.2.3.4 Conduct Certification Team Orienation 18
3.2.3.5 Data Collection, and Monitoring 18
3.2.3.6 Perform Periodic Progress Reporting 19
3.2.3.7 Conduct Certification Readiness Review 19
3.3 Request to CMS for Certification Review 20
3.4 Review Preparation 20
3.5 CMS Certification Review 21
3.6 Certification Disposition 22
3.6.1 Potential Remediation Activity 22
3.6.2 Final Certification Disposition 22
4. Appendices 23
4.1 Appendix A – Acronyms and Terms 23
4.2 Appendix B – Deliverable Acceptance Criteria 24

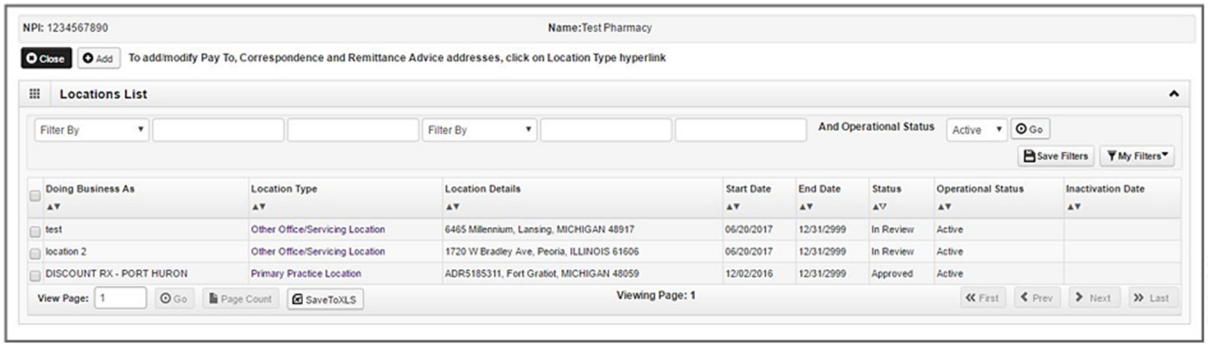
AZHI-PMS-06-167

Figure A.6.4-28. Table of contents produced through CNSI's certification planning process.

A.6.5 Determine Provider Eligibility [SOW, Section 5.5]

A.6.5.1 Single Provider Enrollment of Multiple Locations [SOW, Section 5.5.1]

Providers can be tied to only one primary practice location, but the additional locations for that provider can be added as "Servicing Locations." Each Servicing Location will be of a specific address type such as "Location," "Pay To," "Correspondence," or "Remittance Advice." Figure A.6.5-1 and Figure A.6.5-2 depict this capability.



AZHI-PMS-06-155

Figure A.6.5-1. Multiple Provider Locations. Allows a provider to be associated with more than one location.

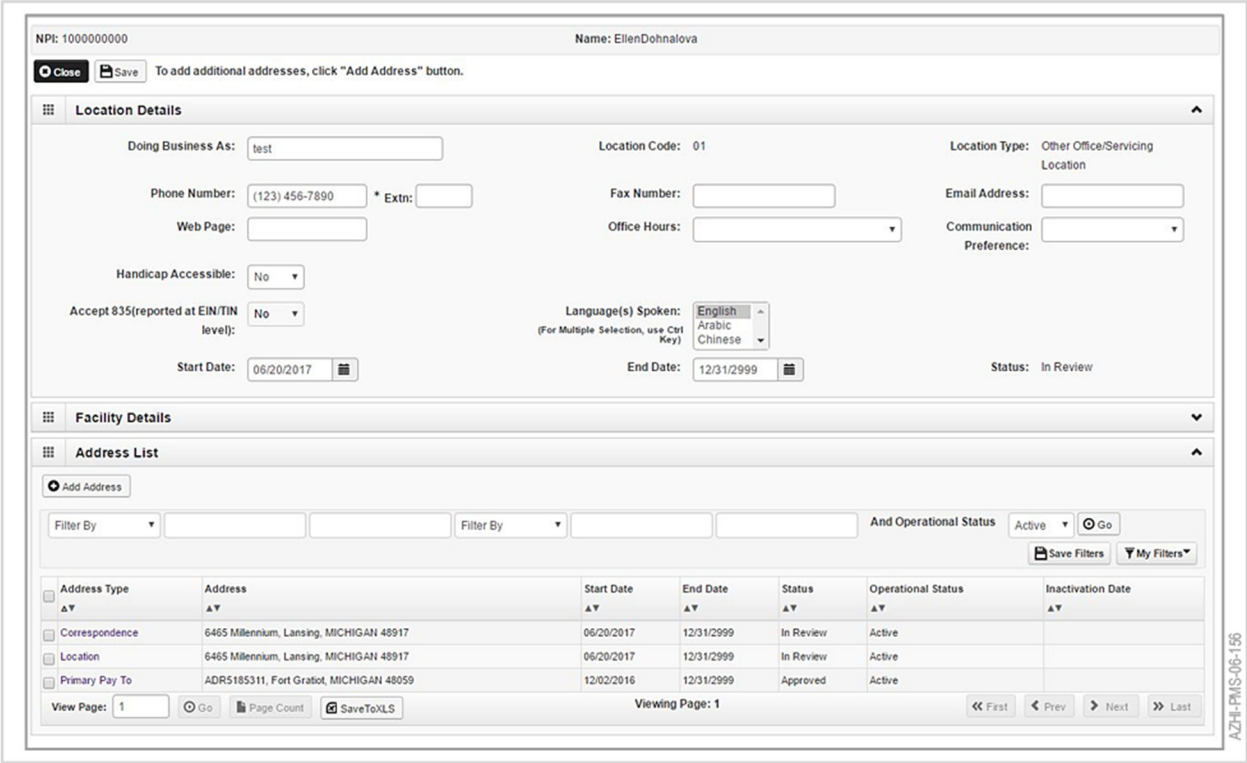


Figure A.6.5-2. Provider Location Details. Displays the different addresses tied to a specific provider location.

A.6.5.2 Optional Configuration for Single Provider to Register Multiple NPIs [SOW, Section 5.5.4]

The evoBrix PMIS provides the option to configure multiple NPIs for the single provider Tax Identification Number (TIN), as shown in Figure A.6.5-3

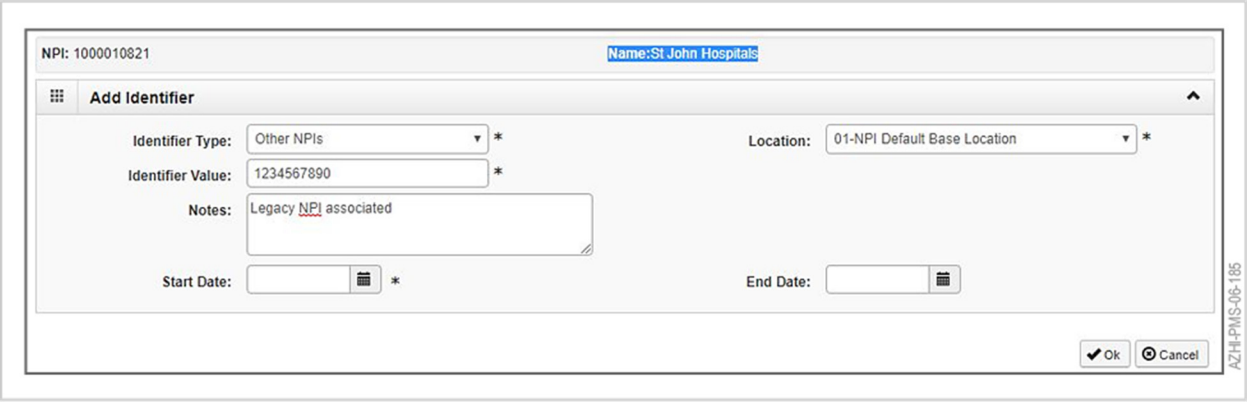


Figure A.6.5-3. Optional Configuration for Single Provider to Register Multiple NPIs. The association page shows the multiple NPIs to a single provider.

A.6.5.5 Collect/Maintain Information Needed to Complete Provider Enrollment [SOW, Section 5.5.5]

The decision management framework in evoBrix PMIS includes features that allow authorized users to perform the following activities:

- Define State-specific provider type and specialty/subspecialty combinations
- Configure mandatory, optional, and conditionally mandatory enrollment and re-enrollment data requirements by provider enrollment type and specialty

- Define and configure credentialing and re-credentialing rules for each unique provider type and specialty combination.

In evoBrix PMIS, business rules for provider management use the following tools to cover three broad areas:

- Permissions Matrix – To define the specialties the State supports under different administrations/programs
- Credentialing Matrix – To define specific credentials, such as licensing, required by the successful applicant for each defined enrollment type/specialty combination
- Rule Composer – To define the enrollment steps needed for each category of enrollment

evoBrix PMIS uses the flexible and comprehensive RuleIT Rule Composer to allow users to define the enrollment rules for each enrollment type and Provider Type/Specialty/ Subspecialty. Authorized users can use the Rules Composer to define each step of the enrollment process and the data elements that are required in determining a step to be complete under a given enrollment type.

The evoBrix PMIS BPW uses State-specific rules in the RuleIT rules engine functions to designate steps as required or optional dynamically depending on data entered by the provider for a given enrollment type based upon the configurable Permission Matrix and Credentialing Matrix. The wizard also displays validation error messages throughout the data entry process. These interactive messages alert the provider to conditions that need to be corrected so that validated and complete data is captured prior to submission.

A.6.5.6 Provider Eligibility [SOW, Section 5.5.6]

Provider eligibility maps to Active or Inactive/Closed or Deceased status, and provider eligibility cannot be directly updated by providers. When the enrollment is approved, the provider eligibility is automatically determined by the dates in the Business Status screen, as shown in Figure A.6.5-4.

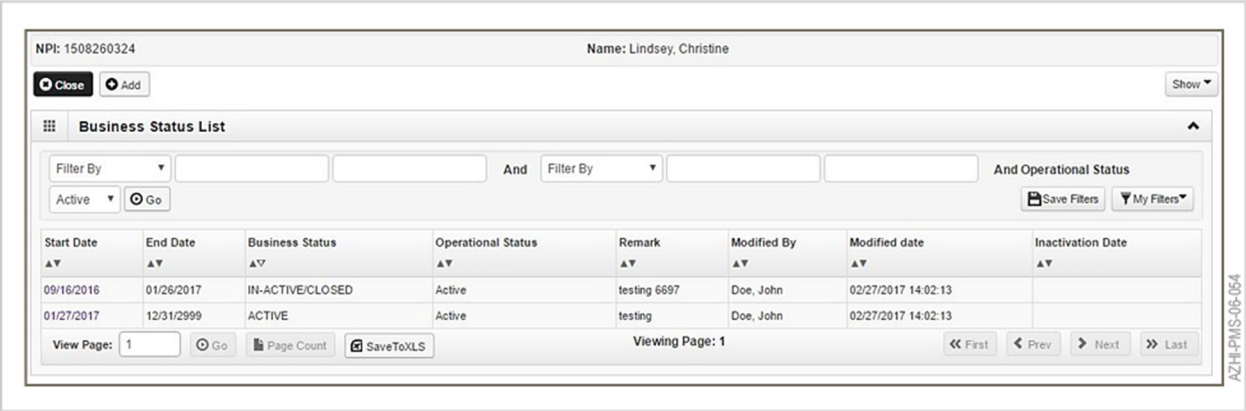


Figure A.6.5-4. Business Status Screen. The business status of a provider determines eligibility.

A.6.5.7 Identification of Provider by CMS Risk Levels [SOW, Section 5.5.14]

Prior to completing enrollment processing, providers are subject to screening tasks based on their risk category. The screening requirement includes:

- Validation of disclosed individuals with the Office of Inspector General (OIG) Excluded
- Individuals database, the Excluded Parties List System (EPLS) and the Social Security Death
- Master List
- In-state and out-of-state professional license verification
- Clinical Laboratory Improvement Amendments (CLIA) and Drug Enforcement
- Administration (DEA) Certification verification
- Proof of Medicare enrollment, if Medicare-enrolled

- REQ Number Detailed Requirements Enrollment SaaS / COTS / Both
- Validation of the NPI with the National Plan and Provider Enumeration System (NPPES)
- All providers classified as “High” and “Moderate” are subject to unscheduled and unannounced site visits. Periodic site visits are also required when existing providers re-validate their information with the timing based on the risk categorization

A.6.5.8 Convert Existing Providers into a New Provider Type [SOW, Section 5.5.20]

The first step in this process will be to perform a Source Data Discovery to identify and account for all historical/active data sources for the Provider Enrollment and Management functional area that is of relevance to the conversion effort. The next step will involve the conversion mapping exercise to map the source data elements to the equivalent target system’s data elements to ensure that every subject area within the evoBrix PMIS solution is fully accounted for. After the finalization of the Conversion Data Mapping, the CNSI’s Data Conversion team will work with the States to finalize the data layouts to facilitate the receipt of the source system’s data for iterative data conversion development needs in a prescribed format that is to be sent on an established basis (weekly/monthly/ad hoc). The provider data will be put through a series of iterative conversion runs to consolidate, analyze, transform, and migrate the data over to the target/new solution.

CNSI’s Data Conversion process is designed to be repeatable and scalable along with extensive support for a robust exception handling, reconciliation, and a reporting framework to provide a comprehensive picture of not only the final conversion data outcome but also the quality of the converted data and/or suggest the necessary corrective actions to make it operationally fool-proof and functional.

A.6.6 Enroll Provider [SOW, Section 5.6]

A.6.6.1 Support Multiple Provider Enrollment Designations [SOW, Section 5.6.1]

The available statuses are In Process, In Review, Denied, and Approved, as shown in Figure A.6.6-1 for provider enrollment status.

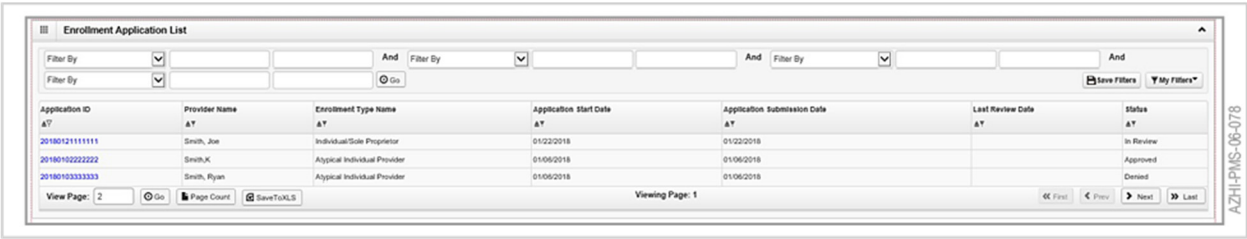


Figure A.6.6-1. Provider Enrollment Status. Allows authorized user to maintain and track enrollment status designations.

Once the enrollment is approved, the system maintains the provider enrollment business status designations, including active, inactive/closed, and deceased, as shown in Figure A.6.6-2.

Figure A.6.6-2. Provider Enrollment Business Status. Allows authorized user to maintain the business status designations after the enrollment is approved.

A.6.6.2 Support Multiple Payment Modalities [SOW, Section 5.6.2]

Figure A.6.6-3 displays the provider fee payment maintenance screen for a provider.

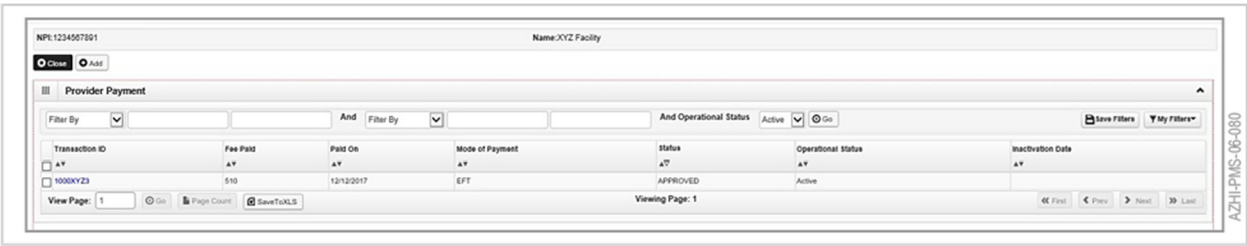


Figure A.6.6-3. Fee Payment Maintenance. Provider Payment Screen tracks and maintains the provider payments. The authorized user will be able to see the history of payments made by the provider in evoBrix PMIS.

A.6.6.3 Support and Notify Provider for Revalidation [SOW, Section 5.6.3]

The revalidation process for a provider is considered as a revalidation cycle in evoBrix PMIS. The revalidation cycle has a start date and due date. evoBrix PMIS sets the revalidation cycle based on the revalidation interval defined for the provider. Each revalidation cycle has well-defined statuses that specify each stage of the revalidation cycle. evoBrix PMIS automatically sets the status of the revalidation at each stage of the revalidation cycle.

Not Started – This is the initial status. This status is set during creation of the revalidation cycle. The first revalidation cycle is created during the approval of new enrollment, and the subsequent revalidation cycles are created during the completion of the current revalidation cycle.

Open – evoBrix PMIS sets the status from "Not Started" to "Open" at the beginning of the revalidation cycle. This status allows the providers to start their revalidation via a self-service portal.

In Review – evoBrix PMIS sets this status when the revalidation is submitted by the provider for the authorized user to review. This status allows the authorized user to start the revalidation review process.

Completed – This is the final status that indicates that the revalidation life cycle has been completed. evoBrix PMIS sets this status when the revalidation review has been completed and a final decision has been made. evoBrix PMIS creates the next revalidation cycle as "Not Started" upon completion of the current cycle.

Terminated – This is the final status that indicates the revalidation life cycle has been terminated because the provider did not complete the revalidation by the revalidation due date.

A.6.7 Disenroll Provider [SOW, Section 5.7]

A.6.7.1 Configurable Business Rules [SOW, Section 5.7.1]

Using RuleIT, which features English-like syntax, a predefined Medicaid dictionary, and standard Medicaid edits and processing flows, evoBrix PMIS has a configurable list of built-in rules to set indicators and flag the enrollment based on a set of restrictions imposed by AHCCCS/Med-QUEST system. RuleIT's flexible architecture allows a business analyst to determine the sequence of rule evaluation, which simplifies setting up the processing chain more manageably - whether it is a single rule or a series of complex process flow rules. Based on this approach, the system is capable of automatically suspending or restricting the enrollment by end dating the eligibility of the enrollment according to the screening results. The list below includes the screening checks performed by the system:

- State/Federal Death Verification
- Sanctions
- OIG Sanctions

- General Services Administration (GSA) Exclusion list (EPLS/SAM)
- License Board Sanctions
- NPI Verification
- SSN, EIN/TIN Verification
- National Council for Prescription Drug Programs (NCPDP) Verification
- License/Certification Verification
- In/Out-of-state professional license
- DEA, CLIA, Board Certification Verification with American Board of Medical Specialties
- Criminal History and Sex Offense Check (Child/Elder/Adult Abuse, Sex Offender)

A.6.8 Inquire Provider Information [SOW, Section 5.8]

A.6.8.1 Search Capability [SOW, Section 5.8.1]

As shown as in Figure A.6.8-, the page has three main filters, which are used to drill down on primary provider attributes. There are two additional filters, which are used to filter on provider identifier and indicators. The system also provides the capability to sort the results by chronological order. This is achieved by clicking on the Date columns. evoBrix PMIS system will sort the results

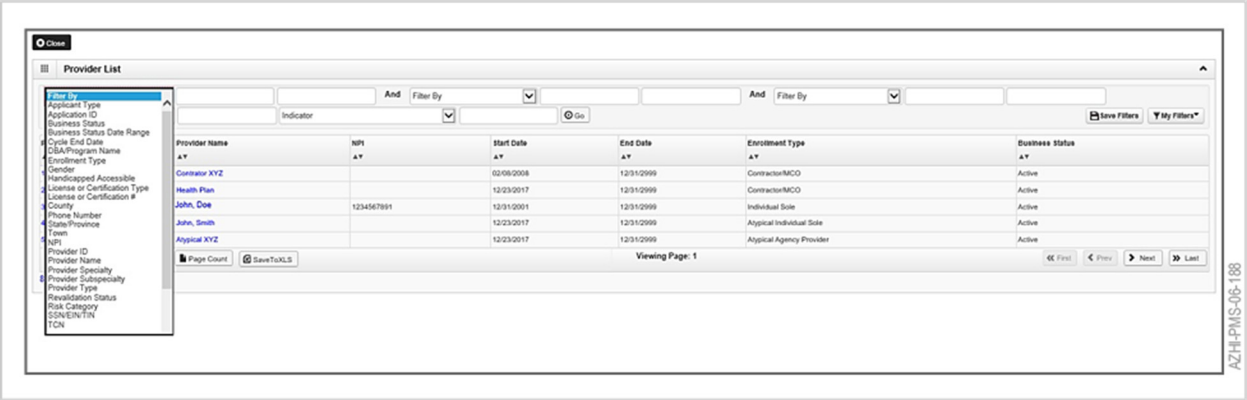


Figure A.6.8-1. Provider List. The provider list page provides filter and sort capabilities on the screen.

A.6.8.2 Query Capability [SOW, Section 5.8.2]

The naming conventions and standards include the following:

- Package which represents the objects that could be used to provide query capabilities in the ad-hoc report
- Query Subject which represents an entity (table) in the evoBrix PMIS solution data mart
- Query Item which represents the attributes (columns/business elements) of an entity (table) in the evoBrix PMIS solution data mart

Users can simply drag and drop the business elements required into their workspace to create their own customized ad hoc report for data inquiry. Due to the granular nature of data storage in OLTP, reports can be created at different aggregation levels (detail or summary) tied to various dimensions. The ad hoc reporting provides the user with the flexibility to create their own customized reports. They can also execute, generate the query or report, and save it in various formats, including HTML, Excel, CSV, and PDF.

Figure A.6.8-2 shows a sample ad hoc report generated in Excel format.

Report Date: 02/01/2018 9:00:01 AM

evoBrix PMIS

Provider Primary Care Report – Board Eligible

Page: 1

Start Date : 02/01/2018 End Date : 02/01/2018

ProviderID	NPI	Provider Name	Business Status	Business Status Start Date	Business Status End Date	Board Eligible	Board Eligible Start Date	Board Eligible End Date
7987087	8997989825	Provider Name	Active	04/29/2014	04/01/2021	98985	07/01/2017	02/15/2018
7687667	6979879898	Provider Name	Active	03/05/2015	08/30/2018	88767	12/04/2009	02/26/2018

AZHI-PMS-06-025

Figure A.6.8-2. Provider Primary Care - Board Eligible Ad hoc Query Report. The report lists the providers who are Board Eligible.

A.6.8.3 Search by Licensure [SOW, Section 5.8.3]

As shown in Figure A.6.8-3, the Provider List displays the license search results in an exportable grid.

Figure A.6.8-3. Provider List with License or Certification number search.

A.6.9 Manage Provider Information Supplemental [SOW, Section 5.9]

A.6.9.1 Support Real-time Edits [SOW, Section 5.9.1]

shows field level edits in the Basic Information screen, which guides providers in completing required information for the enrollment process.

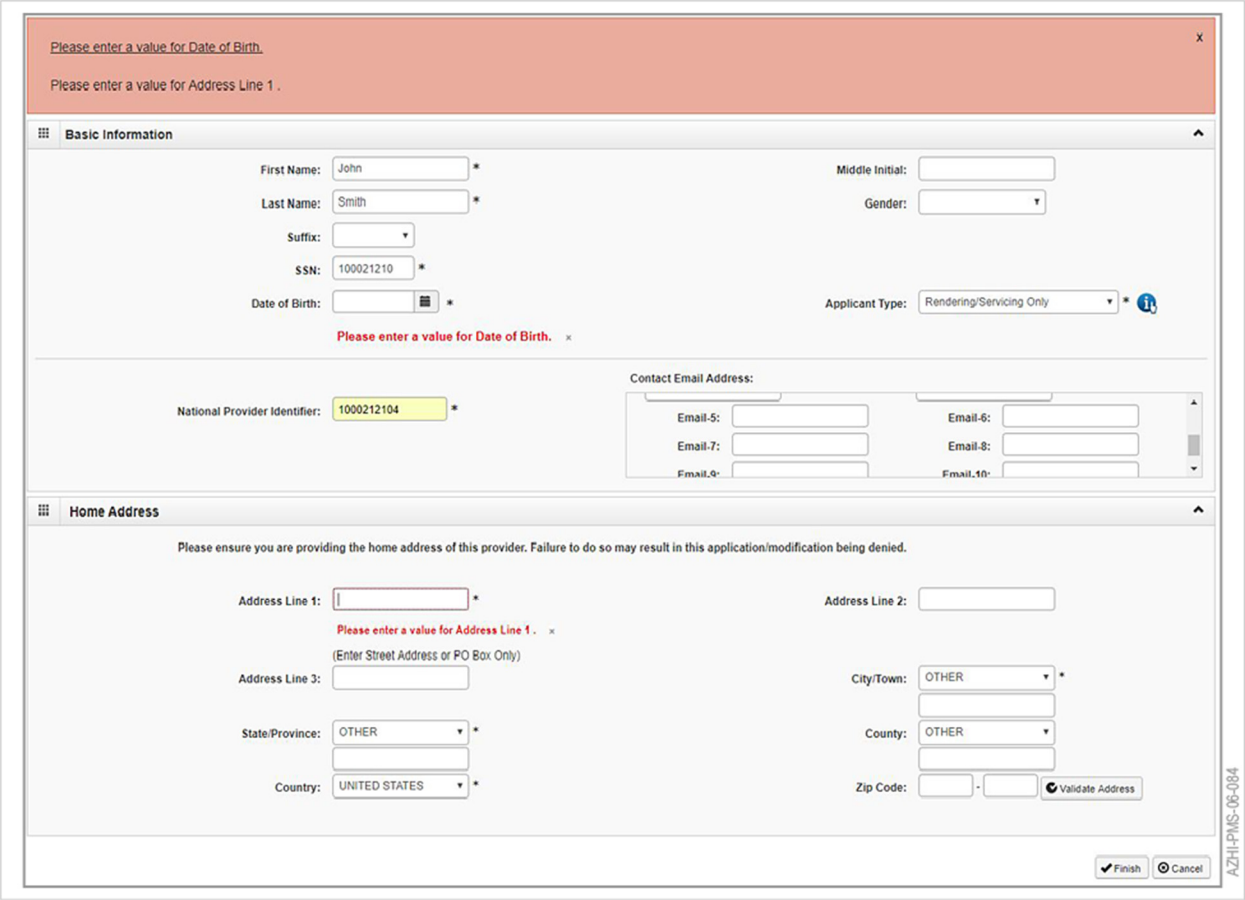


Figure A.6.9-1. Support Real-time Edits. System supports real time edits to check the validity and completeness of the data entered by the user.

A.6.9.2 Maintain Provider's Effective Date [SOW, Section 5.9.2]

Figure A.6.9-2 shows the enrollment approval screen where state staff can pick an effective enrollment start date at the time of approval.

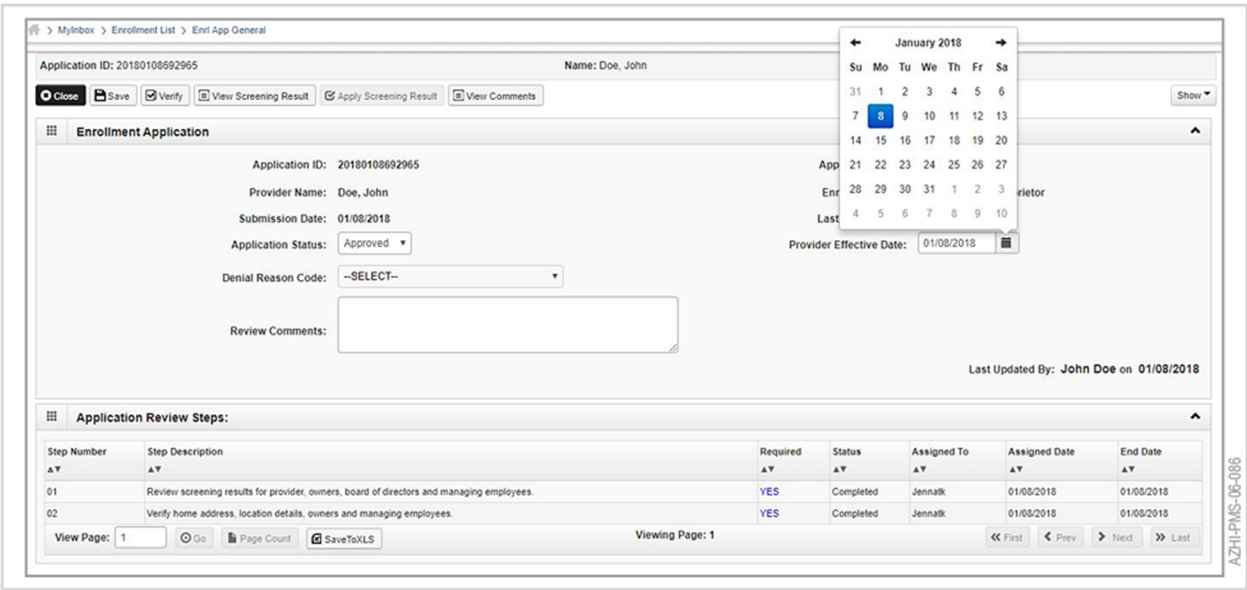


Figure A.6.9-2. Maintain Provider's Effective Date. State staff can pick a data from for effective enrollment date at the time of enrollment approval.

A.6.9.3 Allow Providers to Update Profile Information [SOW, Section 5.9.4]

As shown in Figure A.6.9-3, the provider can update profile information but the system restricts any updates to NPI and SSN.

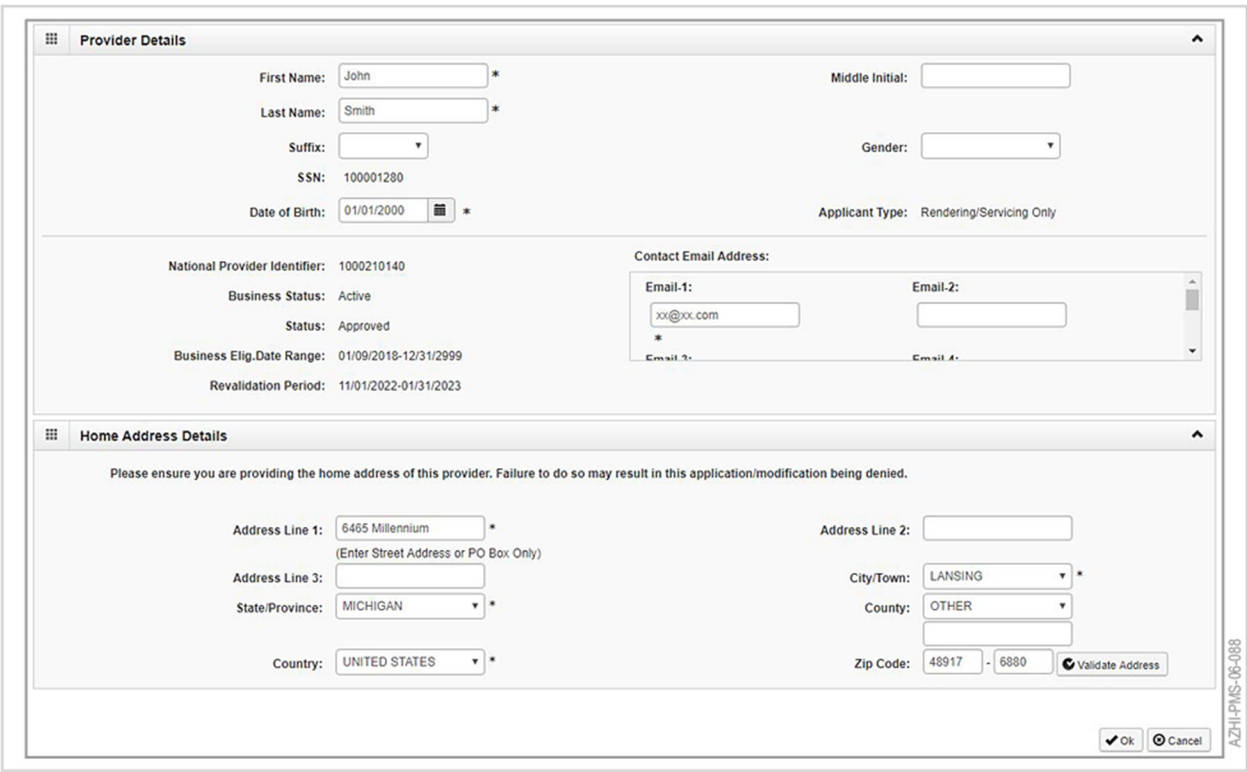


Figure A.6.9-3. Allow Providers to Update Profile Information. Providers can update their demographic data but NPI and Tax ID cannot be updated.

A.6.9.4 Notify Provider and CMS if State Applies for Exclusion Policy [SOW, Section 5.9.5]

Figure A.6.9-4 and Figure A.6.9-5 show the state staff ability to generate on demand notifications based on a predefined template and the ability to edit the content based on the notification type.

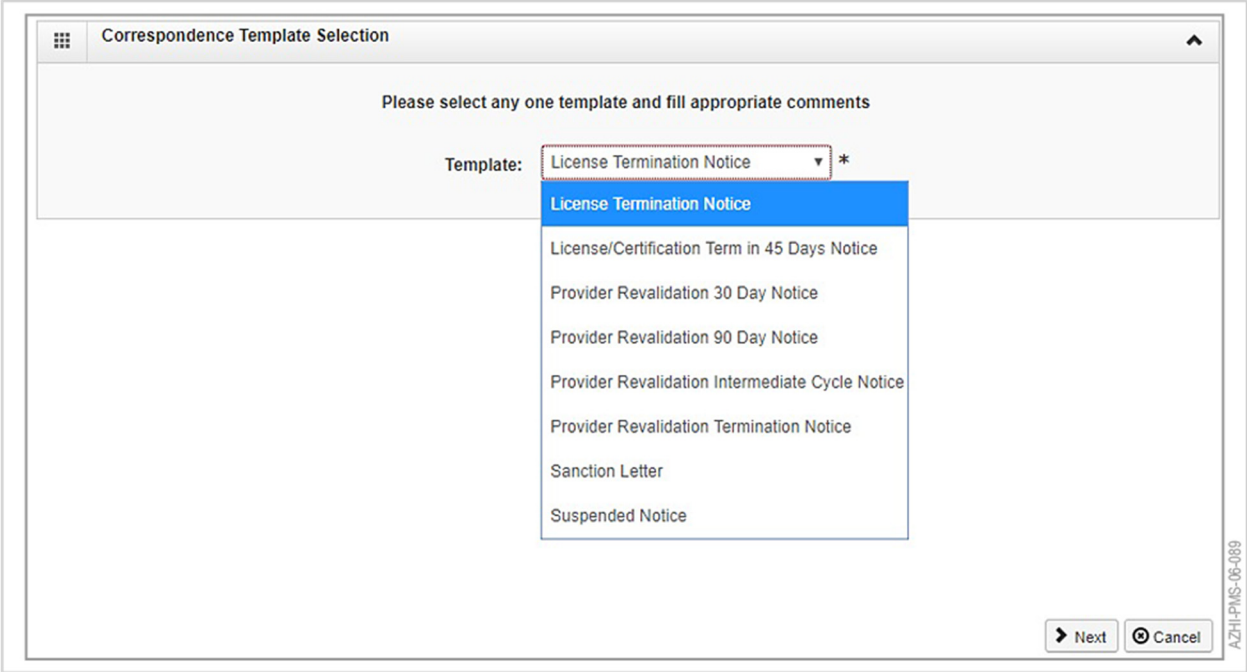


Figure A.6.9-4. A Notify Provider and CMS if State Applies Exclusion Policy shows the state staff's ability to generate a sanction letter for correspondence.

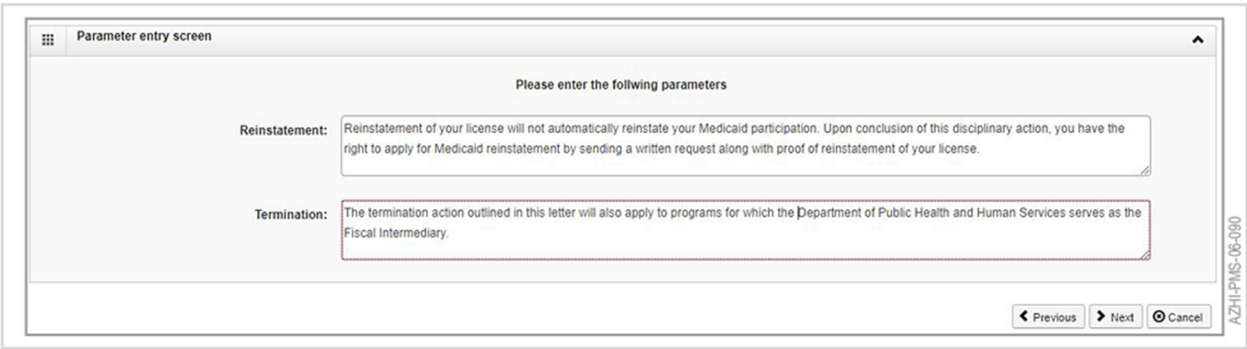


Figure A.6.9-5. Notify Provider and CMS if State Applies Exclusion Policy shows the state staff's ability to edit the notification content before sending it out.

A.6.9.5 Assign Case or Tracking Number for Submitted Documents [SOW, Section 5.9.7]

Figure A.6.9-6 and Figure A.6.9-7 show how a Document ID is created as a tracking number for the uploaded document to allow AHCSS/Med-QUEST to track and/or search for pending documents.

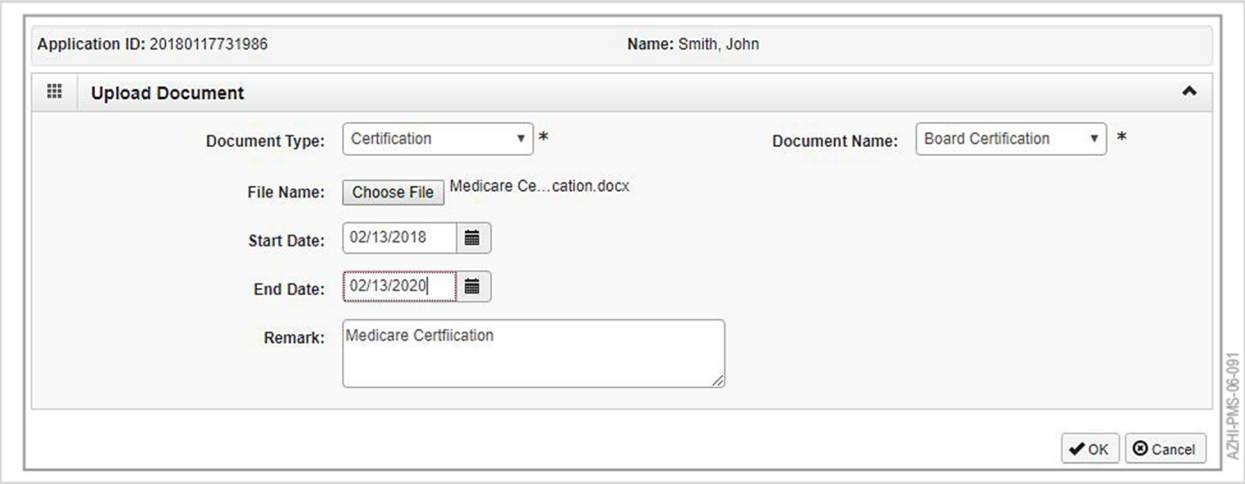


Figure A.6.9-6. Assign Case or Tracking Number for Submitted Documents shows upload document step where provider can upload a document.

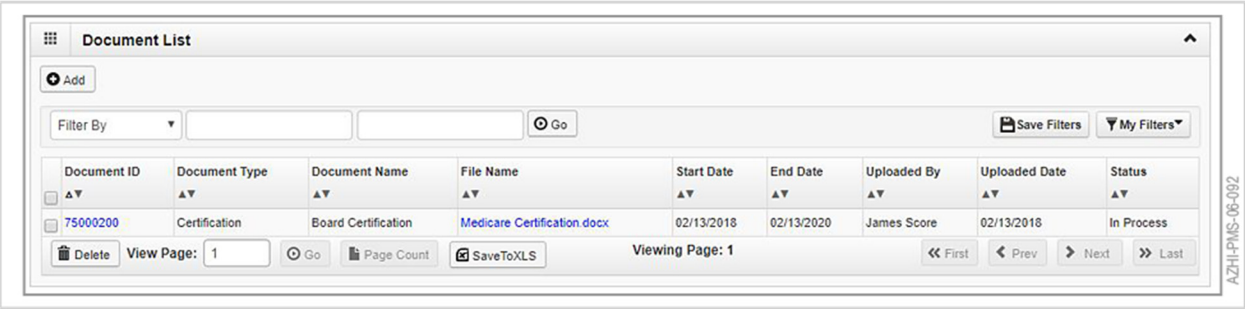


Figure A.6.9-7. Assign Case or Tracking Number for Submitted Documents shows the document ID which is created after a document is uploaded.

A.6.9.6 Automatically Flag Previously Researched Providers [SOW, Section 5.9.8]

Figure A.6.9-8 shows the list of providers who were flagged as Deceased by the State Vital File and Figure A.6.9-9 shows the providers who were flagged for any sanctions by the State.

Provider List

Business Status | DECEASED | And | Filter By
And | Filter By | Identifier
Date of Death Verified Source | State% | Go | Save Filters | My Filters

Provider ID	Provider Name	DBA/Program Name	NPI	Start Date	End Date	Enrollment Type	Business Status	Date of Death Verified Source
8353117	Alivnvla, Pielebob			12/05/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8313533	Samerng, Heetlam			10/17/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8284216	Ioantdr, Kivenny			12/04/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8283854	Eziyakub, Orsayoz			11/30/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8250263	Lizzrog, Kalahfaw			11/25/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8248194	Jorgahba, Nullefk			08/22/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8216987	Anziole, Jaleioh			09/28/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8202319	Gayelho, Wayonerz			12/05/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8198996	Shasazka, Odbypez	2498 e. ellis rd.		07/12/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital
8194693	Roozeehr, Hebamra			09/22/2017	12/31/2999	Atypical Individual Provider	DECEASED	State Vital

View Page: 2 | Go | Page Count | SaveToXLS | Viewing Page: 1 | First | Prev | Next | Last

AZHI-PMS-06-101

Figure A.6.9-8. Automatically Flag Previously Researched Providers who are flagged as Deceased by State Vital.

Provider List

Filter By | And | Filter By
And | Filter By | Identifier
Sanctioned Source | % | Go | Save Filters | My Filters

Provider ID	Provider Name	DBA/Program Name	NPI	Start Date	End Date	Enrollment Type	Business Status	Sanctioned Source
8379679	Smith, John	NPI Default Base Location	7788722669	01/15/2018	12/31/2999	Individual/Sole Proprietor	Active	SAM (EPLS)
8370083	BARBER, TRISHA		1194819052	01/01/2015	12/14/2017	Individual/Sole Proprietor	Active	LEIE (OIG)
8370083	BARBER, TRISHA		1194819052	12/15/2017	12/31/2999	Individual/Sole Proprietor	In-Active/Closed	LEIE (OIG)
8354965	Williams, Robin		1932416690	08/01/2017	12/31/2020	Individual/Sole Proprietor	Active	LEIE (OIG)
8070775	Yavinlab, Damyakuc			09/19/2016	02/20/2017	Atypical Individual Provider	Active	HHS
7999393	Lumirvaz	Tri-County Physician Group PC	1386942035	02/07/2017	12/31/2999	Group Practice (Corporation, Partnership, LLC, etc.)	In-Active/Closed	DCH
7999393	Lumirvaz	Tri-County Physician Group PC	1386942035	06/23/2015	02/06/2017	Group Practice (Corporation, Partnership, LLC, etc.)	Active	DCH
7963130	Ilineenz, Symmshe	NPI Default Base Location	1659555621	03/28/2017	12/31/2999	Individual/Sole Proprietor	In-Active/Closed	HHS
7963130	Ilineenz, Symmshe	NPI Default Base Location	1659555621	04/12/2016	03/27/2017	Individual/Sole Proprietor	Active	HHS
7892904	Eammaka	Shelby Dental Center	1154626687	01/18/2017	12/31/2999	Group Practice (Corporation, Partnership, LLC, etc.)	In-Active/Closed	DCH

View Page: 2 | Go | Page Count | SaveToXLS | Viewing Page: 1 | First | Prev | Next | Last

AZHI-PMS-06-102

Figure A.6.9-9. Automatically Flag Previously Researched Providers who are flagged as Excluded from various sources.

A.6.9.7 Provide Auto-generated Comments Section [SOW, Section 5.9.9]

Figure A6.9-10 demonstrates how evoBrix PMIS saves and maintains all executed actions and updates with comments in the system.

View History

Remark	Created Date	Created By	Modified Date	Modified By	Effective Date	From Date	To Date	Operational Flag	Status Name
Updated Provider Contact Email	02-12-2018 16:12:00	Score,James	02-12-2018 16:12:02	Score,James	02-12-2018 16:12:02	02/12/2018	12/31/2999	Active	Approved
	02-12-2018 16:12:02	Smith,John	02-12-2018 16:12:02	Score,James	11-16-2017 00:00:00	11/16/2017	02/11/2018	Active	Approved
Provider demographic data saved	01-24-2018 10:22:46	Smith,John	02-12-2018 16:12:02	Score,James	11-16-2017 00:00:00	11/16/2017	12/31/2999	Inactive	Approved

View Page: 1 Go Page Count SaveToXLS Viewing Page: 1 First Prev Next Last

Cancel

AZHI-PMS-06-100

Figure A6.9-10. Provide Auto-generated Comments Section shows auto generated comments section and the details of the record update.

A.6.9.8 Identify Discrepancies and Exceptions for Human Review [SOW, Section 5.9.10]

In Figure A.6.9-11 through Figure A.6.9-13, the screens display the state staff ability to find discrepancies at a glance and further research on the information received before making a decision.

Provider Screening Details

Name : RYAN SMITH NPI : 1720338528 SSN : 402259340

Type : Individual ID :8376775

Precision 100

Provider Information | Taxonomy | License | Sanction | Advanced Screening | Ownership | Other License | Additional Information

Field Name	Input Value	Response	Result
Name	RYAN SMITH	Ryan Smith Ryan Smith Jr.	Valid
NPI	1112223334	1112223334	Valid
SSN	111222333	111222333	Valid
EIN/TIN			
Address	2850 Mercer Loop HELENA MT 59602	2850 Mercer Loop Helena MT 59602	Valid

Federal Vital-Death

DOD :

State Vital-Death

DOD : Match Percent : Name :

PECOS Screening

Finger Print : N/A Site Visit : N/A Provider Fee Paid : N/A

Back

AZHI-PMS-06-087

Figure A.6.9-11. Identify Discrepancies and Exceptions for Human Review. The PCS screen displays flags for providers who have sanctions, invalid licenses or Advanced Screening (Criminal & Sex Offense) information.

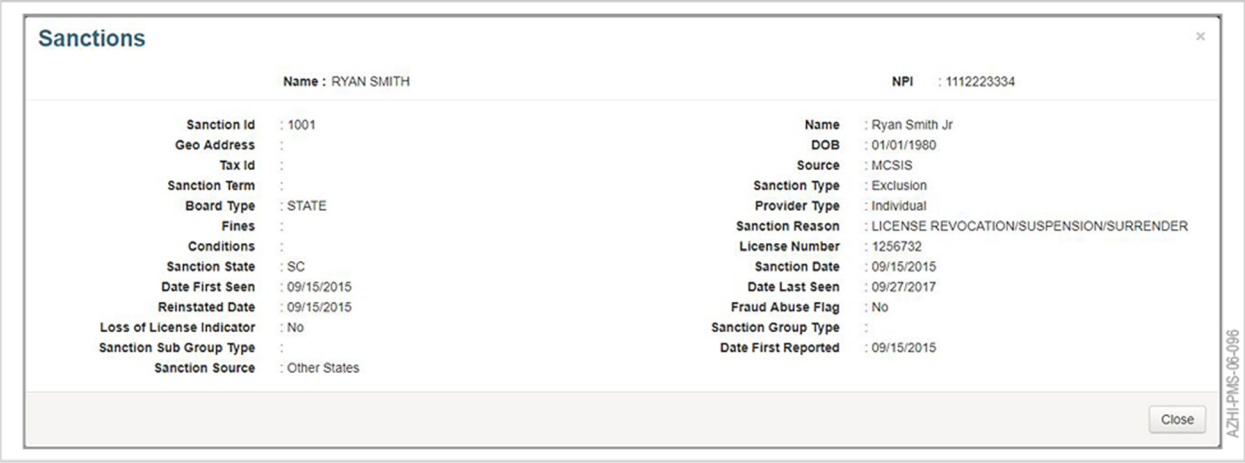


Figure A.6.9-12. Identify Discrepancies and Exceptions for Human Review. PCS Screen displays MCSIS (Medicaid and CHIP State Information System) Exclusion details for state staff to further investigate on this sanction before applying the exclusion on the provider.

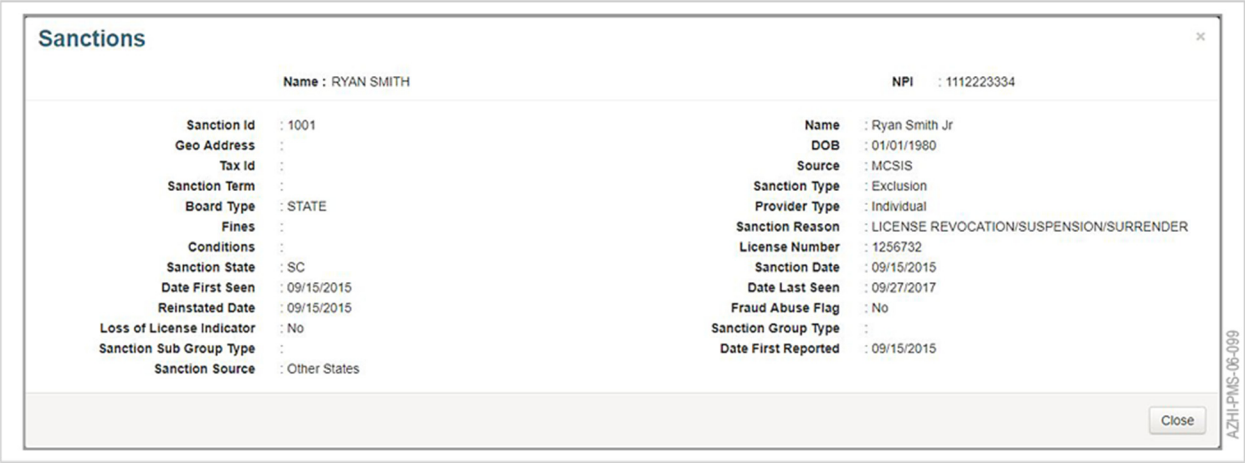


Figure A.6.9-13. Identify Discrepancies and Exceptions for Human Review. PCS screen displays criminal offense details of an individual for state's view for further research.

A.6.9.9 Identify Tribally-owned and Operated Providers [SOW, Section 5.9.11]

Figure A.6.9-14 shows the Specialties screen to which authorized states users can add provider types, such as Tribal Owned and Operated non-IHS/638 and IHS providers. From this screen, providers can select the appropriate type, specialty, and sub-specialty through business process wizards (BPWs) - Specialties step and associate to it.

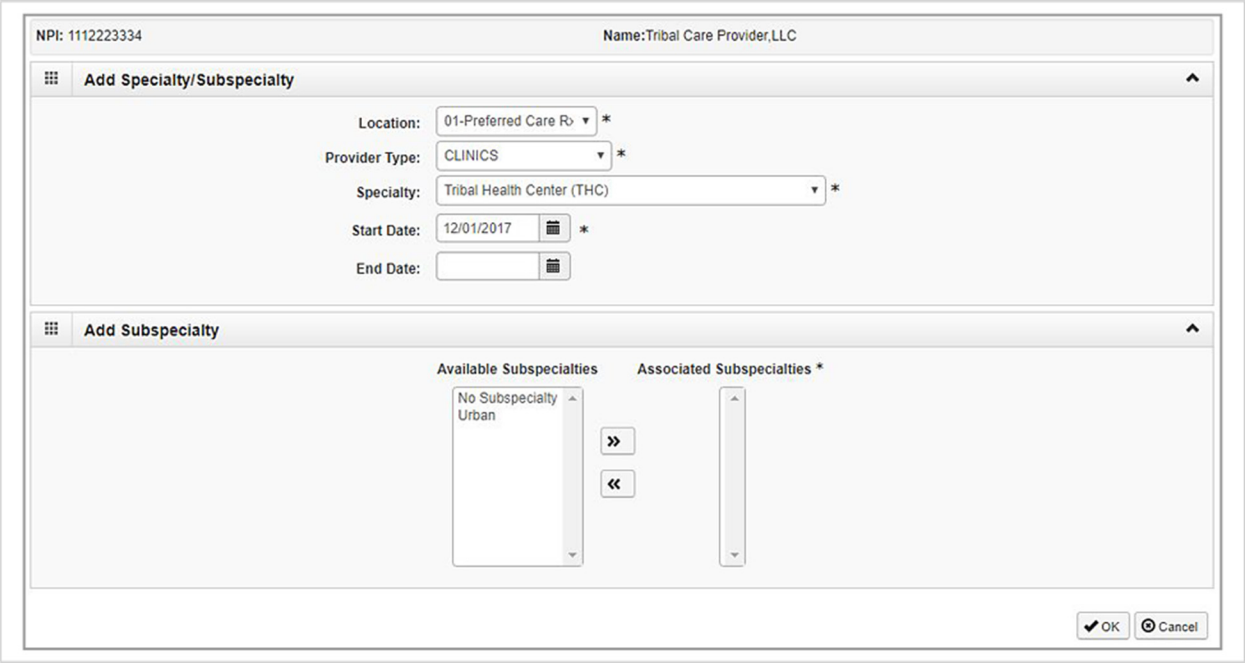


Figure A.6.9-14. Identify Tribally-owned and Operated Providers. Shows screen where providers can select provider type, specialty and subspecialty for Tribal Health Center.

Figure A.6.9-15 shows how State staff can search and identify the providers who have selected Tribal Health Center from the Matrix after a provider has selected the specialty and submits.

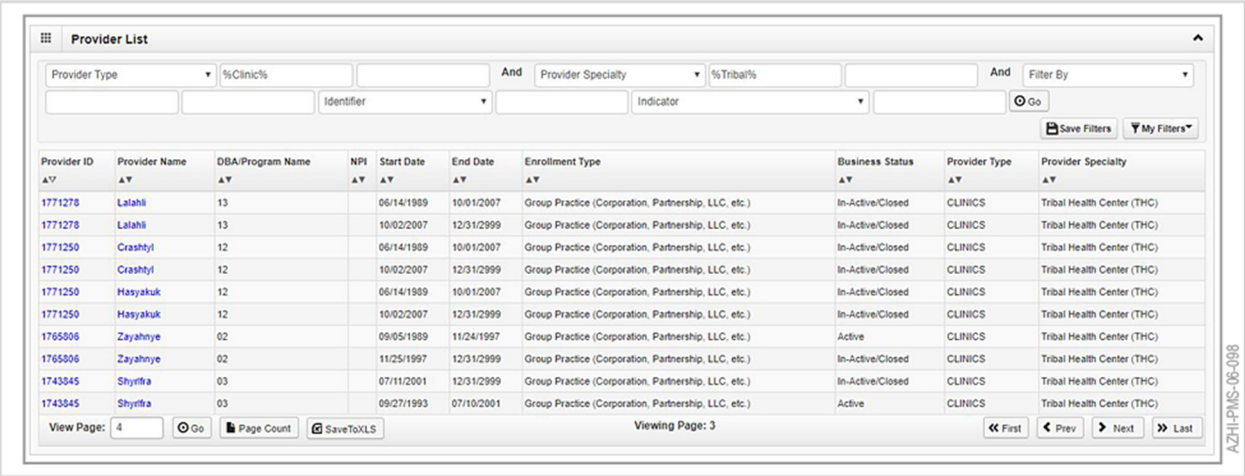


Figure A.6.9-15. Identify Tribally-owned and Operated Providers. State staff can select Tribal owned and operated provider through the list search screen.

A.6.9.10 Identify MCO's Contracted Providers [SOW, Section 5.9.12]

Figure A.6.9-16 shows the "Associate MCO Provider" step, which allows providers to associate to an MCO and Figure A.6.9-17 shows contracted providers to the MCO and State Staff.

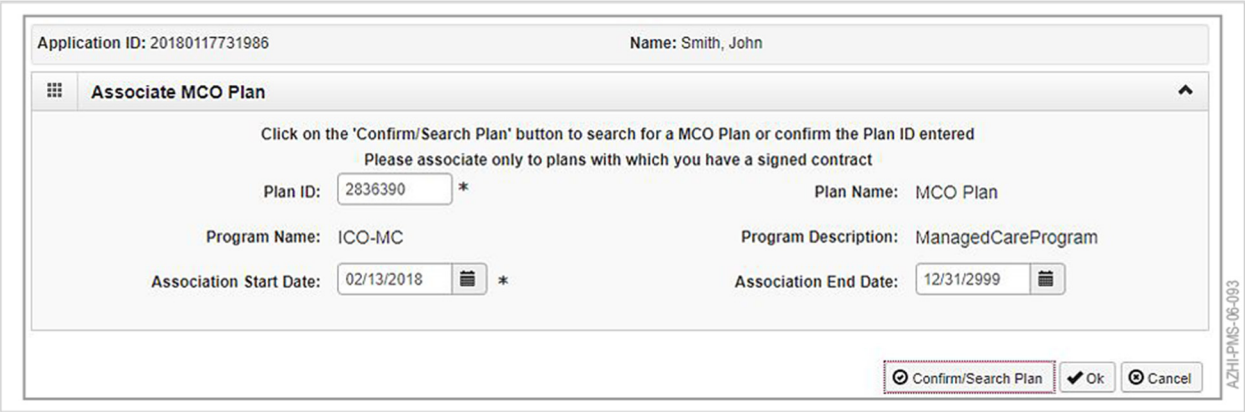


Figure A.6.9-16. Identify MCO's Contracted Providers. Providers can associate to an MCO through "Associate MCO Provider" BPW step.

Figure A.6.9-17 is the "View Network Provider Details" screen, which shows contracted provider information that MCOs can view, as well as State staff that are in expert mode.

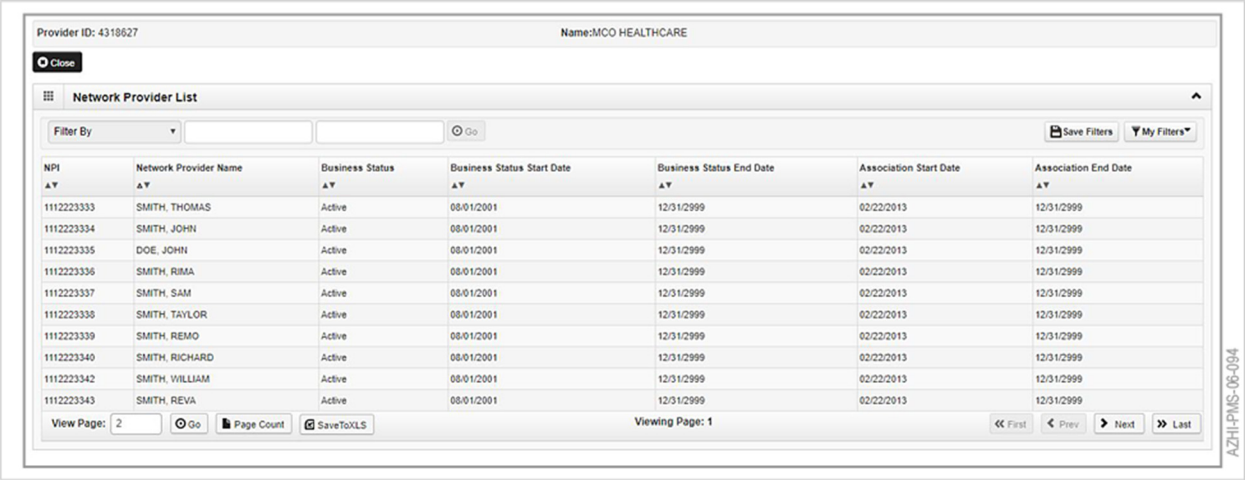


Figure A.6.9-17. Identify MCO's Contracted Providers. MCO and State staff can see the list of providers who are contracted to the MCO from the View Network Provider Details screen.

A.6.10 Manage Provider Communication [SOW, Section 5.10]

A.6.10.1 Trigger Process for Provider Notification [SOW, Section 5.10.1]

Configurable communication templates are included in the PMIS Solution for generating notifications to the provider. Templates include a section(s) that lists missing information or needing correction, along with a due date and instructions to respond. The communications contain information to further educate the provider on who to contact should they have any clarifying questions about the request. The correspondence also indicates the importance of responding, as failure to respond will result in the enrollment application not being processed to completion. evoBrix PMIS provides ability for the authorized user to terminate or deny an enrollment application in the event of incomplete information, or if required information is not received by State-identified auto-closure dates.

A.6.10.2 Electronic and Paper Correspondence/Guidance [SOW, Section 5.10.2]

Figure A.6.10-1 lists current automated letters/notices that are used to support the Provider Business Area.

#	Correspondence Title	Description
1	Provider Welcome Notice	This letter indicates that the provider is approved and welcomes the provider to participate in Medical Assistance Program.
2	Denial Notice	This letter is generated by the system for each application that is denied for enrollment by the State.
3	License/Certification Term in 45 Days' Notice	This letter is generated for all providers whose license/certification expires within the next 45 days.
4	License Termination Notice	This letter indicates the provider license has expired and that provider enrollment is end dated.
5	Provider Revalidation 90 Day Notice	This letter is generated for all providers who have 90 days to revalidate their enrollment.
6	Provider Revalidation 30 Day Notice	This letter is generated for all providers who have not revalidated their enrollment and have 30 more days to complete their revalidation.
7	Provider Revalidation Termination Notice	This letter is generated for all providers who have not revalidated their enrollment within the 90-day time frame and system terminates the enrollment.
8	Provider Revalidation Intermediate Cycle Notice	This letter is generated for all providers who have not revalidated in their intermediate cycle and system terminates the enrollment after the due date.
9	Sanctioned Notice	This letter indicates that the provider has been Sanctioned and is no longer eligible to participate in the Medicaid Program effective from sanction date.
10	Suspended Notice	This letter indicates that the provider has been Suspended and is no longer eligible to participate in the Medicaid Program effective from suspension date.
11	Application ID Notice	This email is generated by the system when the enrolling provider has entered the basic information for the first time successfully.

Figure A.6.10-1. Correspondence List. evoBrix PMIS features automated generation of letters and notices.

A.6.10.3 Notify AHCCCS/Med-QUEST When Site Visit Required [SOW, Section 5.10.3]

The application has an embedded calendar, which the processor can use to look for all the site visits scheduled for a month. Figure A.6.10-2 shows the calendar for the Processor for all the scheduled site visits.

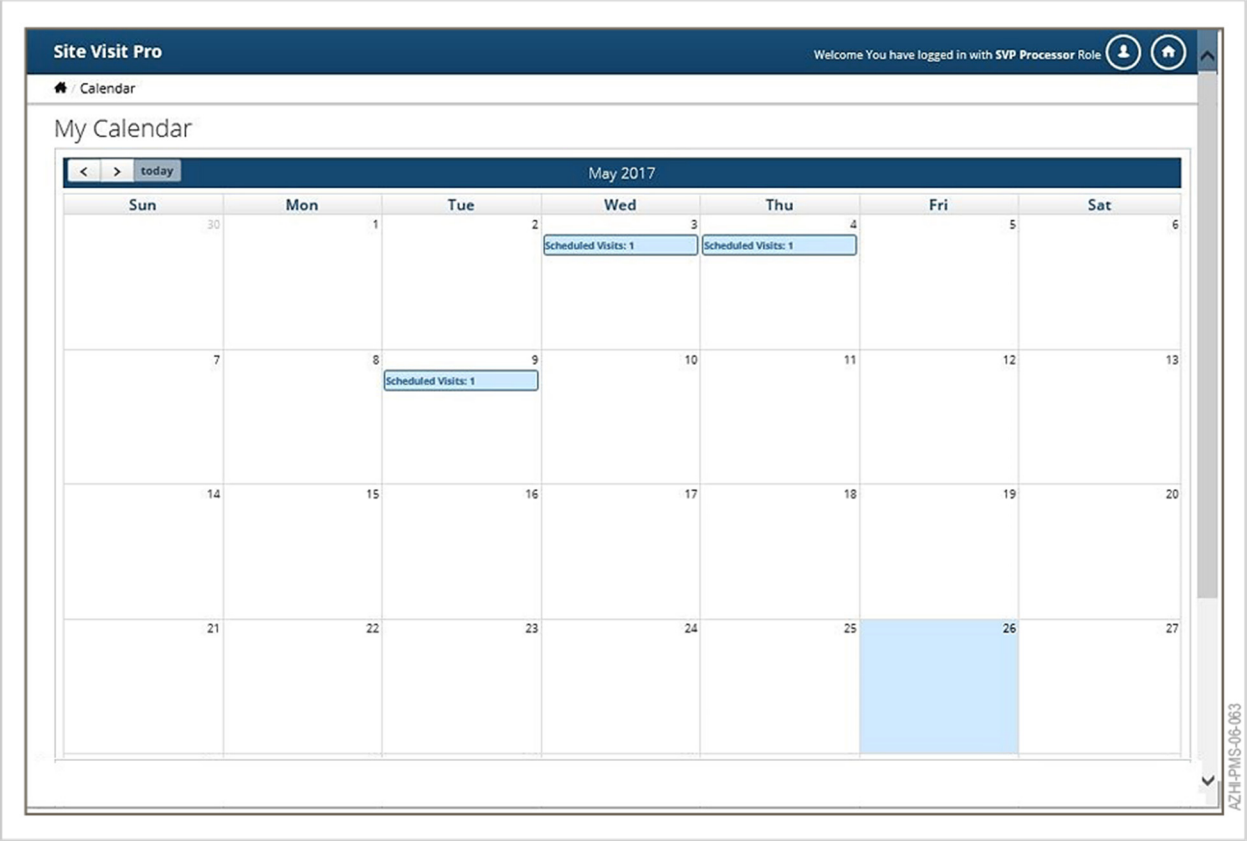


Figure A.6.10-2. Site Visit Calendar Page. This page displays the calendar of site visits for the logged in processor.

Figure A.6.10-3 displays the site visit screenings of the processor and their statuses.

Site Visit Pro — Welcome You have logged in with **SVP Processor** Role

My Screenings

My Screenings

Filter By: Select | Go

RISK	NPI	PROVIDER NAME	PROVIDER LOCATION	SUBMITTED DATE	SCHEDULED DATE	SITE VISIT STATUS	EMAIL REMINDER	MAP	ADD TO CALENDAR	HISTORY	ACTIONS
	1122917036	Tri county home medical	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	09/13/2015	04/27/2017	In- Process	Yes / No				Continue
	1079578773	Advance Pathology Services	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	03/07/2017	04/24/2017	In- Process	Yes / No				Continue
	1103336495	Smith Bryan	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	09/13/2015	10/12/2016	In- Process	Yes / No				Continue
	107573172	EduardMaranova WeiserovaLaylade	1021 NedomovaEbo Dr, CHICAGO, COOK, Illinois 60625	09/13/2015	03/22/2017	In- Process	Yes / No				Continue
	1114604519	FUSION CUSTOM CHAIRS LLC	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	08/13/2015	05/04/2017	In-Review	Yes / No				Continue
	1083611222	HEALTH HOSPITALS SPECTRUM	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	02/24/2017	02/24/2017	In-Review	Yes / No				Continue
	1084780398	SPECIALIZED MEDICAL SERVICES	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	08/13/2015	05/03/2017	In-Review	Yes / No				Continue
	1101407967	University Physician Group	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	08/13/2015	10/23/2015	In-Review	Yes / No				Continue
	1125166490	LIVERNOIS PHARMACY INC	1030 BensonAld Dr, ROCKVILLE, MONTGOMERY, Maryland 20850	02/24/2017	04/24/2017	In-Review	Yes / No				Continue
	1000015085	Woodlands Hospital	1019 BacaAstryd Ave, SOUTH ELGIN, KANE, Illinois 60177	07/23/2016	05/09/2017	Assigned	Yes / No				Start

Showing 1 to 10 of 16 records

Pages: Previous 1 2 Next

AZHI-PMS-06-062

Figure A.6.10-3. Site Visit Screenings Page, for processors. This page displays the screenings scheduled for the logged in processor.

Figure A.6.10-4 shows email notifications that will be received by the Visitor for the upcoming Site visits.

Site Visit Reminder

Date: 08/20/2015

Dear [redacted],

Your Site Visit assignments for the week of **08/22/2015** to **08/26/2015** are listed below:

Total Assignments: 2

1 :

Scheduled Date: 08/24/2015

Provider Name: [redacted]

NPI: [redacted]

County: [redacted]

Address: [redacted]

2 :

Scheduled Date: 08/25/2015

Provider Name: [redacted]

NPI: [redacted]

County: [redacted]

Address: [redacted]

AZHI-PMS-06-024

Figure A.6.10-4. Site Visit Reminder Email. This email shows all the Site visits scheduled by the visitor for the upcoming week

A.6.10.4 Provider Request for Action to AHCCCS/Med-QUEST [SOW, Section 5.10.5]

Figure A.6.10-5 displays the upload document page for a provider to attach the requested supporting documents and enter text in the remarks.

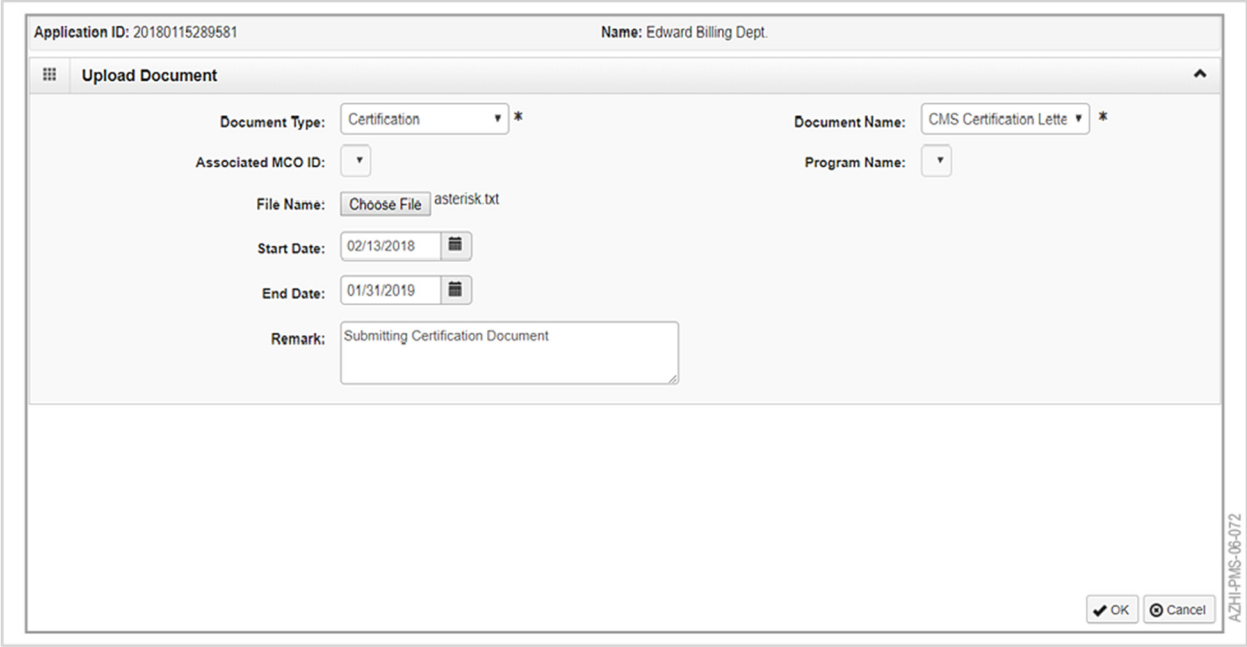


Figure A.6.10-5. Upload of Attachment and Enter Test Description. The page allows the provider to upload the supporting documents and enter the submission notes in the remarks text area.

A.6.11 Perform Provider Outreach [SOW, Section 5.11]

A.6.11.1 Communication with Providers via Portal View [SOW, Section 5.11.1]

Figure A.6.11-1 displays the banner message page in the provider portal.

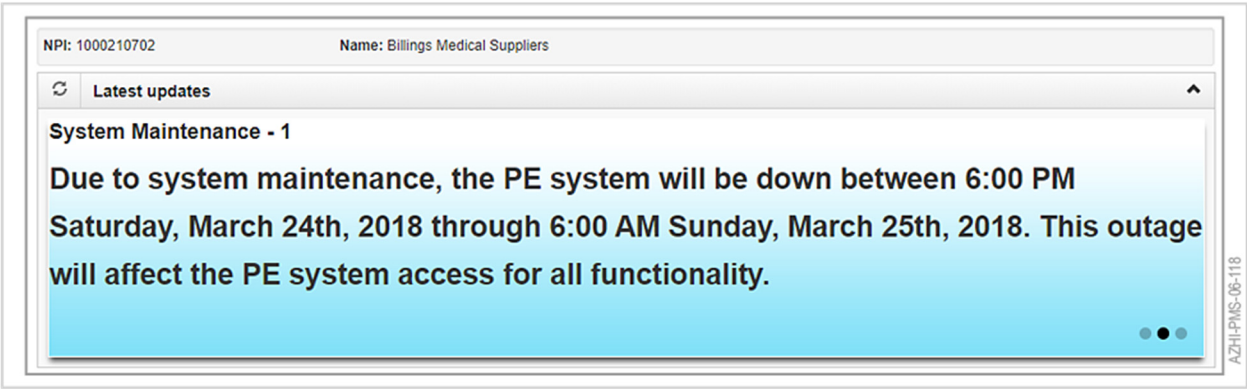


Figure A.6.11-1. Banner Messages. The provider portal displays the banner message about the scheduled system maintenance.

evoBrix PMIS provides the inbox alert to notify the provider about any new messages available to view and read. The alert displays the type, description, and due date. Figure A.6.11-2 displays the inbox alert page in the provider portal.

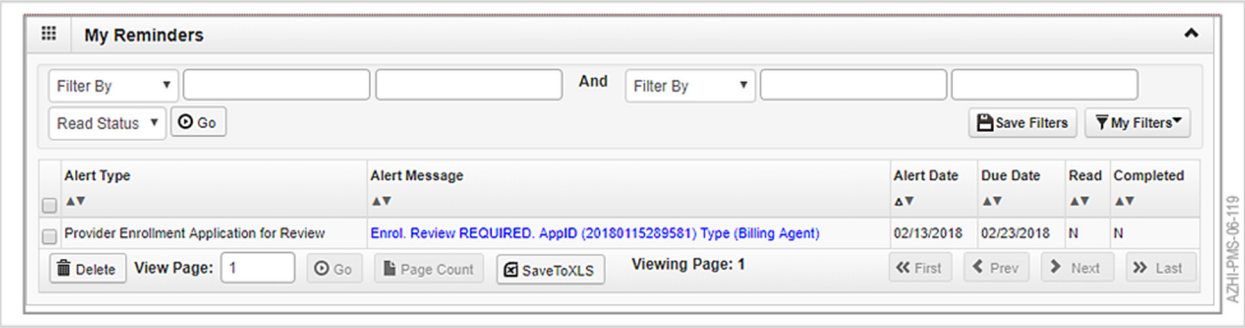


Figure A.6.11-2. Provider Portal Inbox Alert. The home page displays the inbox alert to notify the provider.

A.6.12 Manage Provider Grievance [SOW, Section 5.12]

Not applicable

A.6.13 Reporting [SOW, Section 5.13]

A.6.13.1 Standardized Operational Reports Library [SOW, Section 5.13.1]

Figure A.6.13-1 shows a list of system included reports available from day one of implementation.

Report Name	Report Description
835 Authorizations By Provider Report	This report provides list of all Billing Agent Association and 835 Authorization report.
ABMS Screening Results Report	This report provides a list of those providers whose board certificate has changed from "Yes" to "No" during the batch monthly screening process.
Adverse Action Report – NPI Level	This report will be generated with list of adverse actions ("SUSPENDED" and "SANCTIONED SOURCE") for providers on a particular day.
Adverse Action Report – Owner Level	This report will be generated with list of adverse actions ("SUSPENDED" and "SANCTIONED SOURCE") for Owners on a particular day.
Enrollment Application Referrals and Activity Returns by Provider Type	This report is used to evaluate Enrollment Application Referrals and Activity Returns at the Provider type level.
Enrollment Application Referrals/Activity Returns by User	This report is used to evaluate Enrollment Application Referrals and Activity Returns at the user level.
ERA Enrollment Report	This report is used to print the ERA Agreement that a provider agreed upon when enrolling into evoBrix or submitting a modification request.
Finger Printing Visit Report – NPI Level	This report provides a list of providers with fingerprinting due date based on NPI. The on-demand report will pull the reports based on input dates.
Finger Printing Visit Report – Owner Level	This report provides a list of providers with fingerprinting due date based on ownership. The on-demand report will pull the reports based on input dates.
Home Help Verification Submission Status Report	This report will be used to identify the providers that have not submitted a verification form for the selected service month(s).
Home Help Verification Submission Status Summary Report	This report will provide the total Verification Submissions that have been submitted, saved, and not submitted for the selected month.
Print Permission Matrix Report	This report is used to print the Permission Matrix.

Report Name	Report Description
Print Provider Information Report	This report is used to print the provider information for active providers. This report will also include all active pharmacy providers.
Print Terms and Conditions Report	This report is used to print the Terms and Conditions that a provider agreed upon enrolling into evoBrix.
Provider Advance Screening Report – Criminal Offense	This report provides a list of providers who have criminal offenses.
Provider Advance Screening Report – Sex Offense	This report provides a list of providers who have sex offenses.
Provider List by Invalid NCPDP Report	This report lists Pharmacy providers with an Invalid NCPDP ID.
Provider List by Invalid NPI Report	This report lists providers by Invalid NPI.
Provider Primary Care Report	This report provides a list of all providers who have the primary care specialties/subspecialties selected and who have the Board Certified, Board Eligible and or Eligible Claims Found set.
Provider Primary Care Report – Board Eligible	This report provides a list of all providers that have "Board Eligible" under the license/certification step and their Board Eligible end-date will end during the current month.
Provider Processing Statistics Modification Requests by Provider Type	This report is used to evaluate Modification Request statistics at the Provider Type level.
Provider Processing Statistics Modification Requests by User	This report is used to evaluate modification request statistics at the State Approver (user) level.
Provider Processing Statistics New Applications by Provider Type	This report is used to evaluate New Application statistics at the provider type level.
Provider Processing Statistics New Applications by User	This report is used to evaluate new application statistics at the user level.
Provider Revalidation Report	This report provides a list of providers with Cycle End-Date matching the date range submitted for the report.
Sanctioned-License Expired Pharmacy Providers	This report provides a list of pharmacy providers that have a disciplinary sanction and/or whose licenses have expired.
Site Visit Report	This report provides a list of providers with site visits due.
SSN/EIN/TIN Verification Report	This report provides a list of providers whose "SSN Verified," "EIN/TIN Verified," or "Name Verified" has been set to no.
Vital Records Report	List of providers that were updated to "deceased" within the date range selected.

Figure A.6.13-1. Standardized Operational Reports for evoBrix PMIS. List of configurable detail and summary level reports offered by the evoBrix reporting solution for meeting the needs of AHCCCS/Med-QUEST.

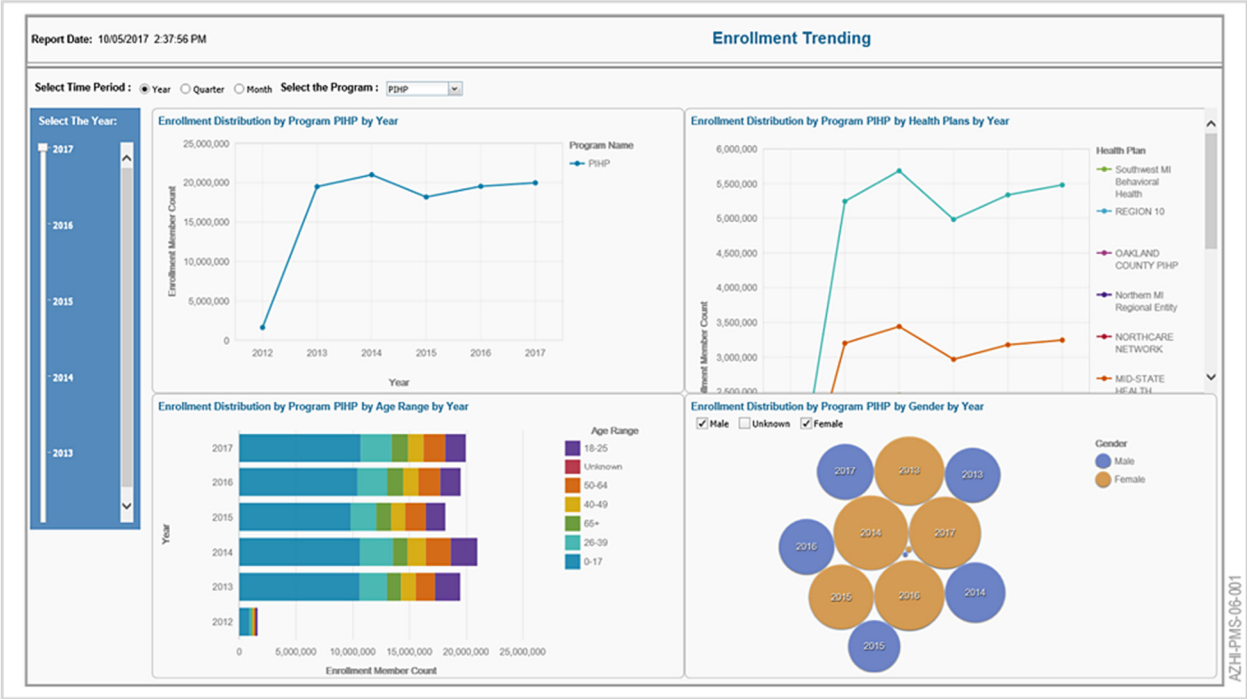


Figure A.6.13-2 shows a sample dashboard designed in IBM Cognos BI Workspace.

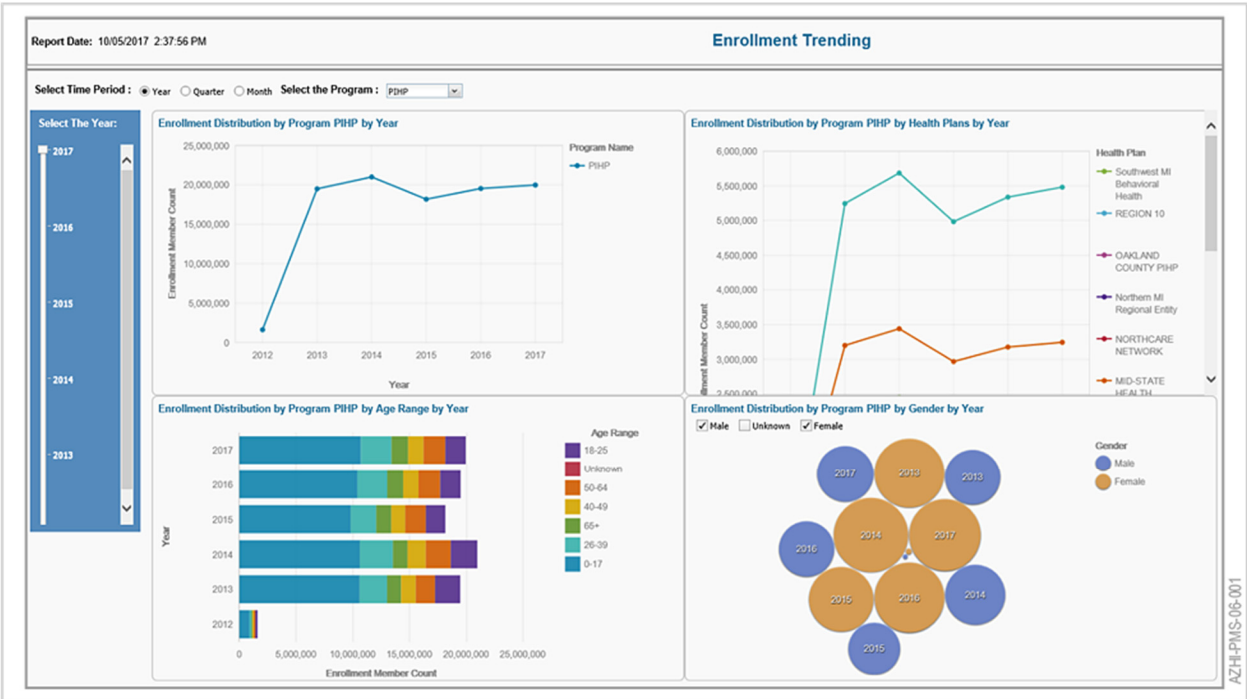


Figure A.6.13-2. IBM Cognos BI Active Dashboard. A sample of pre-built IBM Cognos BI Active Dashboard.

A.6.13.2 Report, Dashboard, and Query Templates [SOW, Section 5.13.3]

IBM Cognos BI Query Studio is the reporting tool that will facilitate users to create simple queries and reports in IBM Cognos BI Business Intelligence. In Query Studio, users can:

- Connect to a data source to view data elements in a tree hierarchy in ad hoc models. Users may expand the query subjects to see query item details.
- Design/create customized reports which can be saved, modified, copied or reused.
- Improve the layout or appearance of the report. For example, users can create a chart, add a title, specify text and border styles, or reorder columns for easy comparison.
- Use filters, summaries, and calculations to compare and analyze data.
- Drill up and drill down to view detail or summary information.

Both Cognos Workspace Advanced and Query Studio could be used to create query templates which could be modified by users to design complex reports according to business requirements. Figure A.6.13-3 shows a sample ad hoc query template designed in IBM Cognos BI Query Studio.

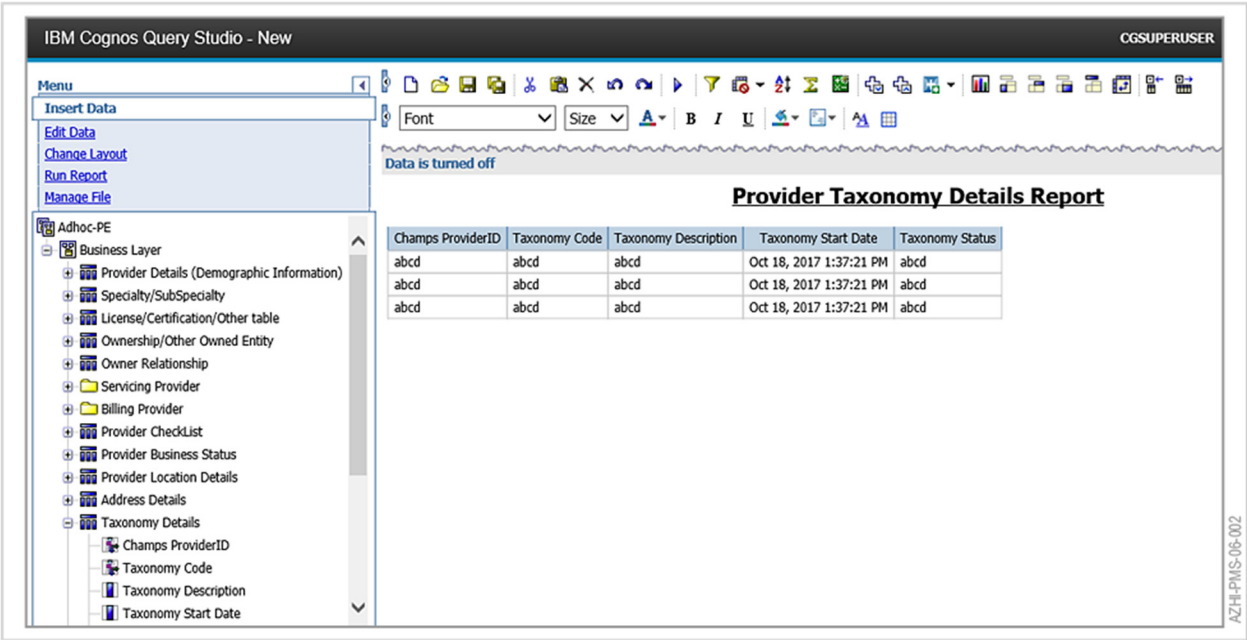
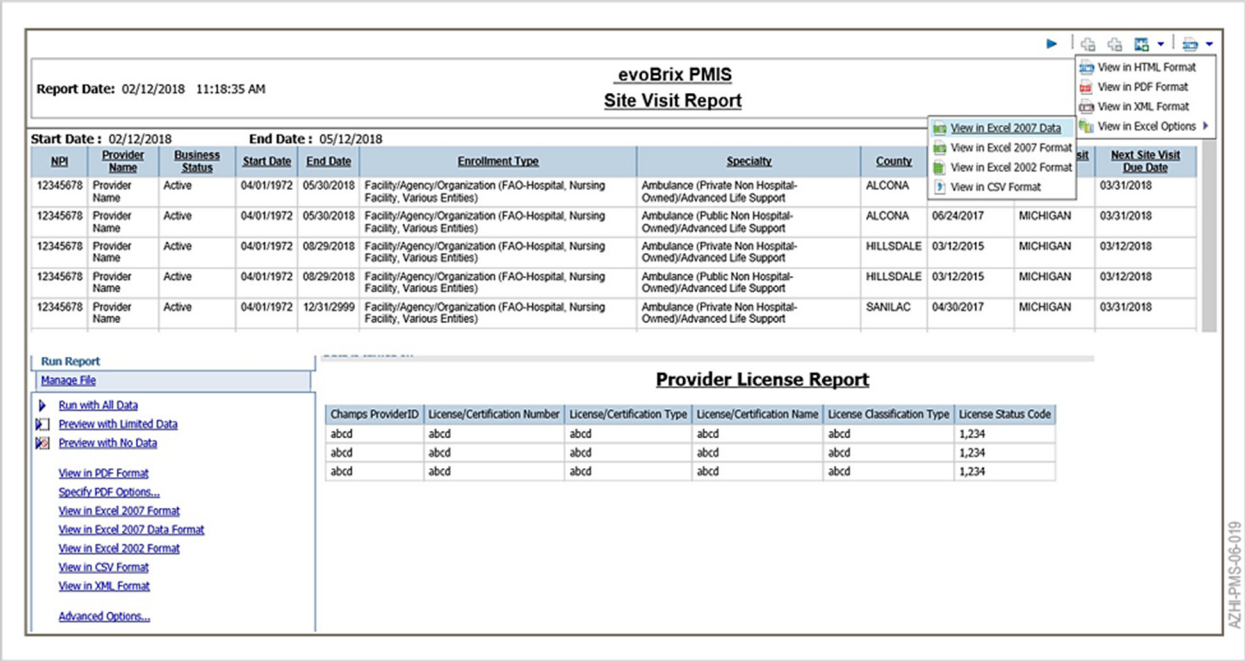


Figure A.6.13-3. Ad hoc Query Template. A sample ad hoc query template designed in IBM Cognos BI Query Studio displaying the query subjects based on the ad hoc provider model within evoBrix PMIS.

Figure A.6.13-4 shows how to view/export a report in IBM Cognos BI Viewer.

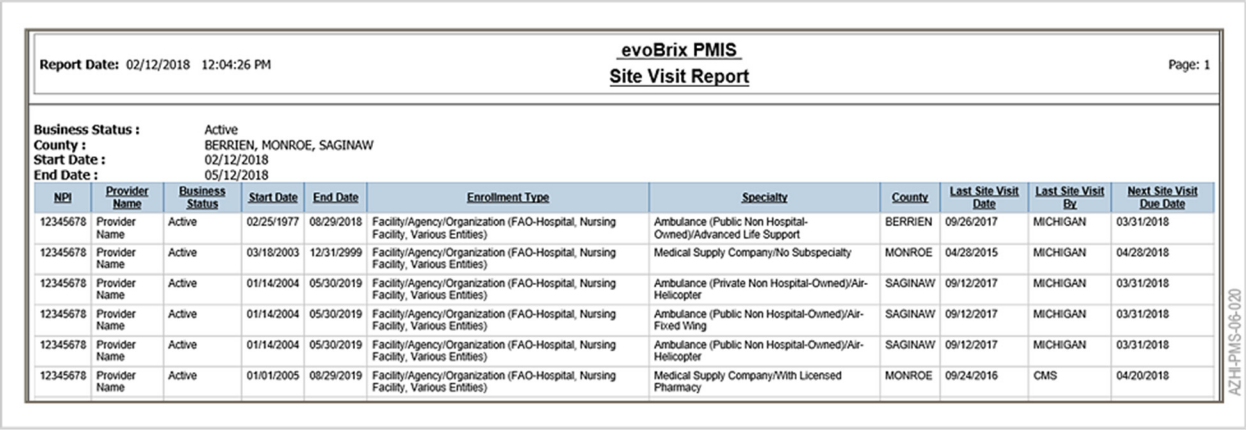


NPI	Provider Name	Business Status	Start Date	End Date	Enrollment Type	Specialty	County			Next Site Visit Due Date
12345678	Provider Name	Active	04/01/1972	05/30/2018	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Private Non Hospital-Owned)/Advanced Life Support	ALCONA			03/31/2018
12345678	Provider Name	Active	04/01/1972	05/30/2018	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Public Non Hospital-Owned)/Advanced Life Support	ALCONA	06/24/2017	MICHIGAN	03/31/2018
12345678	Provider Name	Active	04/01/1972	08/29/2018	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Private Non Hospital-Owned)/Advanced Life Support	HILLSDALE	03/12/2015	MICHIGAN	03/12/2018
12345678	Provider Name	Active	04/01/1972	08/29/2018	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Public Non Hospital-Owned)/Advanced Life Support	HILLSDALE	03/12/2015	MICHIGAN	03/12/2018
12345678	Provider Name	Active	04/01/1972	12/31/2999	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Private Non Hospital-Owned)/Advanced Life Support	SANILAC	04/30/2017	MICHIGAN	03/31/2018

Champs ProviderID	License/Certification Number	License/Certification Type	License/Certification Name	License Classification Type	License Status Code
abcd	abcd	abcd	abcd	abcd	1,234
abcd	abcd	abcd	abcd	abcd	1,234
abcd	abcd	abcd	abcd	abcd	1,234

Figure A.6.13-4. Report Export Formats. A sample of a pre-built IBM Cognos BI Report Studio report that shows how to view or export a standard report in different formats.

Figure A.6.13-5shows a sample parameterized report, showing the actual query parameter values provided.

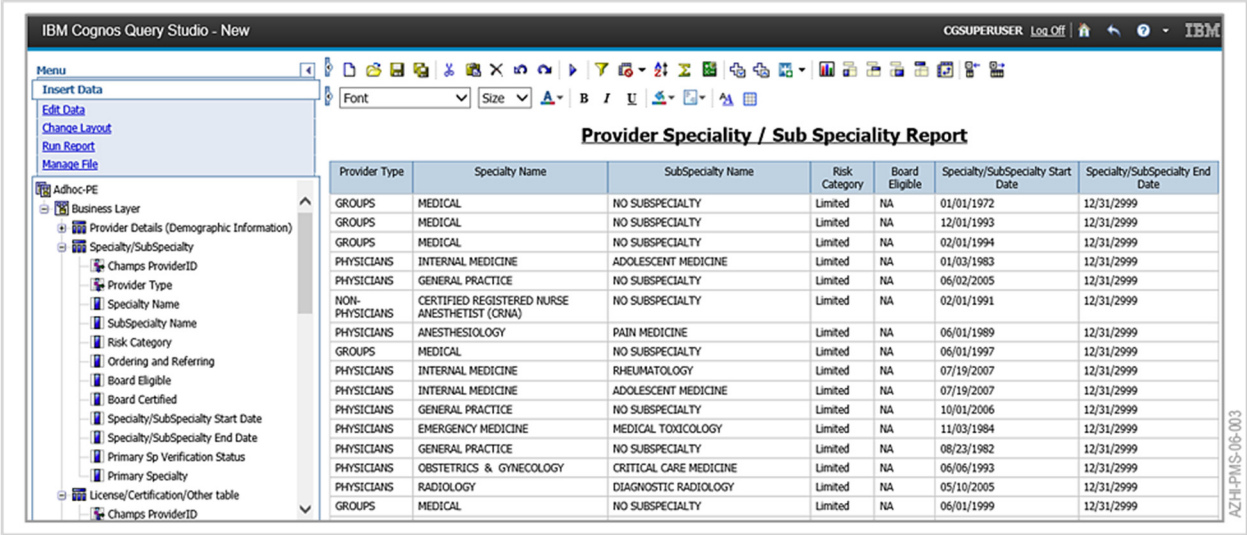


NPI	Provider Name	Business Status	Start Date	End Date	Enrollment Type	Specialty	County	Last Site Visit Date	Last Site Visit By	Next Site Visit Due Date
12345678	Provider Name	Active	02/25/1977	08/29/2018	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Public Non Hospital-Owned)/Advanced Life Support	BERRIEN	09/26/2017	MICHIGAN	03/31/2018
12345678	Provider Name	Active	03/18/2003	12/31/2999	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Medical Supply Company/No Subspecialty	MONROE	04/28/2015	MICHIGAN	04/28/2018
12345678	Provider Name	Active	01/14/2004	05/30/2019	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Private Non Hospital-Owned)/Air-Helicopter	SAGINAW	09/12/2017	MICHIGAN	03/31/2018
12345678	Provider Name	Active	01/14/2004	05/30/2019	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Public Non Hospital-Owned)/Air-Fixed Wing	SAGINAW	09/12/2017	MICHIGAN	03/31/2018
12345678	Provider Name	Active	01/14/2004	05/30/2019	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Ambulance (Public Non Hospital-Owned)/Air-Helicopter	SAGINAW	09/12/2017	MICHIGAN	03/31/2018
12345678	Provider Name	Active	01/01/2005	08/29/2019	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	Medical Supply Company/With Licensed Pharmacy	MONROE	09/24/2016	CMS	04/20/2018

Figure A.6.13-5. Parameterized Report Output. A sample of a pre-built IBM Cognos BI Report Studio report output in IBM Cognos BI Viewer. Note that the query parameters are displayed along with the output.

A.6.13.3 Query Tool [SOW, Section 5.13.4]

IBM Cognos BI Packages, a set of metadata objects, are designed to contain information relating specifically to one or multiple functional areas per business requirements. Packages contain data elements, organized in a user-friendly way, which makes it easy to navigate and identify data elements. The complexity of the tables and relationships is hidden from the user for an enhanced self-service user experience. Users can simply drag and drop the business elements into their workspace to create customized ad hoc reports. The reports could either be at a summary or detail level due to granular level of data storage in the evoBrix Online Transactional Processing (OLTP) system. Figure A.6.13-6 shows a sample ad hoc report designed in IBM Cognos BI Query Studio based on the evoBrix PMIS ad hoc provider model.

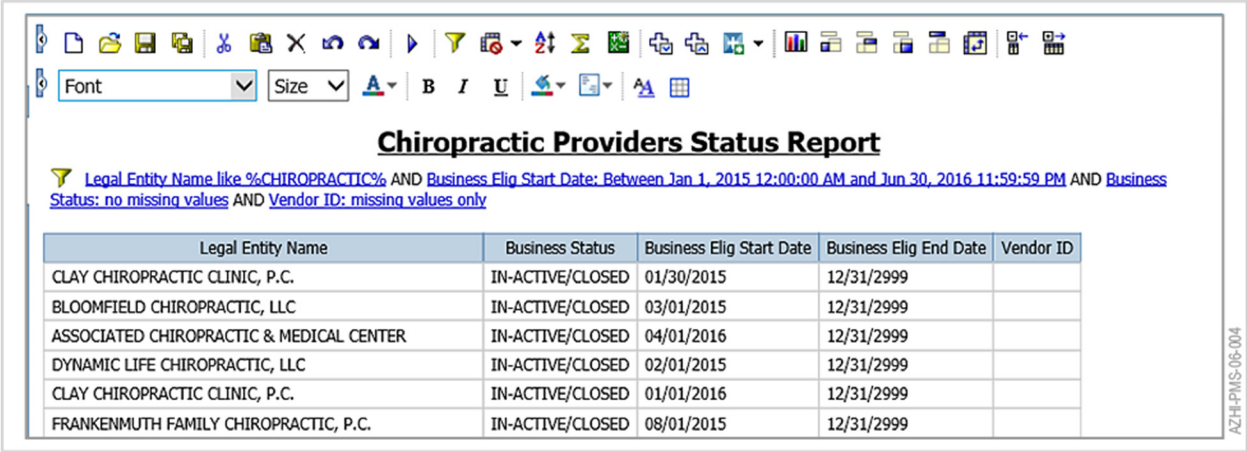


Provider Type	Specialty Name	SubSpecialty Name	Risk Category	Board Eligible	Specialty/SubSpecialty Start Date	Specialty/SubSpecialty End Date
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	01/01/1972	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	12/01/1993	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	02/01/1994	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	ADOLESCENT MEDICINE	Limited	NA	01/03/1983	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	06/02/2005	12/31/2999
NON-PHYSICIANS	CERTIFIED REGISTERED NURSE ANESTHETIST (CRNA)	NO SUBSPECIALTY	Limited	NA	02/01/1991	12/31/2999
PHYSICIANS	ANESTHESIOLOGY	PAIN MEDICINE	Limited	NA	06/01/1989	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	06/01/1997	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	RHEUMATOLOGY	Limited	NA	07/19/2007	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	ADOLESCENT MEDICINE	Limited	NA	07/19/2007	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	10/01/2006	12/31/2999
PHYSICIANS	EMERGENCY MEDICINE	MEDICAL TOXICOLOGY	Limited	NA	11/03/1984	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	08/23/1982	12/31/2999
PHYSICIANS	OBSTETRICS & GYNECOLOGY	CRITICAL CARE MEDICINE	Limited	NA	06/06/1993	12/31/2999
PHYSICIANS	RADIOLOGY	DIAGNOSTIC RADIOLOGY	Limited	NA	05/10/2005	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	06/01/1999	12/31/2999

Figure A.6.13-6. A Sample Ad-hoc Report. A sample ad hoc report designed in IBM Cognos BI Query Studio based on evoBrix PMIS ad hoc provider model to support AHCCCS/Med-QUEST healthcare program business needs.

A.6.13.4 Reporting Tool [SOW, Section 5.13.5]

Figure A.6.13-7 shows a sample parameterized report based on wild card search and operators, in IBM Cognos BI Viewer.



Legal Entity Name	Business Status	Business Elig Start Date	Business Elig End Date	Vendor ID
CLAY CHIROPRACTIC CLINIC, P.C.	IN-ACTIVE/CLOSED	01/30/2015	12/31/2999	
BLOOMFIELD CHIROPRACTIC, LLC	IN-ACTIVE/CLOSED	03/01/2015	12/31/2999	
ASSOCIATED CHIROPRACTIC & MEDICAL CENTER	IN-ACTIVE/CLOSED	04/01/2016	12/31/2999	
DYNAMIC LIFE CHIROPRACTIC, LLC	IN-ACTIVE/CLOSED	02/01/2015	12/31/2999	
CLAY CHIROPRACTIC CLINIC, P.C.	IN-ACTIVE/CLOSED	01/01/2016	12/31/2999	
FRANKENMUTH FAMILY CHIROPRACTIC, P.C.	IN-ACTIVE/CLOSED	08/01/2015	12/31/2999	

Figure A.6.13-7. A Sample Parameterized Report. A sample of a pre-built IBM Cognos BI parameterized report that shows wildcard search pattern and use of operators to design and execute queries to support AHCCCS/Med-QUEST healthcare program business needs.

A.6.13.5 Display Data in Variety of Formats [SOW, Section 5.13.6]

Figure A.6.13-8 and Figure A.6.13-9 show various report styles available and a sample pre-built report in a graph format (designed in IBM Cognos BI Report Studio) respectively.

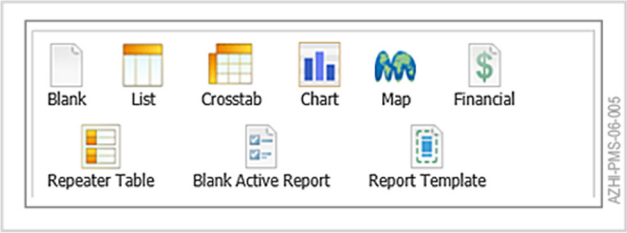


Figure A.6.13-8. Report Styles Available in IBM Cognos BI. Various report styles available in IBM Cognos BI Query and Report Studio.

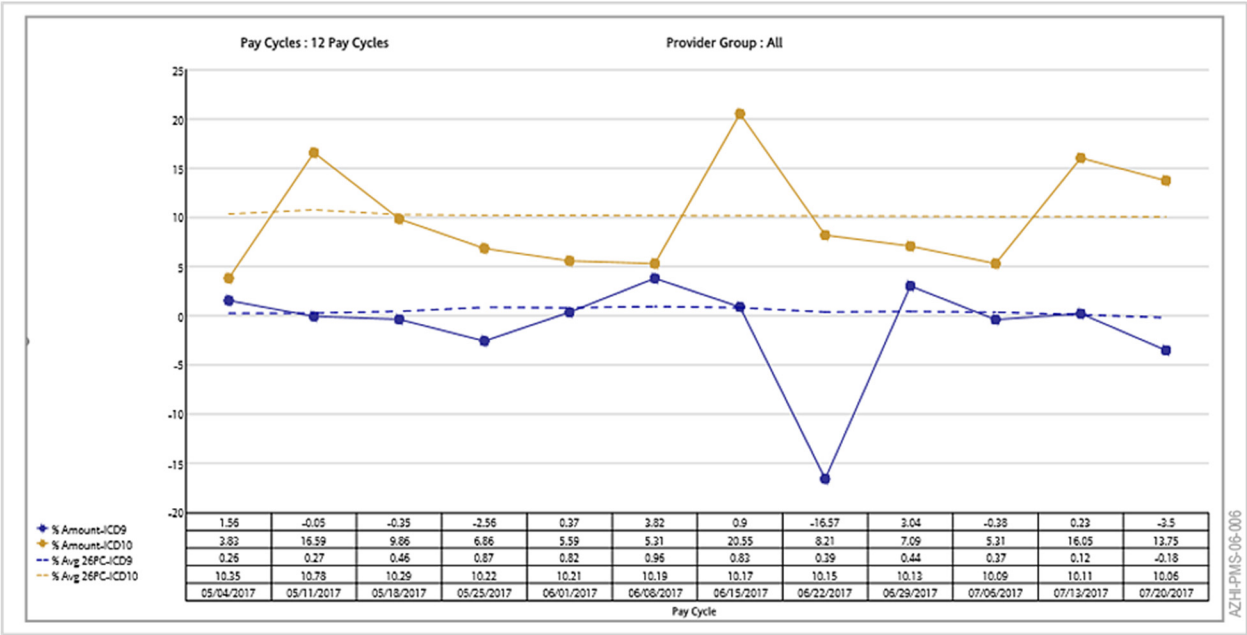


Figure A.6.13-9. A Sample Graph-based Report. A sample of pre-built IBM Cognos BI Report Studio report that represents data in the form of a graph.

A.6.13.6 Produce Reports or Display Output Data [SOW, Section 5.13.7]

Figure A.6.13-10 shows a sample IBM Cognos BI Query Studio Report designed to display NPI, Provider ID, and Taxonomy information.

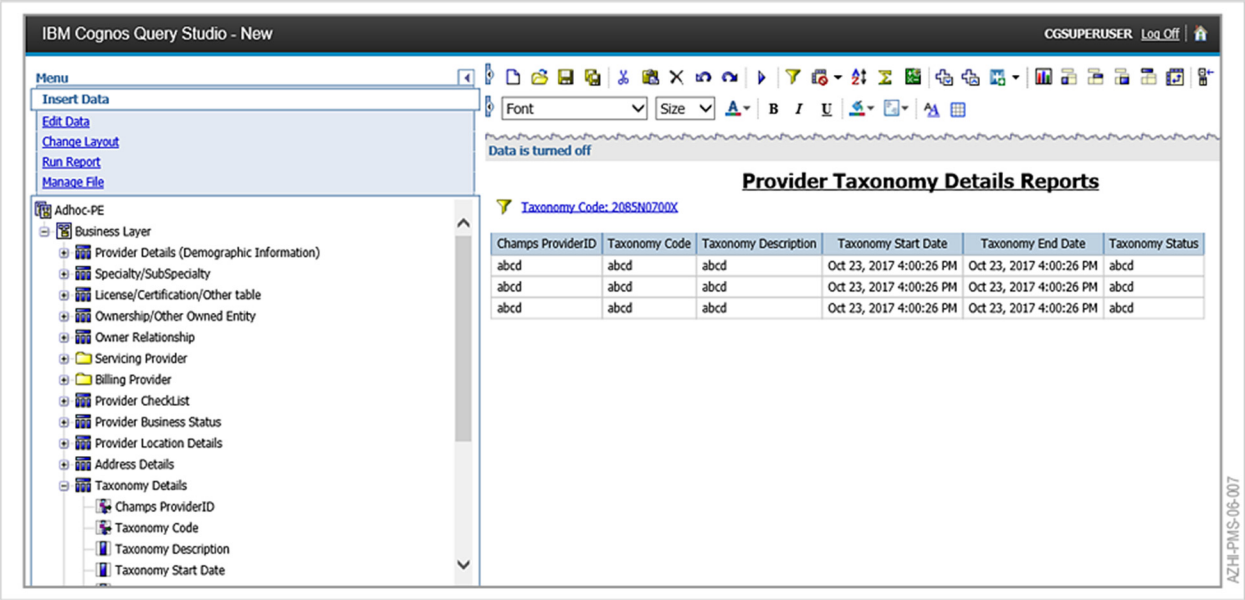


Figure A.6.13-10. Provider Information Report Filtered by Taxonomy. A sample ad hoc report designed in IBM Cognos BI Query Studio to display NPI, Provider ID, and Taxonomy information.

A.6.13.7 Tracking/Reporting Summary and Detailed PE Information [SOW, Section 5.13.9]

Figure A.6.13-11 shows a sample IBM Cognos BI Report Studio report that shows summary and detail versions of provider vital record statistics.

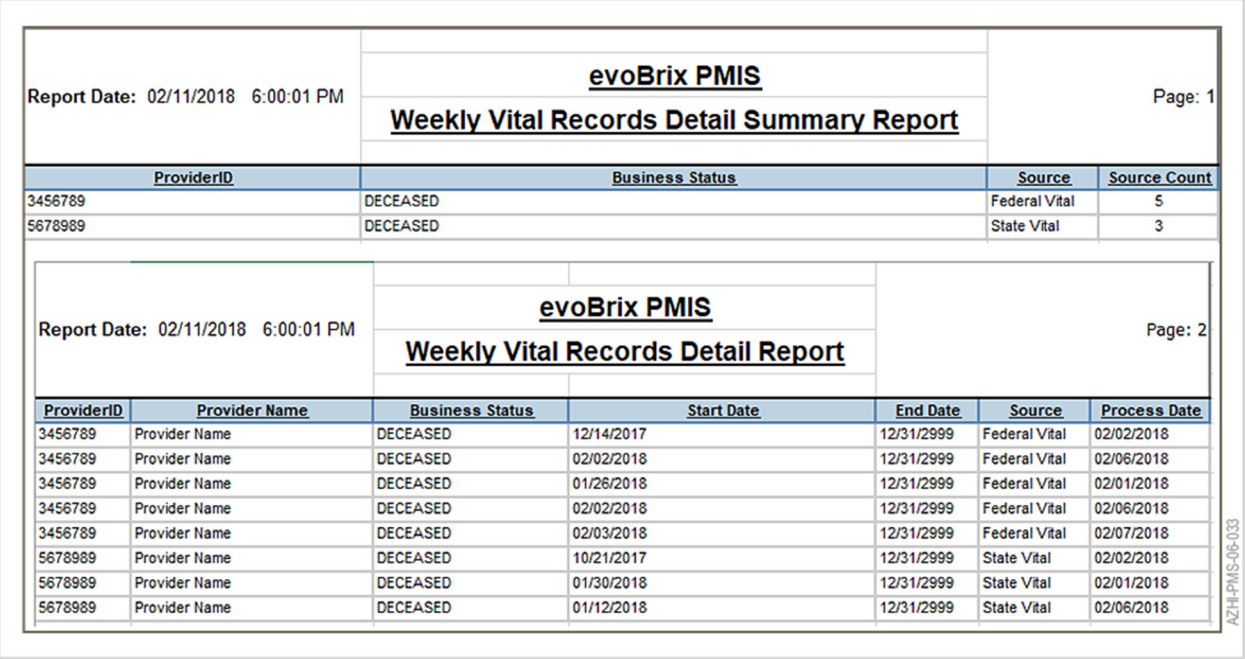


Figure A.6.13-11. Weekly Provider Vitals Report. Sample IBM Cognos BI Report Studio report that shows summary and detail versions of provider vital record statistics.

A.6.13.8 Provider Transaction Error Reporting [SOW, Section 5.13.10]

Figure A.6.13-12 shows a sample interface completion and error reporting for provider screening transactions.

-----Original Message-----
From: evoBrix_PROD@<state>.gov [mailto:evoBrix_PROD@<state>.gov]
Sent: Friday, July 07, 2017 5:12 PM
To: MW_Ops_Interfaces; CNSINOC; MW_TEC_SOA; MW_OPS_PESupport
Subject: DB2DB Job - (PCS monthly screening) Successful

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

**********Do Not Respond To this email**********

Interface : Provider PCS monthly screening (1268) Completed With Errors.

Interface Run Details:

Interface Run SID : 200024211
Interface ID : 1268
Interface Name : Provider PCS monthly screening
Start Time : 07/07/2017 05:08:27 PM
End Time : 07/07/2017 05:11:35 PM
Source Records : 1560
Success Records : 1558
Error Records : 2
Prerequisite Interfaces: N/A
Dependent Interfaces : N/A

All Errors logged in INTERFACE_RUN_ERROR table.

Error Specifics

Error : 1
Error Type : DATABASE ERROR
Error Description : Warning - In Review Record exists for the Provider ID - 1234567 and for the CLIA License Number 03D8765

Error : 2
Error Type : DATABASE ERROR
Error Description: Error Inserting into PCS_SCRNG_RESULTS for Provider_id: 7654321 ORA-06502: PL/SQL: numeric or value error: character string buffer too small at "PCS_BTCH_PRVDR_MNTHLY_SCRNG", line 4031

Error : 3
Error Type : DATABASE ERROR
Error Description : Warning - In Review Record exists for the Provider ID - 3334444 and for the CLIA License Number 42D2038

Error : 4
Error Type : DATABASE ERROR
Error Description : Error Inserting into PCS_SCRNG_RESULTS for Provider_id: 4445555 ORA-06502: PL/SQL: numeric or value error: character to number conversion error at "PCS_BTCH_PRVDR_MNTHLY_SCRNG", line 3894

**********Do Not Respond to This Email**********

AZHI-PMS-06-010

Figure A.6.13-12. CNSI's ISR Interface Completion Notification. A sample interface completion and error reporting for provider screening in PCS.

A.6.13.9 Initiation of Reports [SOW, Section 5.13.11]

Scheduled Reports

Scheduled reports are automatically generated based on a fixed schedule, finalized during the solution phase. Users are notified via auto-generated emails once the report execution completes on a given schedule. CNSI's reporting solution contains several management and operational reports that are scheduled to run from the transaction OLTP system on a daily/weekly basis. These reports will also be made available through IBM Cognos BI Connection Portal for viewing and retrieval. The report outputs are archived and integrated into IBM Cognos BI Content Store and could be retained according to pre-defined retention policies.

Figure A.6.13-13 shows various scheduled report output versions in IBM Cognos BI Connection Portal.

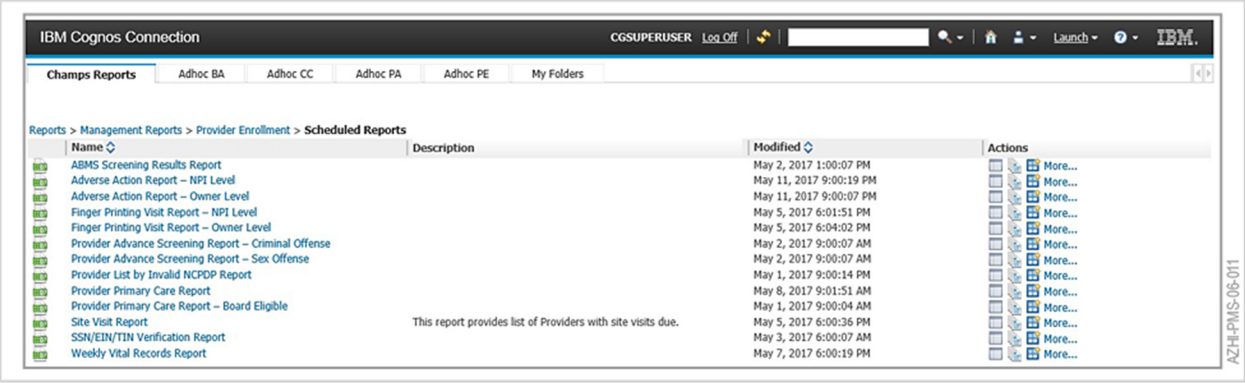


Figure A.6.13-13. IBM Cognos Connection Portal. Screenshot showing different report outputs for scheduled reports in IBM Cognos Connection Portal.

On-Demand Reports

On-Demand Reports are generated based on user action. These reports are generally parameterized and will require some user input before they can be executed. The prompts may be based on dates, numbers or text. IBM Cognos BI validates user input values in the correct format. It will be up to the discretion of the user to save the reports locally, view, or discard them, as these outputs will not be available in the IBM Cognos BI Content Store repository. IBM Cognos BI Connection Portal allows users to access on-demand reports.

Ad Hoc Reports

In the context of evoBrix PMIS, ad hoc reporting is a frequent occurrence. Hence, it is important to have a tool that provides an easy interface to create and execute reports. IBM Cognos BI suite of tools offers Query Studio for analytical users to create, modify, view, and change the appearance and the distribution of ad hoc reports.

CNSI's ad hoc reporting for evoBrix PMIS is facilitated by OLTP, using IBM Cognos BI Query Studio. This is in turn integrated with evoBrix application. IBM Cognos BI Packages, a set of metadata objects, are designed to contain information relating specifically to one or multiple functional areas per business requirements. Packages contain data elements organized in a user-friendly way, which makes it easy to navigate and identify data elements. The complexity of the tables and relationships is hidden from the user for an enhanced self-service user experience.

Users can simply drag and drop the business elements required into their workspace to create their own customized ad hoc report. Due to the granular nature of data storage in OLTP, reports could be created at different aggregation levels (detail or summary) tied to various dimensions. Though this is applicable to pre-built reports as well, ad hoc reporting provides the user with the flexibility to create their own customized reports. They can also execute, generate the query or report, and can save in various formats including HTML, Excel, CSV, and PDF. Figure A.6.13-14 shows a sample ad hoc report in Excel format.

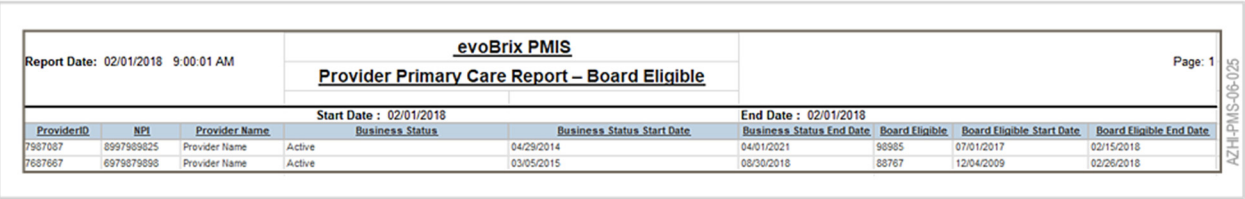


Figure A.6.13-14. Excel Format Output. Screenshot showing a sample ad hoc report in Excel format.

Note: Report shown with de-identified data.

CNSI's reporting solution, using IBM Cognos Content Archival, also provides the capability to configure an enterprise content management (ECM) storage that is outside of IBM Cognos BI to store scheduled report outputs. Cognos Archival decides the archival criteria based on retention criteria in Content Store and uses background jobs to move the files to ECM automatically. Access to the report outputs will be the same as it is in IBM Cognos BI content store. These report outputs can be archived based on AHCCCS/Med-QUEST defined retention policies. The report outputs can be shared with external applications or users who don't have access to CNSI's reporting solution. Figure A.6.13-15 shows the list of report outputs saved in ECM.

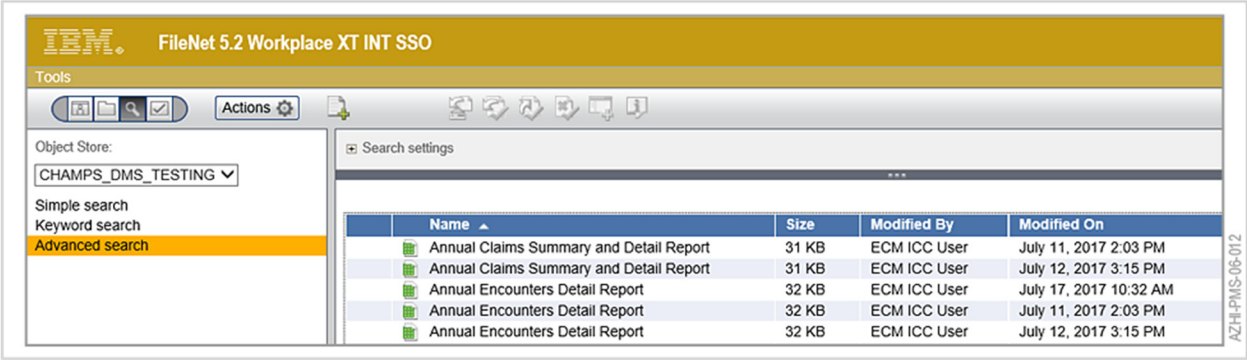


Figure A.6.13-15. Report Output Stored in ECM. A screenshot showing the list of report outputs saved in ECM.

A.6.13.10 Custom Reports [SOW, Section 5.13.15]

Proactively monitoring the health of operations enables CNSI to be more predictive, rather than reactive, in the provision of our services. Figure A.6.13-16 shows how HealthBeat monitors system resources of Real Application Clustered (RAC) databases.

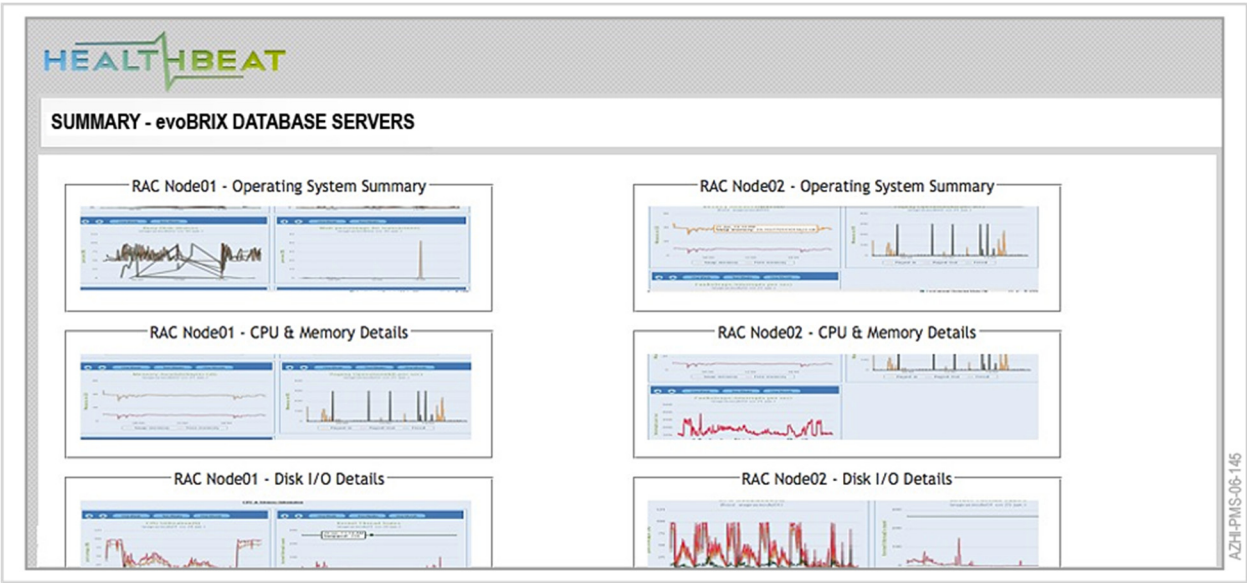


Figure A.6.13-16. HealthBeat for System Monitoring. Monitoring of clustered databases.

Figure A.6.13-17 shows an Incident Report template.

CNSI

Production Incident Report

Incident Headline:	
Incident Date/Time:	
Report Author:	
Team(s)/Individual(s) Involved:	
Date Report Prepared:	
Ticket Number(s):	

Incident Details

Description:

Detailed description of the incident.

Scope and Impact of the Incident:

Who or what was impacted by the incident. List both short term and long term Impacts.

Incident Resolution Timeline

Communications:

List all communications relating to the incident (emails, phone calls etc.). Include individuals involved & timelines.

Solution: Steps Taken to Resolution and Next Steps:

Detailed descriptions of steps taken to resolve the incident including timelines.

Root Cause:

Detailed description on what caused the incident to occur.

Incident Prevention Plan

Lessons Learned and Recommendations:

Describe lessons learned as a result the incident and provide detailed recommendations on how to prevent this incident from reoccurring in the future.

Action Plan:

Describe the Action Plan to implement the Recommendations including Owners and expected completion dates for the Actions.

Step	Task	Owner	Planned Date
1	Example: Install new certificate when there is a change or time to renew the LN SSL certificate.	PCS and MI Deployment team	NA

Incident Report Template.docx CNSI Page | 1

AZH-PMS-06-146

Figure A.6.13-17. Sample Production Incident Report. CNSI focuses on root cause analysis to address incidences during production.

A.6.13.11 Defect Reporting and Tracking Tool [SOW, Section 5.13.17]

CNSI will leverage the Jira tool for defect reporting and tracking to offer the following benefits to AHCCCS/Med-QUEST:

- Improve the quality of the evoBrix PMIS solution using integrated defect and change-tracking capabilities.
- Configure and automate defect tracking workflows for better efficiency and predictability.
- Make compliance management easier with capabilities that help monitor and implement compliance processes and track approvals.
- Provider visibility to the State personnel for changes in the evoBrix PMIS solution right down to the minutest detail with real-time reports for better, more informed decision making.

A.6.13.12 Statistic Reports [SOW, Section 5.13.19]

Figure A.6.13-18 shows a Daily Provider Enrollment Operational Statistics DB report that tracks the high-level provider enrollment operational statistics by application statuses, enrollment and user types.

ctrprd_dbjobs@cns-inc.com
IL PE SUMMARY 02/15/2018 12:00:02 PM
Archive 3/17/2018

Overall Summary

Enrollment Status	Legacy (Converted)	IMPACT (New Enrollment)
Total Approved	94310	90536
Total Denied	861	1385
Total In-Process	90505	5151
Total In-Review	659	3578
Total Enrollments	186335	100650

Summary by Enrollment Type and Application Status

Source	Enrollment Type	Application Status			
		In Process	In Review	Approved	Denied
IMPACT (New Enrollment)	Atypical Agency Provider	224	121	430	54
IMPACT (New Enrollment)	Atypical Individual Provider	1405	2402	47751	148
IMPACT (New Enrollment)	Billing Agent	520	12	524	140
IMPACT (New Enrollment)	Contractor/MCO	1	0	52	2
IMPACT (New Enrollment)	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	364	210	2365	271
IMPACT (New Enrollment)	Group Practice (Corporation, Partnership, LLC, etc.)	444	40	6811	505
IMPACT (New Enrollment)	Individual/Sole Proprietor	2193	793	32603	265
LEGACY (Converted)	Atypical Agency Provider	4284	13	298	146
LEGACY (Converted)	Atypical Individual Provider	68007	492	36001	241
LEGACY (Converted)	Contractor/MCO	0	0	1	0
LEGACY (Converted)	Facility/Agency/Organization (FAO-Hospital, Nursing Facility, Various Entities)	2189	36	9710	319
LEGACY (Converted)	Individual/Sole Proprietor	16025	118	48300	155

User Login - Summary

User Type	Total User Count	Logged-In User Count (15-FEB-18)
Provider	32879	156
State User	3073	167

AZHI-PMS-06-120

Figure A.6.13-18. Daily Provider Enrollment Operational Statistics. Sample operational DB report from CNSI's evoBrix PMIS solution that show the provider enrollment and day-to-day operational statistics.

A.6.14 Solution Help System [SOW, Section 5.14]

A.6.14.1 Link Training Modules [SOW, Section 5.14.1]

Figure A.6.14-1 shows an example of an evoBrix PMIS screen with the links dropdown activated.

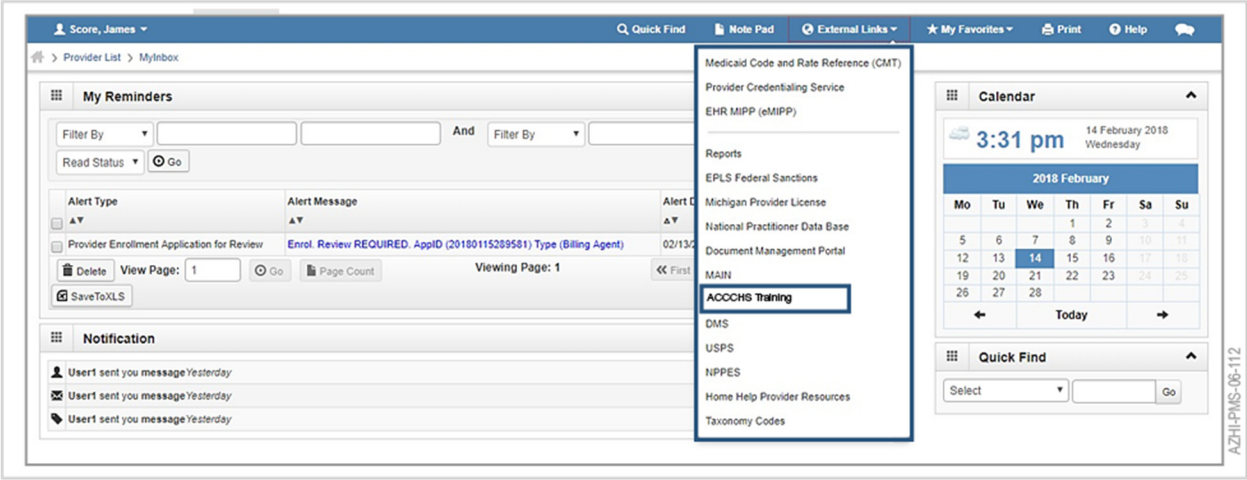


Figure A.6.14-1. evoBrix PMIS Active Links Dropdown Menu. Providers and state users can access training modules without exiting the system using the External Links feature.

A.6.15 System Availability [SOW Section 5.15]

A.6.15.1 Performance Monitoring Dashboard [SOW, Section 5.15.1]

The classification of monitoring tools and their respective modules is specified in Figure A.6.15-1. Detailed architecture, tools, and processes for performance monitoring, although not required as part of the response for this section, are provided as reference material for AHCCCS/Med-QUEST review in Appendix A, Additional Information, section A.6.15.1.

Monitoring Tool	Monitoring Area	Infrastructure Modules
SLA Automation Tool	SLA Management	Application, Interfaces/Web Services, Servers
HealthBeat	System Operations	Application, Interfaces/Web Services, Servers
Oracle Enterprise Manager	Databases, Infrastructure	Databases and Database Servers, SOA Suite Application Servers
Building Management System	Data Center	Data Center Power and Cooling
Data Center Infrastructure Management	Data Center	Infrastructure

Figure A.6.15-1. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

SLA Automation Tool and Operational Performance Standards. CNSI's SLA automation solution provides AHCCCS/Med-QUEST with configurable SLA management capabilities and ensures that SLAs are being consistently met. Figure A.6.15-1 shows the SLA automation tool architecture. Our solution uses an SLA Automation Engine which is configured to automatically or manually track various SLAs related to system and business functions, such as interfaces and report generations thus providing visibility of daily system and business functions. The tool is also equipped with tracking, reporting, and management capabilities using CNSI's HealthBeat as the front-end application. The SLA Automation engine runs on a configurable interval to generate service transactions based on the configured SLA's frequency schedule. The system retrieves data input from various source systems via REST or SOAP web service requests for multiple service configurations at any given time. In the event of a non-compliant transaction, notification alert emails are generated and sent to email addresses linked to that service configuration.

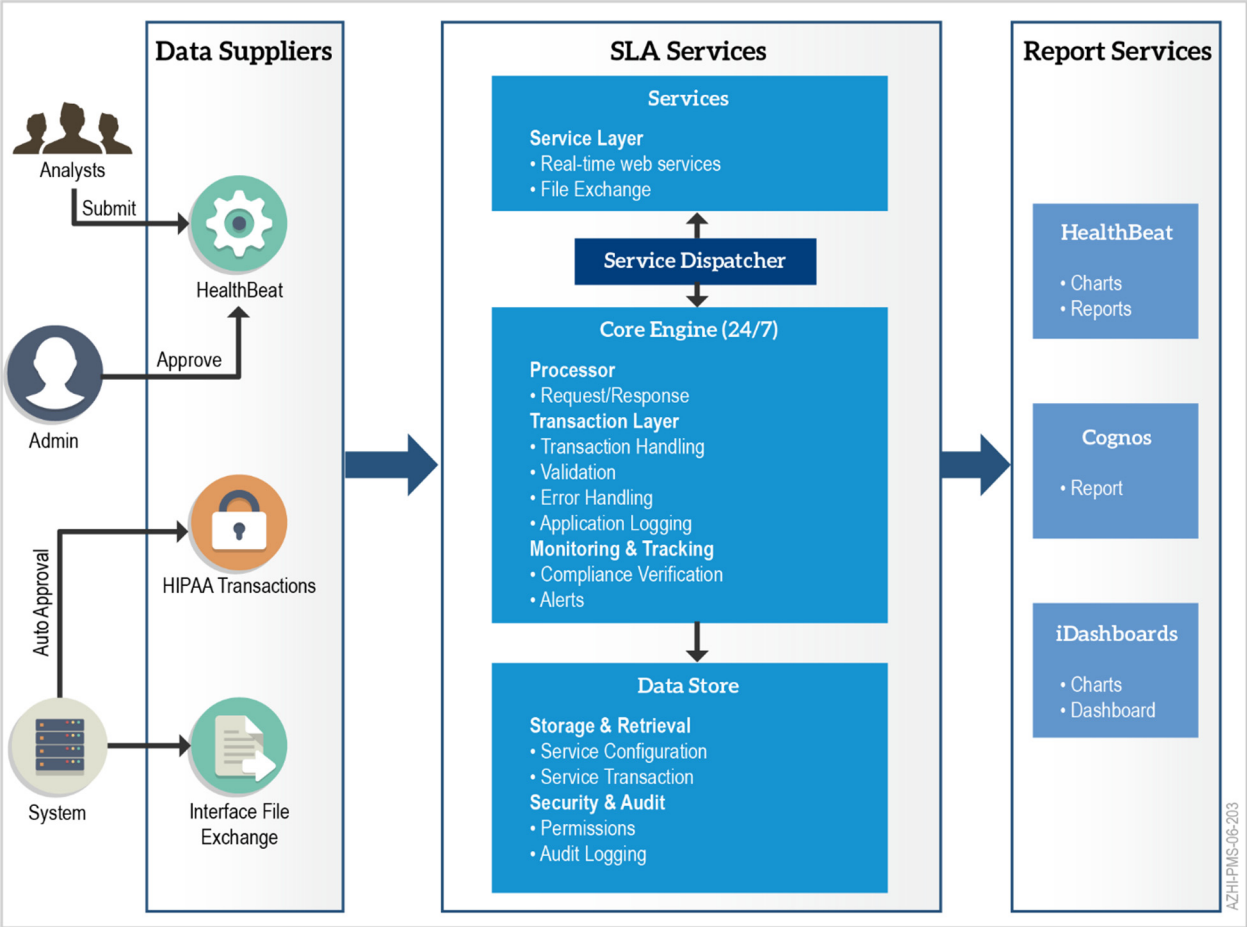


Figure A.6.15-1. SLA Automation Tool Architecture. The SLA Automation Engine is configured to automatically or manually track various SLAs.

HealthBeat - System Monitoring. CNSI's HealthBeat solution provides a comprehensive system monitoring framework along with the capability to facilitate continuous process improvement. As the system handles each process, it collects process-related data in the data store. This data is then used to display the process dashboard and provide visibility to the process metrics and the health of the operation. The system uses workflow-based analytics to provide feedback on potential bottlenecks and application performance issues. Thresholds are configured by CNSI operations team to display performance in the traditional "red," "yellow," and "green" dashboard status.

Related to system monitoring, HealthBeat reports accurate data on items such as end-user response time, CPU utilization, and hourly load averages on different servers. This allows CNSI to see the system from a higher point of view and help make informed, strategic decisions on daily operations or future changes in policy and programs. Application management and monitoring, web services management, systems management and monitoring, network management and monitoring, performance monitoring, and event monitoring are all managed via the framework of HealthBeat. Figure A.6.15-2 shows how HealthBeat monitors system resources of real application clustered (RAC) databases.

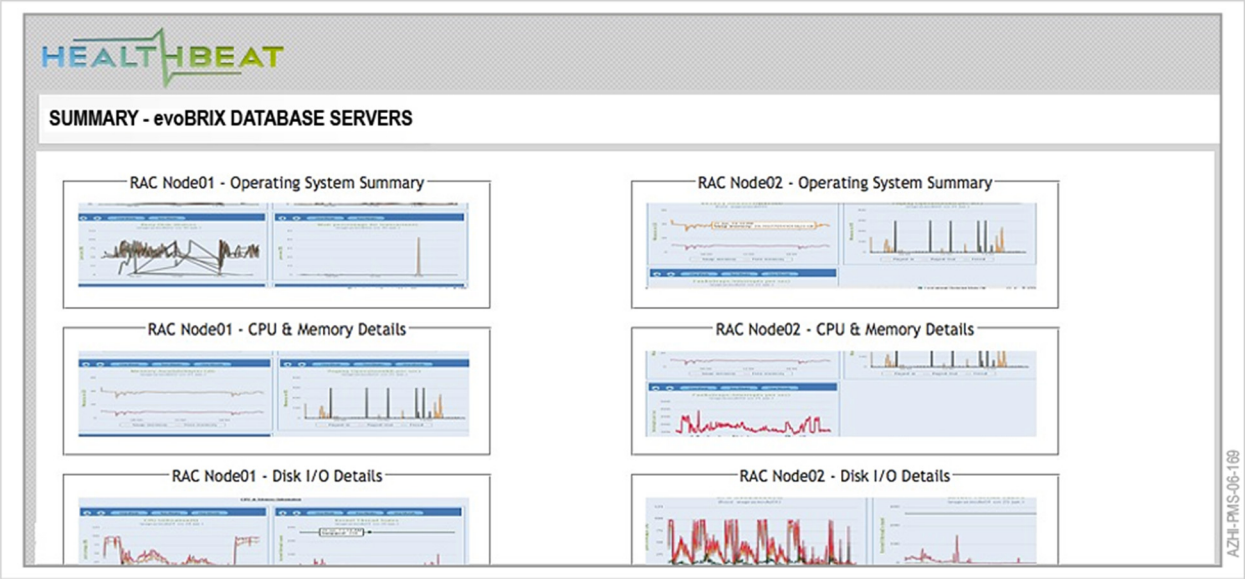


Figure A.6.15-2. HealthBeat for System Monitoring. Monitoring of clustered databases.

HealthBeat also provides various reporting mechanisms, including dashboards and graphs that can be used to report on the metrics associated with performance standards. Operational management staff regularly monitor data displayed through the dashboard and can proactively respond if performance indicators begin to decline. In addition, email alerts are established to notify appropriate CNSI and State staff based on configured exception thresholds. Figure A.6.15-3 shows the HealthBeat architecture that is configurable and automated.

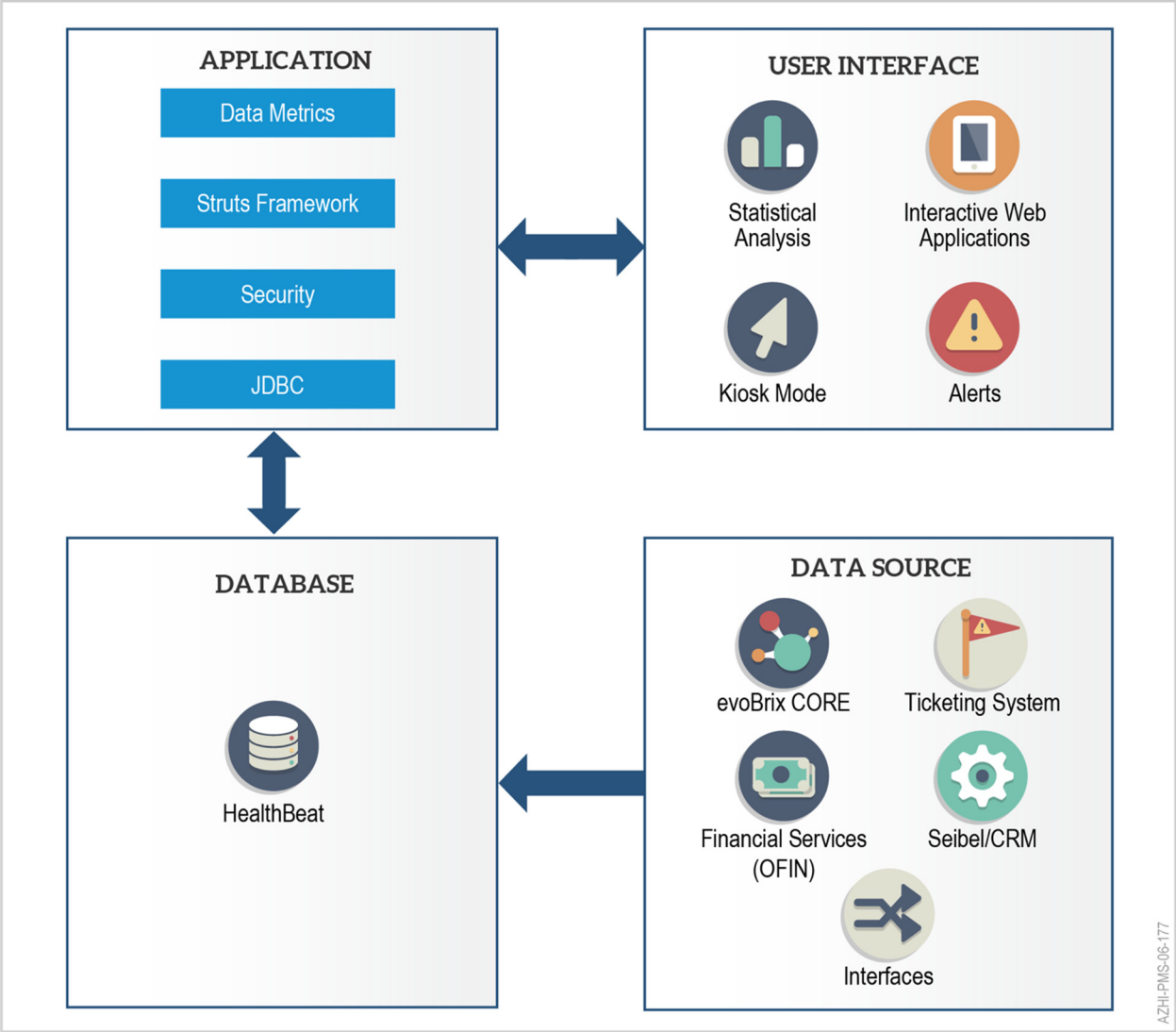


Figure A.6.15-3. HealthBeat Architecture. Provides AHCCCS/Med-QUEST with configurable, automated, real-time visibility into business operations.

Oracle Enterprise Manager. CNSI's database administrators and system administrators rely on OEM to maintain, monitor, and configure proactive alerts for Oracle databases, SOA Suite, and Application Servers. The OEM Console and Enterprise Manager Command Line Interface (EMCLI) enables administrators to access and manage OEM functionalities, which in turn sends notifications and alerts to the NOC. The NOC triages issues to the appropriate operations team for corrective action. Figure A.6.15-4 shows the OEM architecture. Various alerts are configured in OEM to issue immediate notifications as soon as an issue occurs. Alerts are sent to a NOC team that monitors the system 24x7x365 and communicates the same to the respective teams.

Building Management System and Data Center Infrastructure Management. Building Management System (BMS) alerts critical facilities staff and engineers of any issues. Depending upon priority, a ticket is executed and staff resolve or assign vendors for ticket completion and issue resolution. The BMS handles monitoring of power and cooling.

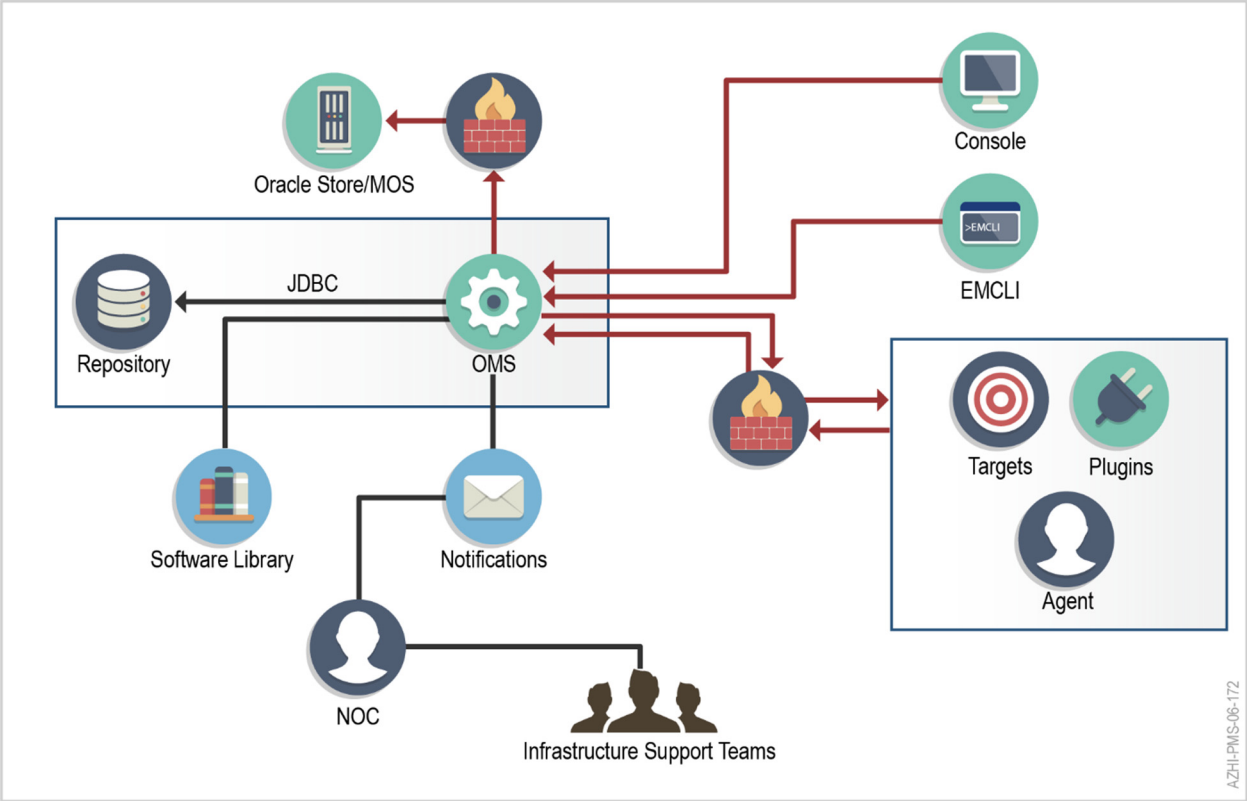


Figure A.6.15-4. OEM Architecture. OEM monitors the availability and performance of the database and application servers and alerts the necessary teams.

Data Center Infrastructure Management (DCIM) monitors all environmental systems (e.g., temperature, humidity, power usage, leakage, efficiencies of equipment and systems). Additionally, DCIM monitors all video and door access surveillance from a central NOC, staffed 24x7x365. Together, BMS and DCIM help to monitor and report any loss in high-availability functionalities across hardware and software components in the data center layer.

A.6.15.2 99.5% Availability [SOW, Section 5.15.2]

CNSI's Availability Management Plan includes but is not limited to the following aspects: Designing high-availability, redundant systems to support mission-critical applications; Testing system availability to meet all AHCCCS/Med-QUEST SLAs; and Monitoring and reporting high-availability to ensure that SLAs are being met.

High Availability Architecture Design. CNSI's evoBrix PMIS solution addresses challenges related to additional volumes and new programs anticipated for the future, as well as issues related to performance, maintenance, and availability. In addition, the solution leverages virtualization technologies to logically partition physical servers. Scalability and elasticity are inherent features of our cloud-based architecture, and our solution supports normal business activities with the ability to increase the demand on the system without modification to the software or degradation in performance. Our architecture includes:

- Clustering at physical host level to provide for physical host failure
- Application server cluster with Web server load balancing
- Oracle Database real application cluster for database high availability
- Oracle Data Guard solution for database replication
- Oracle Recovery Manager (RMAN) for database backups and Flashback for point-in-time recovery

Figure A.6.15-5 depicts the high-level availability architecture covering clustering at the application server and database server level as well as web server load balancing.

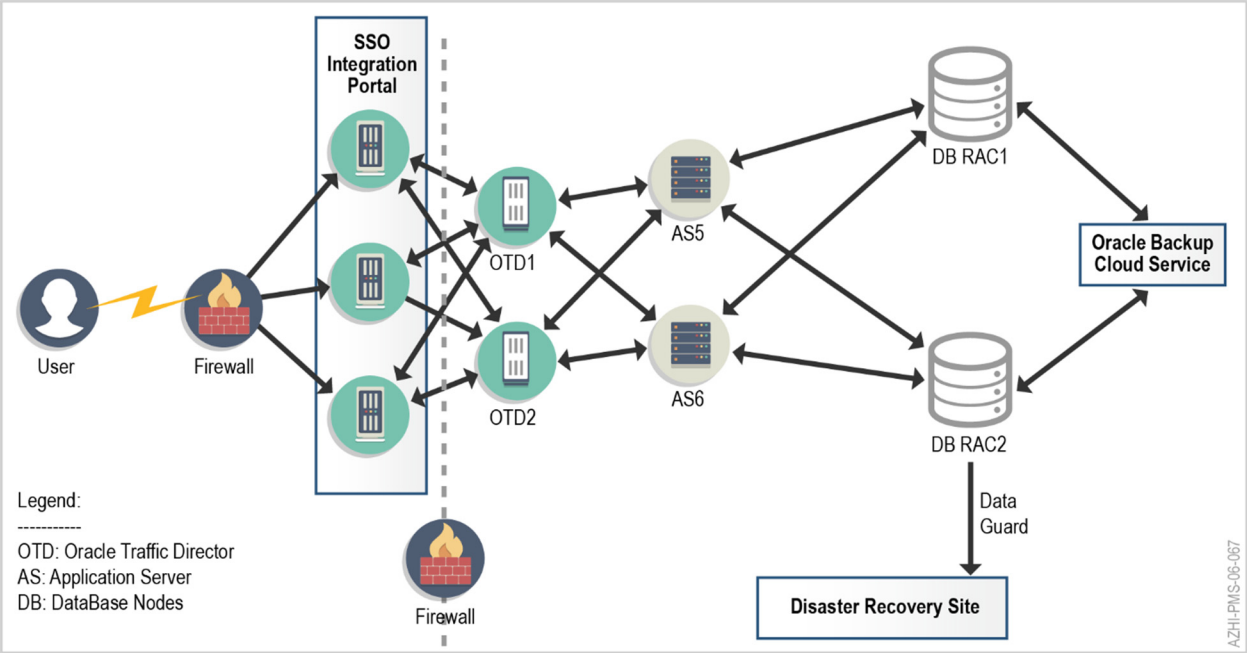


Figure A.6.15-5. High Availability Architecture. Clustered architecture at the application server level and database server level provides load balancing and high availability capabilities.

This high availability architecture in CNSI's evoBrix PMIS solution provides the necessary redundancy and scalability needed to support the system for 99.5% of the time, twenty-four (24) hours a day, seven (7) days a week (excluding AHCCCS/Med-QUEST approved planned downtime). If a downtime windows is required, then CNSI will collaborate with AHCCCS/Med-QUEST to develop and approve a regular monthly maintenance schedule with planned downtime.

System Availability. OEM, HealthBeat, Building Management System (BMS), and Data Center Infrastructure Management (DCIM) solutions, in combination, help to provide the necessary monitoring and reporting capabilities for this high-availability architecture. Please refer to requirement "6.15.1 Performance Monitoring Dashboard" for detailed information on these solutions. Figure A.6.15-6 provides a classification of monitoring tools and their respective infrastructure modules.

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases, Database Servers, SOA Suite and Application Servers
HealthBeat	Application, Interfaces, Web Services and Servers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure A.6.15-6. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

A.6.15.3 Non-disruptive Rules-based Data Restoration [SOW, Section 5.15.5]

The following solutions are a part of the data restoration framework

- **Oracle Data Pump Export/Import:** This tool is used when data needs to be restored at the table level or schema level or record level. This restoration can be done online without disrupting the existing system.
- **Oracle Recovery Manager + Database Backup Cloud Service:** This solution is used for data restoration at the database level or tablespace level. Since it is database level restoration, sometimes it requires downtime but it will be very fast thus making sure that the system is not unavailable for extended period.
- **Flashback Technology:** This solution is primarily used for point in time recovery (incomplete recovery) of the databases and it will involve some level of downtime during the restore process.

A.6.15.4 Software Tools for Routine Monitoring [SOW, Section 5.15.6]

CNSI's evoBrix PMIS solution includes a comprehensive monitoring framework to measure the efficiency of online storage components such as Block volumes and Object Storage as well as to take corrective action plans, when needed. A combination of Oracle Enterprise Manager, Oracle Infrastructure Monitoring Cloud Service, and DCIM provides the necessary monitoring and reporting capabilities covering all layers of online storage access along with capabilities to take corrective actions accordingly. Figure A.6.15-7 provides a classification of monitoring tools and their respective infrastructure modules. This classification of monitoring tools and their associated infrastructure modules forms the backbone of our monitoring framework.

Monitoring Tool	Infrastructure Modules	Corrective Action Plan
Oracle Enterprise Manager	Database Storage Database Backups	Provides corrective action plans related to the defragmentation of tablespaces and placement of datafiles and storage equipment within the database layer.
Oracle Infrastructure Monitoring Cloud Service	Database Storage SOA Suite Storage Application Server Storage	Provides corrective action plans related to file placement strategies for application servers, database servers and SOA suite.
Data Center Infrastructure Management	Infrastructure	Provides corrective action plans related to storage equipment's and software to manage them

Figure A.6.15-7. Monitoring and Performance Reporting Tools for the Storage Layer. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the storage monitoring framework.

A.6.15.5 Data Accessibility from Real-time Interfaces [SOW, Section 5.15.7]

CNSI's CTR framework includes a suite of maintenance tools and performance enhancing tools that are geared towards ensuring that data received from real-time Interfaces will be accessible in the module within three (3) seconds at least 99% of the time. The evoBrix Integrator is used for real time data exchange between different modules in MMIS. Team CNSI's evoBrix Integrator solution uses the Oracle Service Bus (OSB) features within the SOA framework to integrate disparate systems effectively. The solution is capable of handling common industry standard service requests such as SOAP and REST. The use of Web services supports a standards-based XML data exchange to enable interoperability between the system and other external applications to consume/exchange the data.

During Solution, Configuration, and Implementation (SCI) and operations phase, CNSI proactively monitors all infrastructure components as well as defined performance standards to ensure that we meet contract SLAs and performance metrics. CNSI's SLA governance processes establish and document all performance measurement criteria, along with the processes and procedures for monitoring, reporting on, and correcting any deficiencies. CNSI's evoBrix PMIS solution includes a comprehensive and complete system monitoring and reporting framework. This framework ensures that all components are working properly across the system and ensures that the data received from real-time interfaces does not exceed three (3) seconds at least 99% of the time. OEM, HealthBeat, BMS, and DCIM provide monitoring and

reporting capabilities covering all layers of hardware and software components. Figure A.6.15-8 provides a classification of monitoring tools and their respective infrastructure modules

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases, Servers, SOA Suite and Application Servers
HealthBeat	Application, Interfaces, Web Services and Servers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure A.6.15-8. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

A.6.15.6 Response Times for User-initiated Functionality [SOW, Section 5.15.8]

Both the entity-relationship approach and the normalization approach were applied, as appropriate, to develop the evoBrix solution. The degree of normalization also varies. We use higher normalization in the case of tables that are frequently modified by either inserts or updates, enabling easier maintainability. Normalization levels are lower on tables that are used to inquire and report on data to allow for faster query response. Particular sets of tables used heavily in both modification and inquiry pose challenges. Performance and volume testing and, more importantly, implementation experience, were used to reduce impacts to both functions. Team CNSI has conducted specific performance benchmarks testing to determine the throughput of the system and has gradually evolved the performance considerations, as it relates to data modeling and data usage through inquiry, based on the results. The proposed data models and the underlying data store of the evoBrix PMIS solution is currently operational in the states of Washington, Michigan, Illinois, and Utah and is not only purpose-built to handle an array of queries, both simple and complex, but more importantly extensively performance-tested based on implementation and operational experience collaborating with business and technical users to provide the ideal response times for user-initiated functionality.

CNSI maintains high performance standards because of the reasons below:

- **Data Model:** CNSI's evoBrix data model is highly efficient and modular and has been refined and updated based on our past MMIS implementation experiences in the states of Michigan, Illinois, Utah, and Washington. It balances the normalization needs of a data model with the performance needs of large volume transaction processing system. All data items are listed, and then all interrelated rules (known as dependencies) are identified.
- **Data Tier Maintenance Framework**: CNSI's evoBrix PMIS solution is supported by a complete and robust maintenance framework at the data tier called "Centralized Tools Repository (CTR)". This framework is a collection of various tools which are geared towards managing tables, indexes, tablespaces and database objects in the data tier.
- **System Monitoring and Reporting framework:** A comprehensive and complete system monitoring and reporting framework which ensures that all components are working properly across the system. Please refer requirement section 6.15.7, Data Accessibility from Real-time Interfaces, for more information on the monitoring and reporting framework.
- **Data archival and purge process:** A fully tested data archival and purge process that will adhere to the retention timelines of AHCCCS/Med-QUEST's retention period requirements
- **Hosting Platform:** CNSI's PMIS will be hosted in Oracle Government Cloud data centers. Using a mixture of Oracle Cloud Services (PaaS/IaaS/SaaS) and best-in-class on-premises software, this hosting platform provides both horizontal and vertical scalability, thus providing the necessary bandwidth to support the application load.

A.6.15.7 Interfaces Operate in accordance with Specifications [SOW, Section 5.15.11]

A classification of monitoring tools and their respective infrastructure modules is provided in Figure A.6.15-9.

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases, Servers, SOA Suite and Application Servers
SLA Dashboard	Application, Interfaces, Web Services and Servers
HealthBeat	Application, Interfaces, Web Services and Servers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure A.6.15-9. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated application components forms the backbone of the monitoring framework.

A.6.15.8 Alternate Business Site [SOW, Section 5.15.13]

Details regarding the various CNSI business sites, along with a description of these facilities is provided below.

Corporate and Project Support Office: Rockville, Maryland. As CNSI's Global Headquarters, the Rockville, Maryland, facility is a seven-story building housing most of our executive leadership team and those teams central to corporate-wide functions, such as marketing, legal, contract administration and accounting. In addition, this building houses our centralized testing team, support for data conversion, infrastructure personnel and Network Operations Center (NOC).

Technology and Operations Center: Lansing, Michigan. The Lansing, Michigan, CNSI campus consists of three (3) buildings; each facility is expected to continue operation throughout the life of this proposed contract. All buildings have secure entrance and exit points, along with additional security for sensitive areas such as server rooms. This site will perform the role of primary business site for this AHCCCS/Med-QUEST project.

Primary Business Site: Phoenix, Arizona. CNSI will locate key staff and other resources who will collaborate daily with AHCCCS/Med-QUEST project in the AHCCCS/Med-QUEST provided project facility. We understand that we will need to provide any needed equipment such as computers, telephones, printers, or copiers.

These facilities in Michigan, Maryland, and Arizona will provide the additional full-service work environments required for the completion of this proposed contract. In addition to staffing located at those physical facilities identified, remote, telecommuting staff will be utilized to support the delivery of services under the contract. If the primary business site (Lansing, Michigan) becomes unsafe or inoperable, CNSI has all the necessary processes and procedures in place to relocate all critical staff to alternate business sites in Maryland and Arizona within two (2) business days of the primary business site becoming unsafe or inoperable by following the below measures.

- CNSI has identified key personnel required to implement disaster recovery efforts as well as the minimum support team that is required to support the AHCCCS/Med-QUEST solution, scoped out their roles and responsibilities at a high level, and has determined who will assume leadership positions during a disaster recovery process.
- CNSI has prepared a preliminary staffing plan, anticipating the type, number, and level of personnel that will be needed for different recovery scenarios.

- CNSI's Corporate IT system and data is replicated between our Lansing, MI Office and Rockville, MD Office using EMC Data Domain. So even if one site becomes inoperable, the other site will still have the backup data.
- CNSI's business sites in Lansing, MI and Rockville, MD sites have additional office space capacity to support a sudden influx of temporary staff who may be relocating during a disaster recovery scenario.
- CNSI's business locations are geographically apart by at least 100 miles.
- CNSI's business locations are strategically located at least 30 miles to the nearest airport.

A.6.15.9 Error Resolution Timeframes [SOW, Section 5.15.17]

CNSI defines an error/incident as any anomaly in the operational or technical environment that affects delivery of services. When an error occurs:

- CNSI's operations management is notified.
- CNSI Help Desk is notified of the issue and impact to services. The Help Desk opens an incident ticket using OTRS.
    - The ticket describes the event and the module or operational area affected by the issue
    - The Help Desk assigns the Priority Level (i.e., Urgent, High, Normal, or Low) and enters pertinent information
    - Help Desk notifies the appropriate response team
    - Help Desk notifies account management of the issue and the assigned response team
- CNSI assembles the appropriate personnel to conduct an analysis of the issue and define an action plan to resolve the issue depending upon the severity level of the issue.
- Once the course of action is determined, CNSI opens a ticket for internal tracking purposes.
- CNSI assigns the appropriate personnel to conduct its own detailed internal review and obtain the appropriate approvals to commence the resolution. In this meeting, a discussion of the issue, solution, and a review of the scripts, if any, is conducted. Scripts should meet the same standards set by CNSI internally to ensure continuity and reduce the chance of negative effects to the system.
- Once approved, the resolution will be implemented.
- CNSI Operations Management receives periodic updates throughout the incident until the resolution is completed.
- CNSI management notifies the appropriate AHCCCS personnel identified in requirement section 6.15.17.6, Contact Information for Reporting Incidents.
- For all high and critical risks, CNSI documents a Risk Mitigation Plan and the same is submitted to AHCCCS/Med-QUEST within five (5) business days of risk identification.

After the incident or problem has been resolved, CNSI creates an Incident Report. An Incident Report compiles the following information:

- What triggered the incident
- What services are affected by the incident
- A complete timeline of events
- All actions taken to resolve the issue
- Lessons that were learned and ideas for prevention in the future
- List of each person involved at any time throughout the incident
- Summary of each communication
- Attachments, including actual emails and records of phone calls and meetings

A.6.15.10 ESB Data Interfaces [SOW, Section 5.15.18]

The evoBrix's ISR solution uses an enterprise class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations. The evoBrix ISR core architecture leverages ESB features within the SOA framework to integrate disparate systems effectively. CNSI's integration framework is comprised of the below components to integrate the systems with other information systems

- Batch Interfaces via ISR
- Web services vis evoBrix integrator

Batch Interfaces via ISR. CNSI's evoBrix Interface Service Repository (ISR) configurable framework supports automated data exchanges with AHCCCS/Med-QUEST and AHCCCS/Med-QUEST-approved agencies. The framework supports inbound and outbound interfaces and pass-through data exchange within evoBrix and with interface partners. The framework provides features for management of scheduling, auditing, error logging, and escalation along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions. CNSI's evoBrix ISR framework can be leveraged to integrate AHCCCS/Med-QUEST and the external approved federal and state agencies and other authorized trading partners. Data can be transmitted via batch or real-time web services to exchange license information, Provider Credential Service information, Enrollment information from MCOs to AHCCCS/Med-QUEST, and any other required information as part of AHCCCS/Med-QUEST solution. The ISR solution supports secure data exchanges using available standards in the industry such as SFTP, FTPS and SSL.

The key features of the ISR solution include:

- ISR supports the data exchanges between AHCCCS/Med-QUEST and AHCCCS/Med-QUEST approved trading partners by adding the required configurations
- ISR solution handles all industry standard file formats
- Interface schedules, validations, error thresholds, external agency details, email alerts for AHCCCS/Med-QUEST interfaces can be configured in ISR.
- This framework can scale for growth in data volumes and transaction volumes seamlessly and take advantage of the rich features of the underlying hardware and software resources.
- ISR solution is built on scalable and high available infrastructure.
- ISR solution has robust Error Logging and Auditing features. When processing AHCCCS/Med-QUEST interfaces for Credential Verification, License, CMS provider enrollment, National plan and Provider enumeration system and other AHCCCS/Med-QUEST interfaces, errors are logged and the details can be sent to the approved email ids for further correction
- ISR supports modular approach by plug and play of generic code. AHCCCS/Med-QUEST related interfaces can be configured easily
- ISR is Capable of handling large payloads with fail over cluster
- ISR solution enables seamless and simplified connectivity with external agencies using Secure File Transfer and SSL.

Web services via evoBrix integrator. CNSI's evoBrix Integrator solution uses ESB features within the SOA framework to integrate disparate systems effectively. This solution provides an integration backbone that connects core applications and services without directly accessing underlying systems. The evoBrix integrator solution is based on leveraging a series of COTS products that use a services-based integration platform. The evoBrix integrator solution leverages Oracle Service Bus for Service mediation for real-time web services. It supports robust authorization, authentication and validation features using Oracle Service Bus. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix integrator has the ability to change the various attributes of the service without impacting existing clients. The solution will allow Core MMIS to avoid point-to-point communication between different system components and will streamline flow of all information throughout the AHCCCS/Med-QUEST implementation. Here are the key features of evoBrix Integrator

- Leverage light weight Oracle Service Bus built on SOA and SCA principles
- Ability to change the various attributes of the service without impacting existing clients
- Supports Multi Tenancy with easy configurable modules
- Robust Authorization, authentication and Validation features
- Dynamic routing capability
- End-to-end instance tracking with state and error information
- Streamlines business process exception handling
- High availability and scalability of the digitized platform

- Capable of handling common industry standard service requests
- Handles asynchronous callbacks reliably
- Structured conversational interactions with other systems and trading partners

A.6.16 Security [SOW, Section 5.16]

A.6.16.1 Usage Anomalies and User Misuse Reports [SOW, Section 5.16.2]

Oracle Security Monitoring and Analytics (SMA) Cloud Service. Oracle SMA Cloud Service enables rapid detection, investigation, and remediation of the broadest range of security threats across on-premises and cloud IT assets. Security Monitoring and Analytics provides integrated security information and event management (SIEM) and UEBA capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context.

Oracle Log Analytics Cloud Service. CNSI uses Oracle Log Analytics cloud service to monitor, aggregate, index, and analyze all log data from multiple sources. This cloud service includes features that helps to detect usage anomalies and system misuse by enabling users to search, explore, and correlate this data to troubleshoot problems faster and derive operational insight

Oracle Connection Manager (OCM). Access to the Oracle databases by CNSI personnel is monitored and audited using OCM. Oracle Connection Manager is a multipurpose networking solution that offers increased scalability, multiprotocol connectivity, access control, Connection multiplexing and secure network access control. All client and application access to the databases must flow through the OCM. Data download limits are enforced via OCM to prevent mass download of information from the system. This prevents intruders from doing a wholesale data dump limiting exposure if there is an account that has been compromised.

A.6.16.2 Audit Capability [SOW, Section 5.16.3]

Oracle Database Auditing. CNSI uses Oracle database auditing to generate audit records for all users who are accessing the database which is stored in a secure and protected syslog audit trail.

Application Audit Framework. CNSI's evoBrix PMIS solution captures audit information, such as what changes have been made, who made the changes, and when. Based on CNSI's extensive experience in implementing and supporting operations for multiple States, we have refined an approach to support an audit trail of all pertinent events, giving due consideration to storage space and performance constraints. Any errors captured as part of the data updates received from an external interface through the ESB is sent as a back feed to the designated source through an outgoing interface.

A.6.16.3 Encryption of Data at Rest [SOW, Section 5.16.4]

Figure A.6.16-10 provides an overview of all the data-at-rest encryption solutions that are used in CNSI's evoBrix PMIS solution.

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Data Files	Oracle Transparent Database Encryption	AES-256
Database Tier	Encryption Keys	Oracle Key Vault	PKCS#12 file
Database Tier	Backups	Oracle RMAN Encryption	AES-256
Storage Tier	Oracle Data Pump Exports	Oracle Data Pump Encryption	AES-256
Storage Tier	Flat Files (at rest)	Linux eCryptfs	AES-256
Physical Transmission	Disks/Disk Partition	IDRIX VeraCrypt	AES-256

Figure A.6.16-10. Data Encryption Solutions. An overview of Data Encryption solutions that are used in CNSI's evoBrix PMIS solution.

A.6.16.4 Security Warning Banner [SOW, Section 5.16.7]

The application usage banner message is described in Figure A.6.16-11.

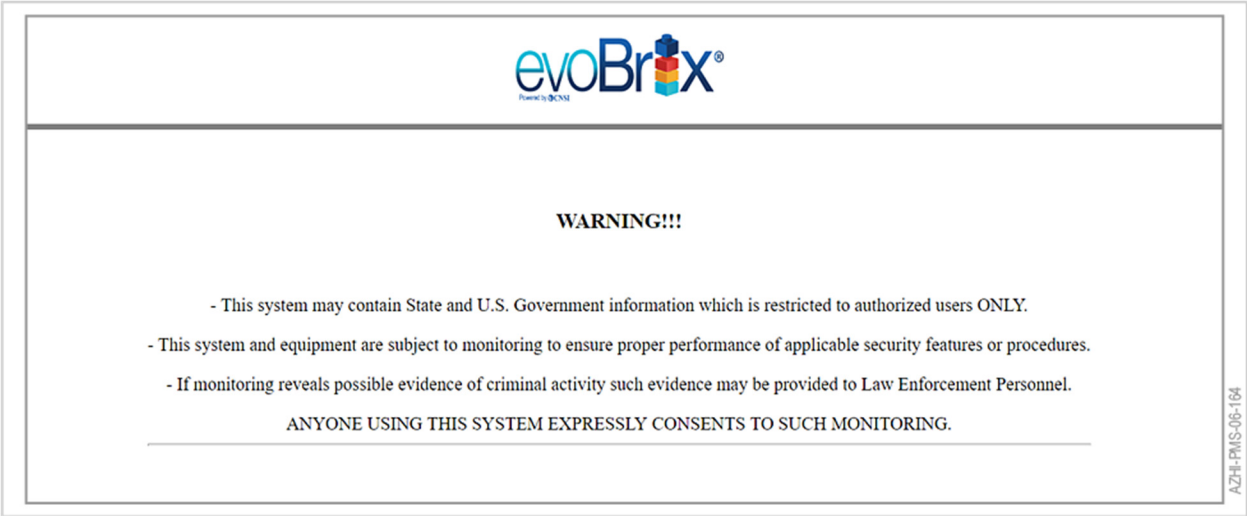


Figure A.6.16-11. Application Usage Banner Message. A security warning banner when logging into CNSI's evoBrix PMIS Application.

Login screens for access to backend systems by systems administrators also displays appropriate security warning banners that is prominently displayed on login and the banner message is displayed in Figure A.6.16-12.

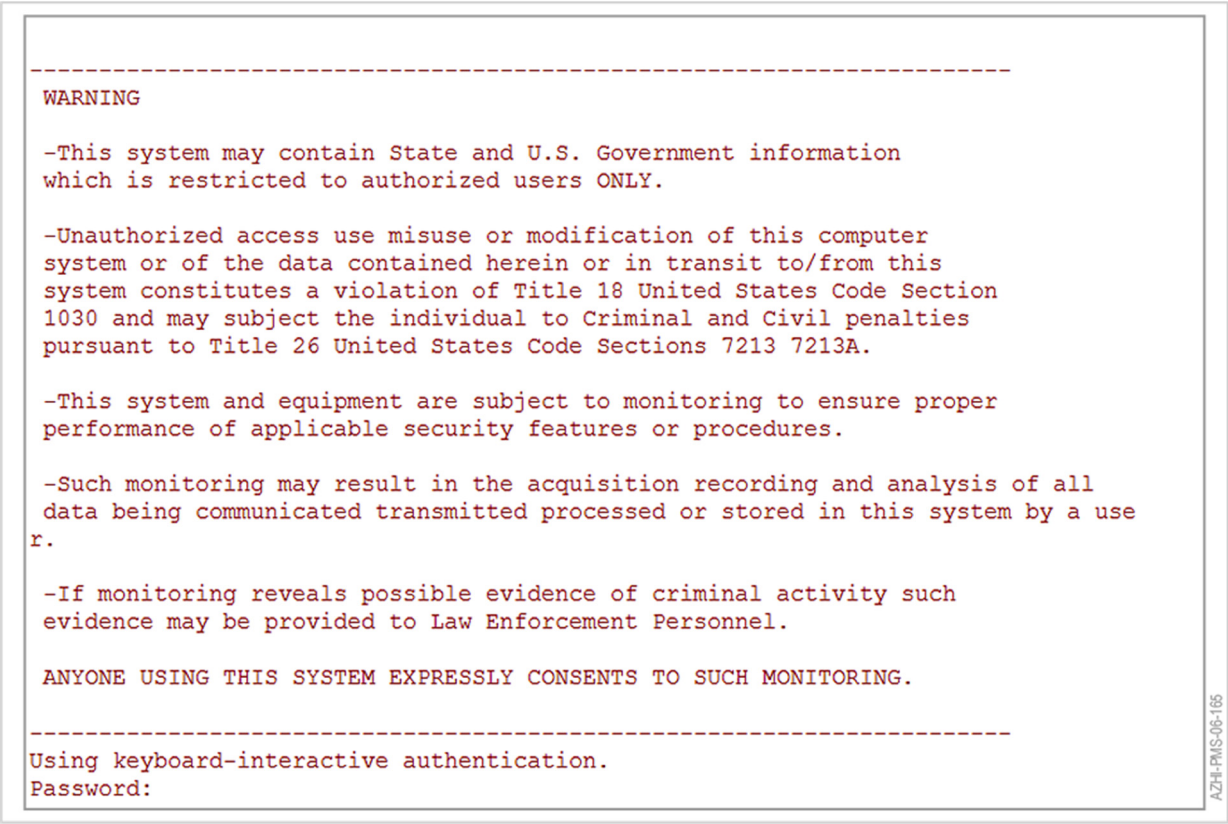


Figure A.6.16-12. Backend System Access Banner Message. A security warning banner when accessing backend systems in CNSI's evoBrix PMIS solution.

A.6.16.5 Annual Security and SSAE-16 Assessment [SOW, Section 5.16.11.6]

CNSI's evoBrix PMIS undergoes security risk assessment covering NIST SP 800-53 Rev 4 standards using NNT's Change Tracker product. Additionally, CNSI's FedRAMP and HIPAA compliant Data Centers perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC).

Annual Security Risk Assessment: Vulnerability and Penetration Testing. Change Tracker's built-in NIST 800-53 report assesses the configured state of our system for compliance with the key NIST Security Controls and performs the necessary vulnerability testing. The result is a simple percentage score with clear remediation guidance, wherever non-compliance is highlighted. Thereafter, Change Tracker provides real-time monitoring of core configuration settings covering installed software, running processes, services and startup states, registry keys, user accounts, audit and security policy, open network ports, and the overall integrity of the filesystem. This risk assessment covering NIST SP 800-53 Rev 4 is conducted in the following situations:

- Annual basis
- Whenever new or modified functionality impacts the security framework or architecture
- Whenever a new vulnerability exists

Additionally, CNSI's hosting platform undergoes penetration testing periodically through an independent third-party security firm. Penetration Testing will be conducted in the following time periods and the resultant test reports will be submitted to AHCCCS/Med-QUEST. If there are any major or critical vulnerabilities, a mitigation plan will also be provided by CNSI to AHCCCS/Med-QUEST.

- Within 6 months prior to implementation
- Annual basis
- Whenever new functionality impacting the security framework gets added or modified

SSAE-16 Assessment

CNSI's FedRAMP and HIPAA compliant Data Centers perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC). The following certifications are in place to provide for the confidentiality, integrity, and availability of the information systems:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II

All the above reports coming out of the security assessment related to systems hosting or environment will be provided to AHCCCS/Med-QUEST within 24 hours of finalizing the report.

A.6.16.6 Security Incident Reporting and Assessment [SOW, Section 5.16.11.8]

CNSI's evoBrix PMIS solution includes a comprehensive security framework for reporting and mitigating security incidents. This solution suite enables rapid detection, investigation, reporting, and mitigation of the broadest range of security threats across CNSI's cloud IT assets. Once these security violations are detected and mitigated, the necessary audit data is preserved and archived using Oracle Archive Storage Classic Cloud Service. Detailed information about these cloud services and tools is provided in response to section 6.16.2, Usage Anomalies and User Misuse Reports. Figure A.6.16-13 provides an overview of these solutions that are used for security incident reporting

Tier	Solution	Features
All Tiers	Oracle SMA Cloud Service	■ Threat Detection ■ Predictive Analytics ■ Automated Incident Response

Tier	Solution	Features
		■ Simplified Monitoring and Reporting
All Tiers	Oracle Log Analytics Cloud Service	■ Topology-Aware Exploration ■ Efficient Machine Learning ■ Smart Clustering ■ Insightful and Custom Dashboards ■ Light Touch Aggregation
Database Tier	Oracle Connection Manager	■ Connection Multiplexing ■ Access Control and Source Routing ■ Firewall Proxy Support ■ Multiprotocol Support

Figure A.6.16-13. Security Incident Reporting and Mitigation Solutions. An overview of solutions that are used for security incident reporting and mitigation along with their relevant features.

As specified in the Business Associate Addendum, CNSI affirms and agrees to maintain compliance with current Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements unless otherwise noted. HIPAA and HITECH established a set of federal standards intended to protect the security and privacy of PHI, and impose requirements related to the use and disclosure of PHI, appropriate safeguards to protect PHI, individual rights, and administrative responsibilities. HIPAA requires entities that handle electronic PHI (ePHI) to implement policies necessary to secure such information. In addition, the HITECH Act includes provisions that require organizations that store ePHI to implement procedures to report the breach of unprotected ePHI. Due to the importance of maintaining compliance to these standards, CNSI performs regular assessments to protect the confidentiality, integrity, and availability of the information systems. More specifically:

- Administrative Safeguards security includes the overall security management process; assigned security responsibility; workforce security; information access management; security awareness and training; security incident procedures; contingency planning; evaluation; and business associate contracts or other arrangements
- Technical Safeguards security includes audit controls, integrity, personnel or entity authentication, and transmission security
- Physical Safeguards security includes facility access controls, workstation use, workstation security, as well as portable devices and media controls
- Policies and Procedures and Documentation Requirements implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications, or other requirements

A.6.16.7 Role-based Security [SOW, Section 5.16.11.13]

Figure A.6.16-14 provides an overview of different compliance factors that are built into the CNSI's evoBrix solution to enforces the below required security controls.

Security Control	Compliance Factors
Requires a unique sign-on (ID and password)	Each system administration account/password is unique Each end user account/password is unique
Supports a user security profile that controls user access rights to data categories and system functions	CNSI evoBrix PMIS solution use RBAC policies defined in our applications to control access to system functions thus satisfying the separation of duties principle based on roles.
Permits supervisors or other designated	CNSI requires verification from the State and/or designated stakeholders

Security Control	Compliance Factors
officials to set and modify user security access profile or group access	before account creation is initiated. Upon verification, CNSI systems provide ability for authorized individuals to modify user security access profiles or group access through screens.
Mandatory Password standards	■ Enforce minimum password requirements compliant with State-provided security policies ■ Allow a user to change his/her password at any time. ■ Have mandatory security questions for the user to answer for username and password validation in case of any user requested changes.
Alerts appropriate staff authorities of potential violations of privacy safeguards, such as inappropriate access to confidential information	The evoBrix PMIS solution notifies the systems team via email of potential risks and violations detected by our automated systems tools.

Figure A.6.16-14. Standard Access Controls Configuration. CNSI collaborates with the State to ensure RBAC policies align with existing AHCCCS/Med-QUEST policies.

A.6.16.8 Enforcement of Password Policies [SOW, Section 5.16.11.14]

Figure A.6.16-15 provides a complete listing of password guidelines that form an integral part of CNSI's password policy. These guidelines surpass the minimum password requirements set by AHCCS/Med-QUEST and we can modify the password policy to meet any new State-provided security policies.

Password Parameter	Description	Value
Failed Login Attempts	This is the number of failed login attempts before locking the user account.	3 times
Password Lock Time	This is the number of days that must pass before an account is unlocked.	1 day
Password Life Time	This is how long an existing password is valid.	60 days
Password Reuse Time	Number of days before which a password cannot be reused.	30 days
Password Reuse Max	Number of password changes required before the current password can be reused.	30 times
Password Reset Time	Number of hours before which a password cannot be reset.	24 hours
Password Minimum Length	Minimum password length	8 characters
Password Complexity	Contain characters from 3 of the following 4 categories a. English uppercase characters (A through Z) b. English lowercase characters (a through z) c. Base 10 digits (0 through 9) d. Non-alphabetic characters (for example, !, $, #, %) Does not contain the user's account name or parts of the user's full name that exceed two consecutive characters	

Figure A.6.16-15. Password Guidelines. A complete listing of password guidelines within CNSI's password policy.

A.6.17 Project Governance [SOW, Section 5.17]

Not applicable

A.6.18 Project Management [SOW, Section 5.18]

Not applicable

A.6.19 Training [SOW, Section 5.19]

Not applicable

A.6.20 Testing [SOW, Section 5.20]

A.6.20.1 Test Environments [SOW, Section 5.20.1]

Figure A.6.20-1 shows our testing approach as a visual hierarchy building from the bottom to the top. Each component of the hierarchy is conducted in its own environment.

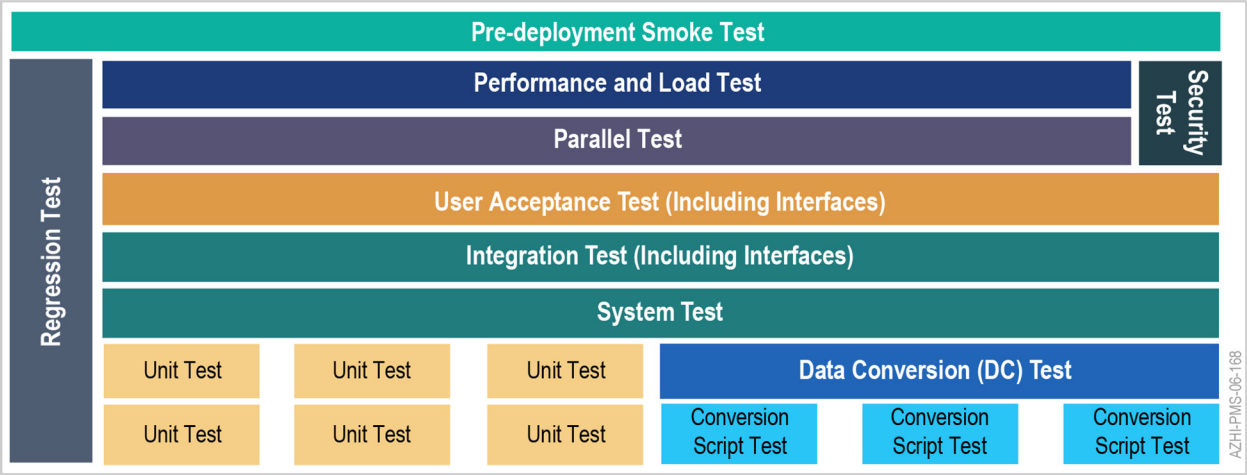


Figure A.6.20-1. CNSI's Test Hierarchy. CNSI's layered testing approach builds from the smallest testable units to full system and user acceptance testing. Security testing is conducted along with UAT, optional parallel testing, and performance and load testing. Regression testing is a continual process across all testing stages.

A.6.20.2 Develop Test Criteria and Algorithms for Expected Outcomes [SOW, Section 5.20.11]

For user-interaction testing, CNSI tests both positive and negative conditions. Positive conditions are those where the tester uses input that is consistent with the goal of the use case and its business rules. Negative conditions are those where the tester intentionally uses invalid data or data outside the range of valid values for the situation being tested. Both positive and negative testing results in executing all alternative flows in the use case and any system messages that evoBrix PMIS produces to guide or correct user input.

For interface testing, we follow the same process of positive and negative testing for both outbound and inbound interfaces. To prove that the business rules for selecting and transmitting data are working as expected for outbound interfaces, we execute the use case logic and compare the output produced to the expectations provided by the interfacing organization before attempting to send the outbound file to the receiving system for test processing. For inbound data files, we execute the use case logic against manufactured data before attempting to test with data from an interfacing organization. We collaborate with the interfacing organizations to ensure that all test conditions for both parties are examined. CNSI uses both manual and automated testing techniques to ensure that every aspect of the system is tested.

A.6.21 Maintenance/Operations [SOW 5.21]

A.6.21.1 Automatic Inclusion of New Data Items in Migration Paths [SOW, Section 5.21.1]

The evoBrix PMIS solution enhancements/software upgrades are closely tied to and follow the evoBrix PMIS operational release processes. All new data items are tied to the evoBrix PMIS functionality which

is version maintained and could be reverted in conjunction with the corresponding operational release rollback. This ensures that once a new data item is defined and operational, the integrity of that data item is maintained through software changes including, but not limited to, upgrades, patches, fixes, defect corrections, and enhancements.

The evoBrix PMIS solution's adaptability and extensibility capabilities will allow AHCCCS/Med-QUEST to add new functionality and modify existing functionality due to changes in policies, mandates, and business needs providing the necessary agility for the Medicaid enterprise. Key capabilities in this area include:

- Adaptability to business process changes via configurability by leveraging rules-based architecture utilizing our rules engine, RuleIT.
- Adaptation and extensions of business rules, via rules configurator and rule authoring tools.
- Automation of business processes via workflow services.
- Business process configurability and workflow management via workflow enablement tools.
- evoBrix Configurator supports configurability of business process variations and changes and extending business rules via meta-data driven design. Extensible Message Management for application and business messages.
- Configurable user interfaces and services.

The evoBrix PMIS solution is also scalable to accommodate any additional data elements introduced due to changes in existing processes, new functionalities, and new interfaces. The solution uses the concept of flexible (flex) fields in the applicable transaction tables to handle new element additions/customization, reducing the changes to the underlying code. Instead of defining the actual attributes/fields for certain tenant-specific business elements directly in a target entity, the flex-field provides logical placeholders. CNSI's evoBrix PMIS solution team will define what those flex fields should store based on AHCCCS/Med-QUEST's business needs (i.e., defining the meta-data details), whether they should be mandatory or optional, the formats/lengths/precision/scale, the default value (if any), and the order in which the flex fields are to be displayed. A flex-field table's sole purpose is to not only reuse it for multiple tenants/States for accommodating a specific business function depending on the tenant-specific usage, but to be able to provide support for future business needs for a given State without adversely impacting the underlying data structures that house the operational data.

Figure A.6.21-1 shows a sample transactional entity, PROVIDER_DETAIL, with a "numeric" flex-field (FLEX_FIELD_NUM1) and the configuration of this flex field for storing an additional phone number for one tenant and the reuse of that same flex-field for storing an additional fax number for another tenant or potentially store additional data elements for future expansion within the AHCCCS/Med-QUEST Medicaid enterprise.

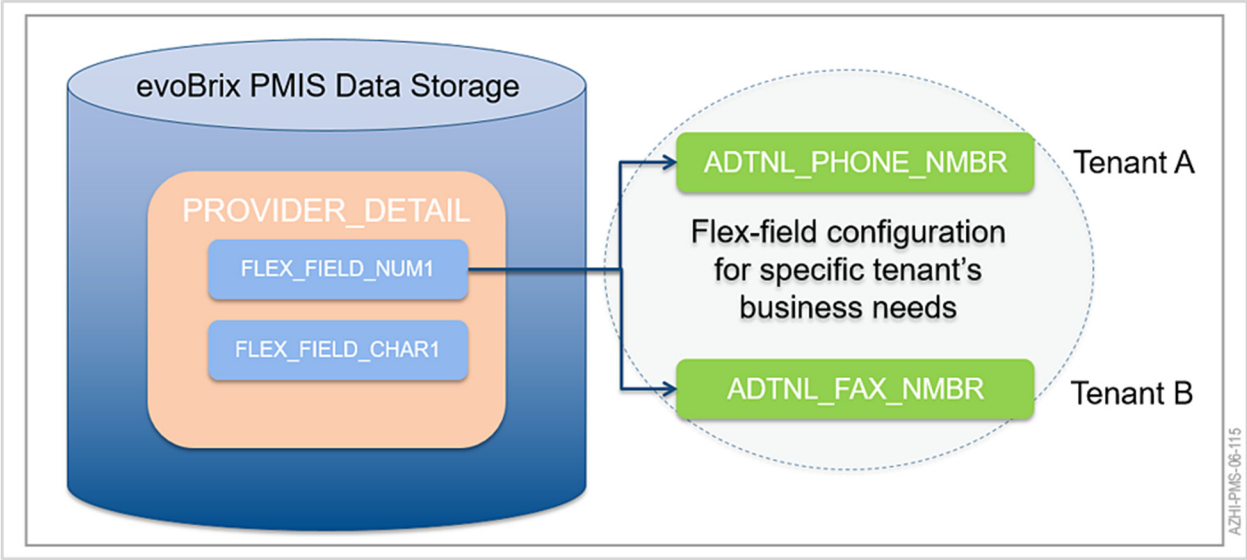


Figure A.6.21-1. Support for Flex-fields. CNSI's evoBrix PMIS solution supports the use of flexible (flex) data fields to accept new and incremental data items from AHCCCS/Med-QUEST module components without adversely affecting the operational system in migration paths during software upgrades.

A.6.21.2 Consistent Use of Acronyms and Codes [SOW, Section 5.21.2]

CNSI's Cloud evoBrix solution utilizes generic frameworks and codes to handle business functions widely used within the system. For example, a generic model framework referred to as Message Management Framework (MMF) is used to maintain and interact with application to generate messages and correspondences. MMF addresses the need to streamline application and system messaging by following a universal framework across various modules in the evoBrix PMIS solution. This is a multi-tenant, multi-language compliant framework that dynamically builds messages based on configurable pre-defined parameters stored in the MMF configuration data mart. This approach helps messages and parameters to be easily configured without having to alter the program code. Figure A.6.21-2 shows the nomenclature that is used to drive the configuration of messages in the evoBrix PMIS solution using the Message Management Framework.

Various message categories are handled by MMF including, but not limited to:

- Application Message - Warning/errors related to the application screens or operations
    - Services Validation Message
    - Persistence Validation Message
    - Message Encrypt Validation Message
- Security Message - Authentication/ unauthorized access related messages
    - Authentication Validation Message
    - Application Access Validation Message
    - Unauthorized Access Validation Message
    - Validation Message - Any generic validation that doesn't conform to a specific function
    - Tenant Validation Message
    - Login Validation Message
- Other Generic Messages

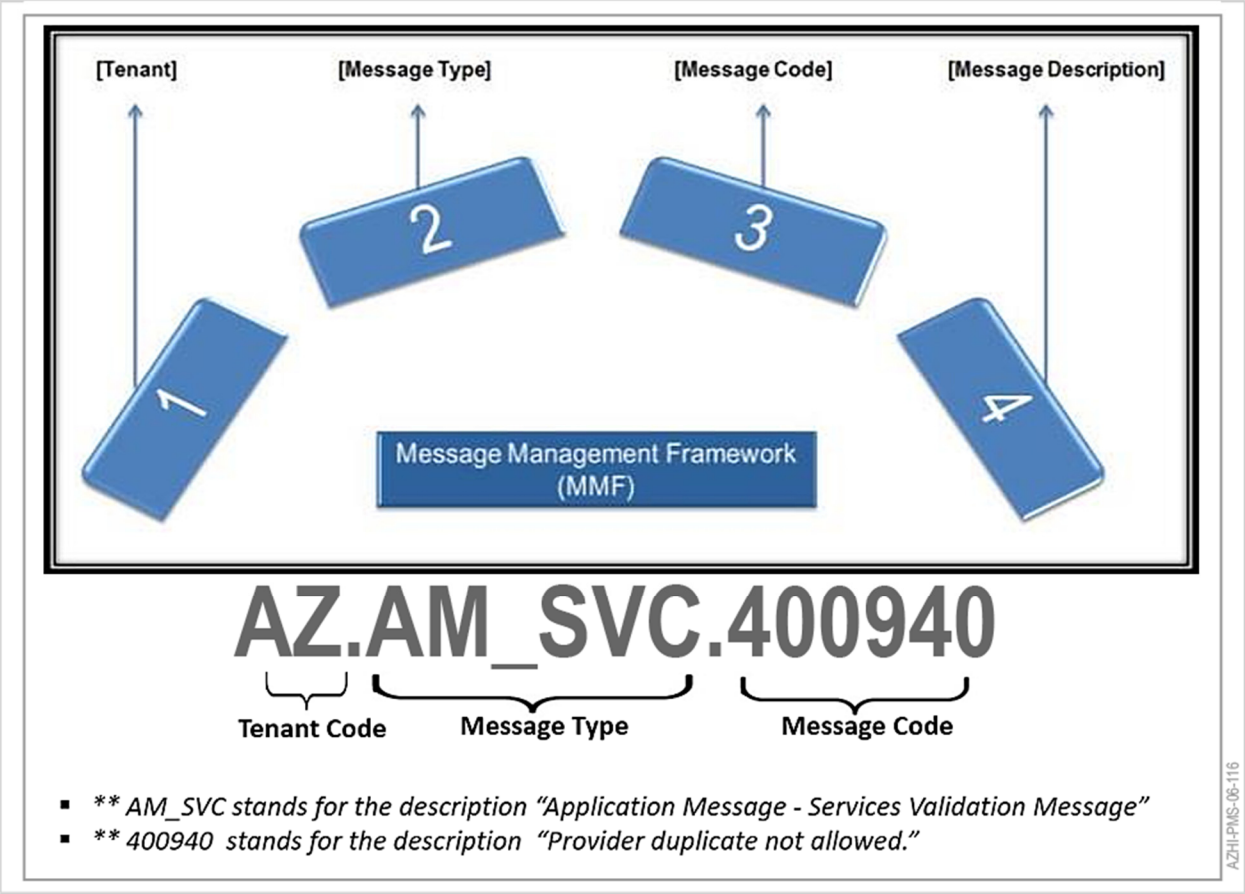


Figure A.6.21-2. Message Management Framework. The CNSI evoBrix Message Management Framework (MMF) supports the configuration of messages in the PMIS solution that demonstrates the consistent and streamlined use of code and acronyms.

A.6.21.3 Effective-dated Table Updates [SOW, Section 5.21.3]

Figure A.6.21-3 illustrates the concept of slicing/dicing a data record using effective dates to accommodate a data change with versioning support. Versioning is implemented using a combination of the following attributes:

- Effective Date: The transaction date on which the updated information was added to the evoBrix PMIS solution
- From date: The start date of effective period of the updated information
- To date: The end date of effective period of the updated information
- Operational Flag: A flag that shows whether the system is actively using the information (Active) or has been "soft-deleted" and is retained only for historical purposes (Inactive)
- Status: The code identifier that identifies the workflow status of the record (In-Review/Approved/Rejected)

Data Versioning

Treatment Type 'MFS' was created on 11/25/2012 to be in use from 11/25/2012 to 12/31/2999

Treatment Type	Name	Effective Date	From Date	To Date	Operational Flag	Status
MFS	Maxillofacial Surgery	11/25/2012	11/25/2012	12/31/2999	A	2 (Approved)

Event: On **10/01/2013**, the name for this code changed from "Maxillofacial Surgery" to "Maxillofacial Prosthetics" to be used from a future date - **5/13/2014**

Data Versioning - Method #1

Treatment Type	Name	Effective Date	From Date	To Date	Operational Flag	Status	
MFS	Maxillofacial Surgery	11/25/2012	11/25/2012	12/31/2999	I	2 (Approved)	Existing Record
MFS	Maxillofacial Surgery	11/25/2012	11/25/2012	**05/12/2014**	A	2 (Approved)	New Records
MFS	Maxillofacial Prosthetics	**10/01/2013**	**05/13/2014**	**12/31/2999**	A	2 (Approved)	

Data Versioning – Method #2

Treatment Type	Name	Effective Date	From Date	To Date	Operational Flag	Status	
MFS	Maxillofacial Surgery	11/25/2012	11/25/2012	**05/12/2014**	A	2 (Approved)	Existing Record
MFS	Maxillofacial Prosthetics	**10/01/2013**	**05/13/2014**	**12/31/2999**	A	2 (Approved)	New Record

AZHI-PMS-06-117

Figure A.6.21-3. Data Versioning. CNSI's evoBrix Provider solution supports a comprehensive versioning mechanism to archive historical data changes.

A.6.21.4 Read-only Access to Designated Staff [SOW, Section 5.21.4]

The evoBrix PMIS will provide AHCCCS/Med-QUEST with access to system job and maintenance schedules, job submission queues and provides processing statistics via several system monitoring tools.

System Tools

- evoBrix ISR Interface Scheduling Screens - CNSI developed the ISR solution from the ground up to manage numerous types of data exchanges typical of every MMIS implementation. To facilitate administration, the solution provides features for management of scheduling, auditing, error logging, and escalation along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions.
- HealthBeat Dashboard- Business and System Interactive reporting dashboard and system performance monitoring tool

Interface Scheduling Screens. The evoBrix ISR solution framework supports inbound, outbound interfaces, service mediation and pass-through data exchanges within AHCCCS and AHCCCS approved agencies. The solution also provides configurable screens to administer the various aspects of the AHCCCS interface operations and provides a dashboard for reporting the status of all the scheduled interfaces. After processing provider data, license information and other required transactions with approved agencies, email notifications will be sent to the configured personnel on the status of the interfaces, including audit details of the interface.

HealthBeat Dashboards. Indicative of CNSI's commitment to service and transparency, our solution also includes the HealthBeat Dashboard and monitoring tool, which provides AHCCCS with configurable, automated, and real-time visibility into business and system operations, SLA compliance, operational events, and system monitoring. Figure A.6.21-6 represents a few screenshots of the HealthBeat real-time performance statistic and a snapshot of a calendar showing the maintenance activities and jobs scheduled for a given month.

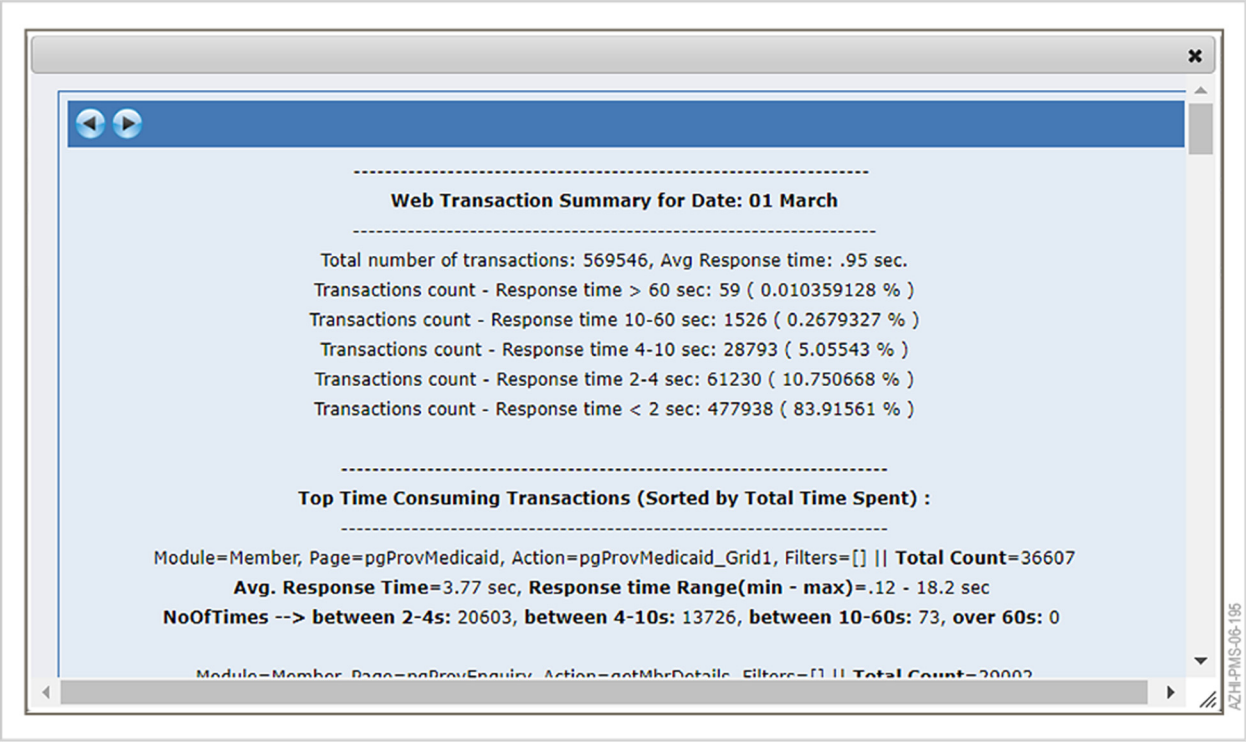


Figure A.6.21-4. Sample HealthBeat Screen. HealthBeat presents real-time performance statistics.

Figure A.6.21-5. Sample HealthBeat Screen. HealthBeat presents real-time performance statistics at a glance.

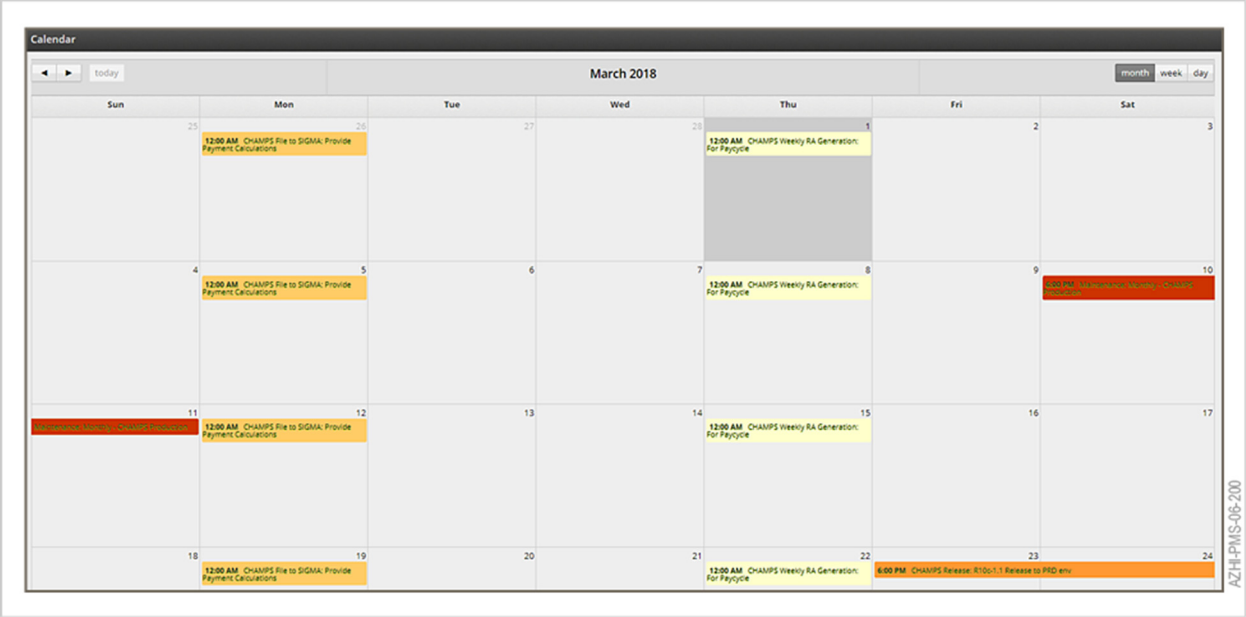


Figure A.6.21-6. Sample HealthBeat Screen. A snapshot of a calendar showing the maintenance activities and jobs scheduled for a given month.

The HealthBeat tool provides a comprehensive application activity monitoring framework along with the capability to facilitate continuous process improvement. As the system handles each process, it collects process-related data in the data store. This data is then used to display the process dashboard and provide visibility to the process metrics and the health of the operation. The system uses workflow-based analytics to provide feedback on potential bottlenecks and application performance issues. Thresholds are configured to display performance in the traditional “red,” “yellow,” and “green” dashboard status. CNSI operations staff sets appropriate thresholds during service design. Thresholds that have AHCCCS visibility will be reviewed with AHCCCS to meet our commitment for transparency.

Related to system monitoring, HealthBeat reports accurate data on items such as end-user response time, CPU utilization, and hourly load averages on different servers. This allows the AHCCCS and CNSI to see the system from a higher point of view and help make informed, strategic decisions on daily operations or future changes in policy and programs. Application management and monitoring, web services management, systems management and monitoring, network management and monitoring, performance monitoring, and event monitoring are all managed via the framework of HealthBeat. Figure A.6.21-7 shows how HealthBeat monitors system resources of real application clustered (RAC) databases.

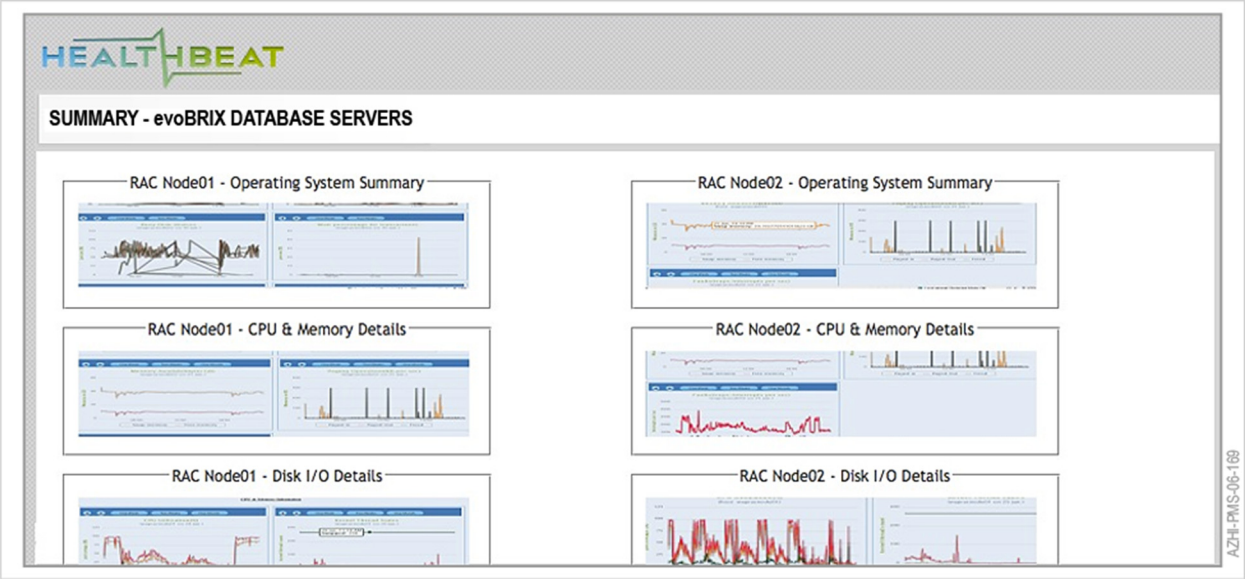


Figure A.6.21-7. HealthBeat for System Monitoring. Monitoring of clustered databases.

HealthBeat also provides various reporting mechanisms, including dashboards and graphs, that can be used to report on the metrics associated with performance standards. Team CNSI uses the HealthBeat tool to collect and report on final performance measures and standards. HealthBeat uses automation to extract, analyze, and report data from various business processes and systems, and to provide a centralized reporting database. This tool provides a robust interface to the various AHCCCS components for gathering and compiling data, allowing near-real-time access to workload and system performance information.

Operational management staff regularly monitor data displayed through the dashboard and can proactively respond if performance indicators begin to decline. In this way, Team CNSI can implement corrective actions before a “red flag” situation occurs. In addition, email alerts are established to notify appropriate Team CNSI and State staff based on configured exception thresholds. Team CNSI also compiles information collected through HealthBeat and summarizes it in our regular reporting mechanisms, including statuses and required workload reports.

The tool produces visualizations of data in various formats, including dashboards and graphs that provide quick summaries for trending. Figure A.6.21-8 shows the HealthBeat architecture that is configurable and automated.

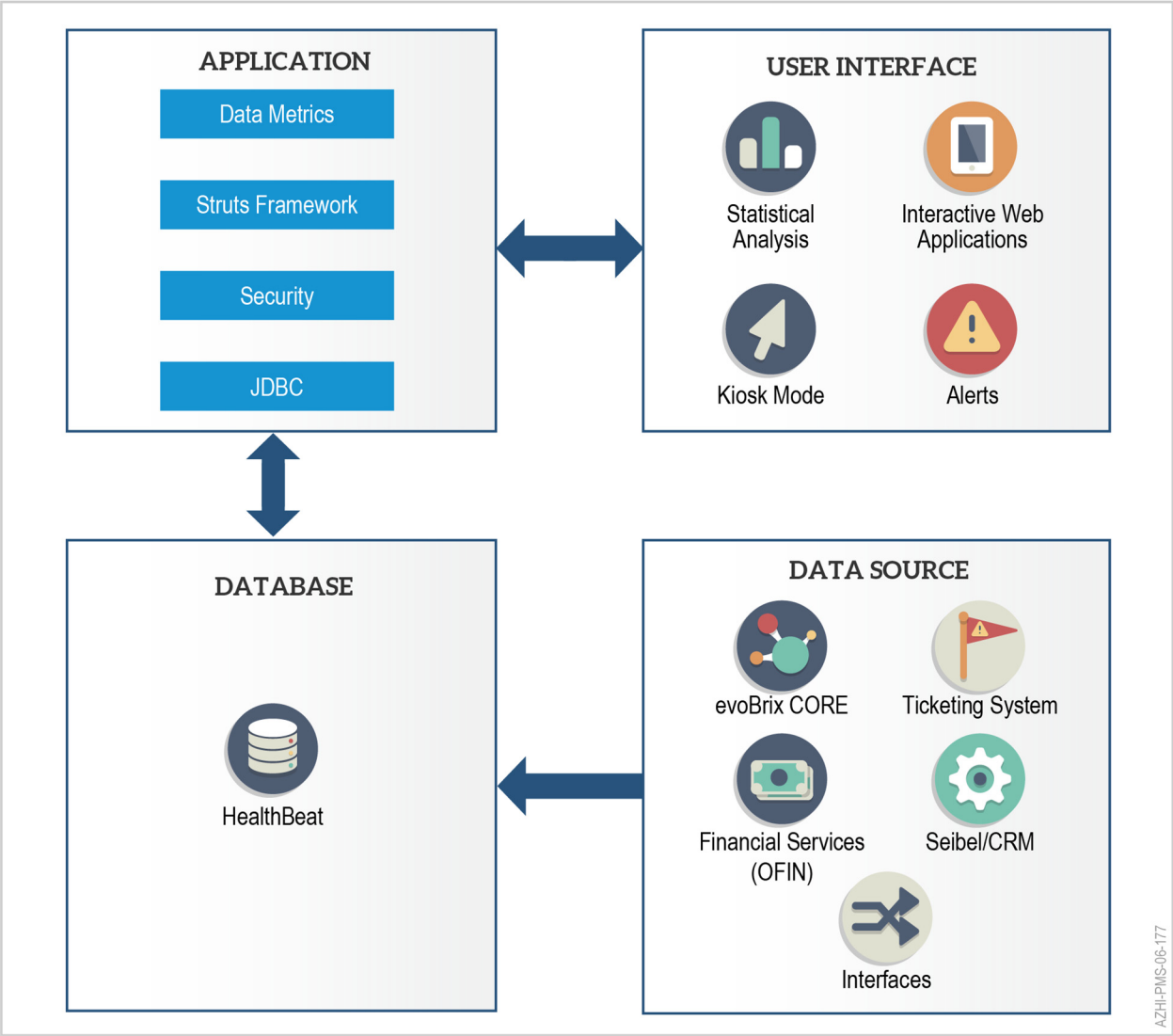


Figure A.6.21-8. HealthBeat Architecture. Provides AHCCCS with configurable, automated, real-time visibility into business operations.

Proactively monitoring the health of operations enables CNSI to be more predictive, rather than reactive, in the provision of our services. However, it is essential that up-to-date metrics be available to provide us with the visibility needed for conducting this proactive monitoring. For these purposes, CNSI uses our HealthBeat solution as the operations dashboard to monitor business processes and system performance. Supporting performance measures that are aligned to MITA business processes, HealthBeat is in production in the states of Michigan, Utah, and Washington. In addition, the Centers for Medicare & Medicaid Services has implemented HealthBeat to monitor operational data related to their interaction with insurers on health exchanges. Over 120 metrics, including SLAs, will be available to AHCCCS through HealthBeat.

HealthBeat is central to our commitment to collaboration, transparency, and accountability. Developed by CNSI as our operations dashboard, HealthBeat provides optimized, configurable, automated, and near real-time visibility into business operations through well thought-out and presented dashboards organized by business area. HealthBeat provides aggregation, analysis, and ongoing performance monitoring data to stakeholders in the form of interactive scorecards, dashboards, and drill-down functionality.

A.6.21.5 Ability to Terminate, Reverse, or Back Out a Software Update [SOW, Section 5.21.5]

Most of the configuration changes to the solution will either be part of the source code binary bundle or a configuration change to a COTS product. Any changes made to the source code are recorded in the version control system that is packaged together when time comes for code promotion from one environment to another, all the way up to Production. At any given point, if an issue is found as part of a software update made either to the source code or the underlying COTS product, an attempt is made to diagnose and fix the issue. If that is not an option, the change is rolled back, actions are recorded in the appropriate version control tool, and the build is repackaged using the automated framework and is tested again and promoted upon successful validation. Figure A.6.21-9 shows a checklist form that is used for verification and validation of all the changed CIs during every Production release.

Project:	MIMMIS	
Date:	Start: 3/25/2015	End: 3/26/2015
Time:	Start: 7:00pm	End: 2:00am
App Deployment Summary:	EAR: MIMMIS_20160324_W_1.0_2330.ear	XESERVER Jar: MIMMIS_20160324_1815_EDI_1.0_2330.jar
Tickets:	1. CNSI00032636 2. CNSI00032637 3. CNSI00033175 4. CNSI00033529 5. CNSI00033621 6. Click here to enter text. 7. Click here to enter text. 8. Click here to enter text. 9. Click here to enter text. 10. Click here to enter text.	Special Steps: Click here to enter text.
DB Deployment Summary:	DB Jar: DB_MIMMIS_20160324_1.0_2331.jar	R.E. Dumps: 1. Exp_prdmmisrecl_ruledev_6.2.58.dmp 2. PRDMMISREPR_51_040216.dmp 3. Click here to enter text.

AZHI-PMS-06-158

Figure A.6.21-9. Snapshot Checklist of Various Types of CIs. Representation of various types of CIs such as Application, Database, and Infrastructure changes that are packaged and verified among various teams before and after Production release.

A graphical representation of the steps followed along with the various teams that participate through the lifecycle of the change request is shown in Figure A.6.21-10.

There is a comprehensive check performed by the Configuration (Functional)/Development Team in coordination with the Release Team at each stage of code promotion from one Test environment to another to make sure that all the configuration changes promised for a given release is available in the bundle.

This page intentionally left blank.

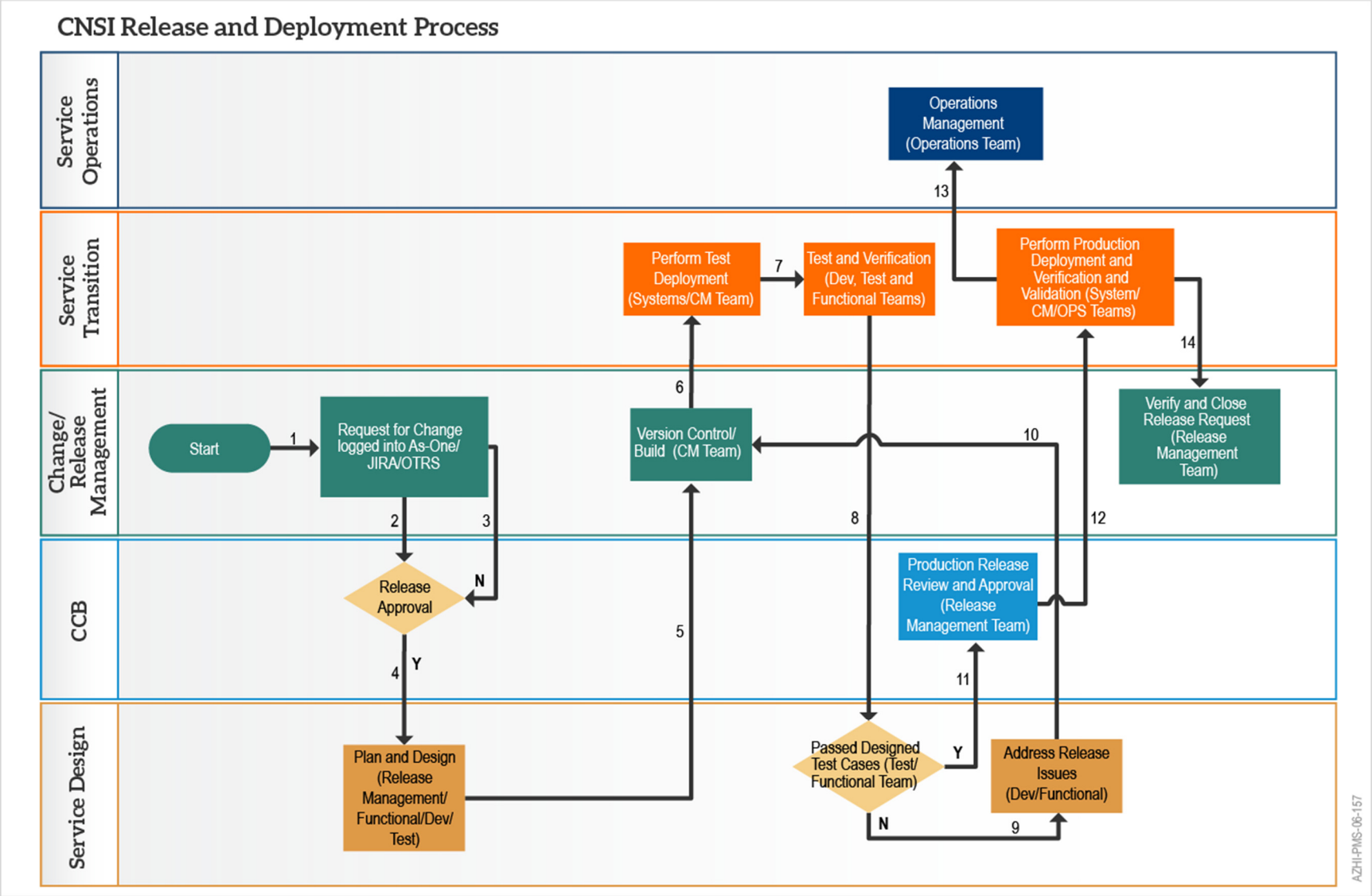


Figure A.6.21-10. Graphical Representation of Configuration Change Validation and Verification. Depicts the process flow from the request initiation to closure.

This page intentionally left blank.

When the time comes for code-promotion to Production, a comprehensive/exhaustive check is performed, independently of each other, by the SCM Team and Configuration (Functional)/Development Team in coordination with the Release Management Team, and the lists are reconciled.

Once the code-promotion activity is complete in Production, another exhaustive round of checks is performed to validate/verify the configuration changes across each of the module/COTS product that was changed during the release process by authorized personnel across Configuration (Functional), Development (Operations) Teams. The typical areas of checks cover Application Screens, Database, Interfaces, Webservice, Reports, and any infrastructure changes at a minimum.

Once the systems are brought up, there is a comprehensive non-intrusive sanity check performed by the Operations/Configuration (Functional) teams to make sure all configuration changes planned for the release are applied and working as desired. The Release activity is marked as complete with necessary notifications to the concerned stakeholders after this last step of non-intrusive checks. A similar process is followed during every major release in lower environments also.

A.6.21.6 Authorized Users Allowed to Sequence Multiple Jobs [SOW, Section 5.21.6]

The ISR solution in evoBrix PMIS triggers multiple dependent jobs in a sequence after the successful completion of the parent job, as depicted in Figure A.6.21-11

Inbound Interface Completion Acknowledgement (ChildWaiver from DCH[DCHC001.4404.20180206201618.dat])

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

**********Do Not Respond To this email**********

Interface ChildWaiver from DCH (1015.10) was successfully completed.

Interface Run Details:

Interface Run SID : 201429512
Interface ID : 1015.10
Interface Name : ChildWaiver from DCH
File Name : DCHC001.4404.20180206201618.dat
Start Time : 02/07/2018 09:07:16 AM
End Time : 02/07/2018 09:07:41 AM
Archive Location : /data/int/MI/1015-10/c/DCHC001_201429512_20180207.txt
Source Records : 1049
Success Records : 1048
Error Records : 1

Dependents List :
EE - LG1 - 2.3.2 Assign benefit plan for eligibility and authorization changes[1105]

Triggered List :
EE - LG1 - 2.3.2 Assign benefit plan for eligibility and authorization changes[1105,201432363]All Errors logged in INTERFACE_RUN_ERROR table.

Error Specifics

(up to 50 errors will be shown here):

Error : 1
Error Type : DATABASE ERROR
Error Description : The transaction did not match a member on file - transaction rejected.

**********Do Not Respond to This Email**********

AZHI-PMS-06-166

Figure A.6.21-11. Sample ISR email notification of triggering the dependents after successful completion of an interface job.

A.6.21.7 Accommodate Varying Retention Periods [SOW, Section 5.21.7]

The data retention framework has evolved via managing technical MMIS operations and has been implemented in the states of Michigan, Washington, Illinois, and Utah. The framework has the capability to address the data retention needs for audit, history, core partitioned, and non-partitioned entities managing the current and historical transactional/operational data for providers. Any provider data that falls outside the defined data retention period would be considered as operationally non-relevant historical data and the data retention framework will physically delete the applicable data record in the evoBrix PMIS solution. CNSI will ensure that any active provider records with the supporting datasets including electronically imaged documents and images, along with 100% of all history for an entity that has been active within the retention periods, will be retained. Data from all supporting inbound and outbound interfaces will be retained for a period as defined by AHCCCS/Med-QUEST.

Although the data retention framework is designed to be implemented at varying frequencies, such as daily, monthly, annual, or ad-hoc, CNSI considers it important to ensure that day-to-day business operations aren't impacted due to the implementation of the data retention policies. The physical deletion of data is managed via a combination of daily archival for high-volume transactional entities followed by a physical removal from the archival entities during the monthly or annual maintenance cycles, and via direct physical daily deletes for low-volume transactional entities, thus balancing the needs of the data retention requirements on one hand and the optimal system performance on the other.

CNSI understands the importance of proper maintenance and storage of data, records and program information, and has experience in record retention and maintenance through ISO 9001:2015 certified record retention schedules used in Medicare operations and program data management in Medicaid operations. Based on experience from multiple MMIS implementations, CNSI is aware that different artifacts mandate different retention periods. In collaboration with AHCCCS/Med-QUEST, CNSI will configure and maintain appropriate data retention schedules for periodic archiving of an array of artifacts such as:

- Transactional and historical provider data
- Interface files
- Supporting documents
- Correspondence and Communications
- Images

A.6.21.8 Import/Export Data with Popular Desktop Applications [SOW, Section 5.21.13]

Under the Manage Provider menu, authorized users can access the robust Provider List feature, an extremely powerful function within the Provider Services business area. Provider List allows the user to search on multiple provider attributes to locate a specific enrolled provider (e.g., NPI) or group of providers sharing a common set of attributes (e.g., zip code and specialty). As shown in Figure A.6.21-12, the Provider List page has three primary filters and two secondary filters. The secondary filters are Identifier and Indicator. The user can save favorite search criteria by selecting the Save Filters button. Saved filters are retrieved under the My Filters dropdown. The list retrieved may be exported to Excel for additional analysis using the Save to XLS button. The sorting functionality on the list page can allow the user to display the data in reverse chronological order.

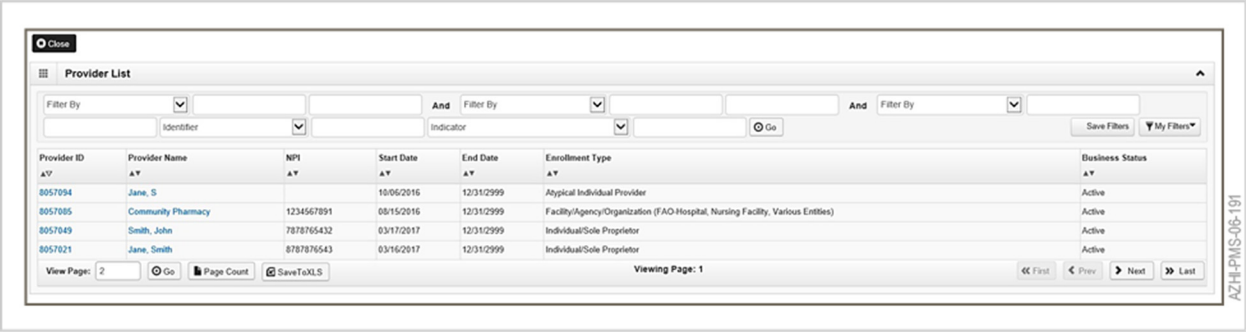


Figure A.6.21-12. Provider List Page Showing Filter Capability. This screen highlights the three major filters, the secondary filters, the Save Filters and My Filter retrievals, and Save to XLS features.

A.6.21.9 Meeting Service Level Agreements [SOW, Section 5.21.14]

CNSI's strategy for monitoring and managing key categories of SLA compliance begins with a robust **SLA Tracking and Reporting process. Our r**eporting solution contains several management and operational reports that are scheduled to run from the Online Transaction Processing System (OLTP) on a daily, weekly, monthly, or quarterly basis, as per business requirements. These reports will be made available to AHCCCS/Med-QUEST through IBM Cognos BI Connection Portal for viewing and retrieval. We also provide AHCCCS/Med-QUEST with configurable SLA management capabilities via an SLA automation tool that provides both CNSI and the State(s) to have visibility into daily system and business functions and their corresponding SLA performances. The tool is also equipped with tracking, reporting, and management capabilities using CNSI's HealthBeat as the front-end dashboard. Highlights of our SLA compliance strategy includes:

- Commitment to Excellence. CNSI brings a comprehensive set of practices, policies, procedures, and processes that will enable us to focus on business value by providing consistent, predictable, and measurable results.
    - Extensive project and quality management plans for accurate and timely deliverables
    - Innovative tools for managing, tracking, and reporting service level agreements electronically
    - Comprehensive business continuity and disaster recovery plans to ensure high availability
- Quality Management. CNSI has an extensive library of process assets, procedures, best practices, and templates to implement our operations management strategy and subsequent processes. Our Project Management team is staffed with years of proven experience in delivering quality and accuracy with iVision360. In addition, our SDLC model has recently underwent CMMI for Development, V1.3 assessment, and was assessed as Level 3 compliant. CNSI continually measures business processes and records, normalizes, and analyzes metrics data to provide insight into our performance. Our experience allows us to create internal metrics to support SLA timeframes.
- High Availability and Disaster Recovery. CNSI's evoBrix PMIS solution architecture, process redundancies, and maintenance procedures provide stability to AHCCCS. We continually review business process availability requirements and aligns them with our ITIL framework. This ensures that cost-effective contingency plans are in place and tested on a regular basis to ensure that the business needs of AHCCCS are met. CNSI's Availability Management plan includes but is not limited to the following aspects:
    - Designing high-availability, redundant systems to support mission-critical applications
    - Utilizing state of the art technology for Disaster Recovery operations
    - Monitoring and reporting high availability to ensure SLAs are being met
- Proactive Support System. CNSI's support staff utilizes a configurable set of tools (e.g., HealthBeat, SLA Dashboard, Automation Oracle Enterprise Manager, Building Management System, and Data Center Infrastructure Management) to monitor the system and assist in the day-to-day operations activities to meet SLAs. Our quality support service provides transparency in reporting, fulfilling user

requests, resolving service failures, fixing problems, and carrying out routine operational tasks. CNSI's support structure consists of the following areas to ensure quality and proactive support is provided to AHCCCS.

- Project Teams
- Call Center
- Help Desk/Operations Support
- Infrastructure

- Innovative Solutions. CNSI establishes solutions in all areas and phases of implementation of the PMIS solution for measurable performance standards. Our performance strategy is also about monitoring performance measures with our SLA Automation tool and reporting dashboard, HealthBeat, in addition to other operations monitoring tools and reports. Focusing on metrics enables CNSI to make data-driven decisions and be accountable for our performance.
- The following sections outline our strategy for monitoring and managing key categories of SLA compliance.
- **SLA Tracking and Reporting.** CNSI's reporting solution contains several management and operational reports that are scheduled to run from the Online Transaction Processing System (OLTP) on a daily, weekly, monthly, or quarterly basis, as per business requirements. These reports will be made available through IBM Cognos BI Connection Portal for viewing and retrieval. The report outputs are archived and integrated into IBM Cognos BI Content Store and could be retained according to pre-defined retention policies. The daily and weekly reports, though they vary according to business requirements, are scheduled within the same day or the next business day of the reporting period and are expected to complete the same day. All monthly reports are scheduled to execute within the first business day following the reporting period and are expected to complete the same day. All quarterly reports are scheduled to execute within the first two business days following the reporting period and are expected to complete the same day.
- **Service Level Agreement (SLA) Automation Tool.** CNSI's SLA automation solution provides AHCCCS with configurable SLA management capabilities. It is one of the tools that allow CNSI and AHCCCS to track and ensure that SLAs are being met. Our solution uses an SLA Automation Engine which is configured to automatically or manually track various SLAs related to system and business functions, such as interfaces and report generations.
- Our solution allows CNSI and AHCCCS to have visibility of daily system and business functions and their corresponding SLAs performances. The tool is also equipped with tracking, reporting, and management capabilities using CNSI's HealthBeat as the front-end application. For example, the tool allows NSI to measure SLAs on interface processing or ticket resolution statistics. This allows CNSI the necessary visibility to monitor performance and provide SLA course correction when necessary.
- The SLA Automation engine runs on a configurable interval to generate service transactions based on the unlimited number of configured SLA's frequency schedules. The system retrieves data input from various source systems via REST or SOAP web service requests for multiple service configurations at any given time. The retrieved data – such as process start/end times and status codes – is matched to the SLA transaction based on unique criteria linked with the reference number, and automatically updated with the provided data. In the event of a non-compliant transaction, notification alert emails are generated and sent to email addresses linked to that service configuration.

A.6.21.10 Automated Application and Network Performance Measuring Tools [SOW, Section 5.21.16]

Figure 6.21-13 provides a classification of monitoring tools and their respective infrastructure modules. All of these tools have built-in alerts and notification features that are configurable through multiple communication methods, such as email, SMS (messages), reports, and dashboards.

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases and Database Servers, SOA Suite

Monitoring Tool	Infrastructure Modules
HealthBeat	Application, Interfaces/Web Services, Servers
Oracle Application Performance Monitoring (APM)	Application, Databases, Network
Oracle Infrastructure Monitoring Cloud Service	Containers and Host Servers, Network, Databases, Application Servers, Load Balancers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure 6.21-13. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

A.6.22 Method of Approach for Software Development/Configuration [Special Instructions, Section 3.1.1]

[redacted]

[redacted]