



VERMONT
**HEALTH
CONNECT**

Find the plan that's right for you.

CGI

Experience the commitment®

D-18 System Design Document

Version 1.0

April 25, 2013

Table of Contents

1	Introduction	1
1.1	Business Context.....	1
1.2	Functional Areas.....	1
1.3	Purpose of this Document.....	2
1.4	Referenced Documents	3
2	Solution Overview	3
2.1	Vermont Health Benefit Exchange Components	4
2.2	OneGate Design Overview	6
2.3	Functional Design	6
2.4	OneGate Technical Design.....	6
3	Assumptions / Constraints / Risks / Scope	9
3.1	Assumptions	9
3.2	Constraints	10
3.3	Risks.....	10
3.4	Scope	11
4	System Design	12
4.1	System Design: Functional Layers.....	12
4.1.1	Functional Layer Components	13
4.2	System Design: Logical Architecture.....	16
4.2.1	Logical Architecture: Presentation Layer.....	17
4.2.2	Logical Architecture: Application and Middleware Layers.....	17
4.2.3	Logical Architecture: Data Layer	18
5	Design Considerations	18
5.1	Design Goals and Guidelines	18
5.2	Architectural Strategies.....	19
5.3	Architectural Drivers	20
5.4	Architectural Goals	20
5.5	Development Methods and Contingencies.....	21
5.5.1	Introduction.....	21
5.5.2	Development Contingency	23
5.5.3	Operational Contingency	23
5.6	State of Vermont SOA Principles Summary	23
5.7	Development Tools.....	26

6	General Testing Approaches	30
6.1	Integrating and Testing with the Federal Hub.....	30
6.2	Integrating and Testing with Carriers	30
7	System Architecture	31
7.1	Design Patterns	32
7.2	SOA Architectural Patterns	32
7.3	Model – View – Controller Pattern	33
7.4	Other Design Patterns	34
7.5	Hardware Architecture	34
7.6	Network Diagram	36
7.7	Non-Production Environment Configuration	38
7.8	Production Environment Configuration.....	39
7.9	vCloud integration.....	39
7.10	Database Services and Storage	39
7.11	Security Hardware Architecture	40
7.12	Additional Infrastructure Requirements.....	40
7.13	Descriptions of Operational/System Environment and Special Considerations	41
7.14	Applicable Laws or Regulations: VT HBE Security.....	42
7.15	Rules of Behavior: Security.....	42
7.16	Review of Security Controls.....	43
8	Security Controls Detail and Comment.....	43
9	Other Hardware Protection and Security Measures.....	43
9.1	Security Devices	43
9.2	Security Zones.....	44
9.2.1	Security Zones – External Zone.....	44
9.2.2	Security Zones – Application Zone.....	45
9.2.3	Security Zones – Database Zone.....	45
10	Performance Hardware Architecture	46
10.1	Architectural Performance Guidelines.....	46
10.2	Software Architecture	46
10.3	Security Software Architecture.....	49
10.4	Functional Activity Logging	49
10.5	Technical Monitoring, Logging, and Auditing.....	50
10.6	Other Security Measures	50

10.7	VT HBE User Authentication, Authorization, and Account Management	51
10.8	Logical Design: Access and Identity Management	51
10.9	Logical Architecture for User Account Management	52
10.10	Logical Architecture for User Authentication and Authorization	53
10.11	Performance Software Architecture	54
11	Records Management	55
11.1	Internal Communications Architecture	55
11.2	System Architecture Diagram	55
12	Data Design	55
12.1	Data Objects and Resultant Data Structures	56
12.2	File and Database Structures	57
12.3	Database Management System Files	57
12.4	Non-Database Management System Files	57
13	User and Machine Readable Interface	57
13.1	Inputs	57
13.2	Outputs	59
	Operational Scenarios	59
13.3	Scenario 1: Pre-Screening Individual	59
13.4	Scenario 2: Individual Enrollment	60
13.5	Scenario 3: Individual - On-going Payments	62
13.6	Scenario 4: Employer – Pre-Screening	63
13.7	Scenario 5: Employer / Employee Enrollment – Employer Side	64
13.8	Scenario 5: Employer / Employee Enrollment – Employee Side	65
13.9	Scenario 5: Employer / Employee Enrollment	66
13.10	Scenario 6: Customer Support	67
13.11	Scenario 7: Weekly Premium Processing	68
13.12	Scenario 8: Monthly Premium Processing	69
13.13	Scenario 9: General Carrier Processing	70
13.14	Scenario 10: Monthly Carrier Processing	73
13.15	Scenario 11: Federal Hub Processing	74
13.16	Scenario 12: Plan Management	77
13.17	Scenario 13: Administrative – End User Security	78
13.18	Scenario 14: Reporting	79
13.19	Scenario 15: Notice Processing	80

13.20	Scenario 16: On-line Documents and Notices.....	81
13.21	Scenario 17: Physical Document Capture.....	82
14	Detailed Design.....	83
14.1	Hardware Detailed Design.....	83
14.1.1	Development Environment.....	83
14.1.2	Testing Environment.....	84
14.1.3	Training Environment.....	85
14.1.4	Client Backup /Recovery Requirements (by host):.....	86
14.1.5	All Network Devices to be Configured.....	86
14.1.6	Site Information.....	87
14.1.7	MPLS Circuit End Points (include both circuits if redundant).....	87
14.1.8	Physical Server and Virtual Machine VLAN Assignment.....	88
14.1.9	VMware Host Management Firewall requirements VMware Management	88
14.2	Software, Security, Performance, Internal Communication, and System Integrity Controls Detailed Design	88
15	External Interfaces	88
16	Glossary.....	89
17	Acronyms	103

Table of Figures

Exhibit 1: Referenced Documents	3
Exhibit 2: OneGate System Requirements and Software Versions.....	7
Exhibit 3: Vermont Health Benefit Exchange (HBE) Functional Layers	12
Exhibit 4: Functional Layer Components.....	13
Exhibit 5: Functional Layer Components.....	16
Exhibit 6: Main Architectural Goal Characteristics	21
Exhibit 7: SOA Principles Acronyms.....	24
Exhibit 8: Descriptive Names of the SOA Principle.....	24
Exhibit 9: Core SOA Principles.....	24
Exhibit 10: Development Tools.....	26
Exhibit 11: Controlled Software Category File Types	29
Exhibit 12: VT HBE Solution Overview	31
Exhibit 13: MVC Architecture	33
Exhibit 14: Other Design Patterns	34
Exhibit 15: VT HBE Wide Area Network.....	36
Exhibit 16: Environment Definitions.....	37
Exhibit 17: Non-Production Environment Configuration.....	38
Exhibit 18: Production Environment Configuration	39
Exhibit 19: Other Design Patterns	40
Exhibit 20: External Zone	44
Exhibit 21: Application Zone.....	45
Exhibit 22: Database Zone	45
Exhibit 23: Software Utilized for the VT HBE Solution	48
Exhibit 24: Technical Architecture Capabilities and Features	49
Exhibit 25: Oracle Identity and Access Management Solution Tools	51
Exhibit 26: User Authentication & Authorization: Solution Overview	52
Exhibit 27: User Account Management: Components	52
Exhibit 28: User Authentication & Authorization: Components by Tier.....	53
Exhibit 29: Component Features.....	54
Exhibit 30: User and Machine Readable Inputs.....	57
Exhibit 31: Pre-Screening Individual (Business Architecture – Flow 1).....	59
Exhibit 32: Pre-Screening Individual (Business Architecture – Flow 2).....	60
Exhibit 33: Individual Enrollment (Business Architecture – Flow 1).....	60
Exhibit 34: Individual Enrollment (Business Architecture – Flow 2).....	61
Exhibit 35: Individual Enrollment (Business Architecture – Flow 3).....	61
Exhibit 36: Individual Enrollment (Business Architecture – Flow 4).....	62
Exhibit 37: Individual On-going Payments (Business Architecture – Flow 1)	62
Exhibit 38: Employer – Pre-Screening (Business Architecture – Flow 1).....	63
Exhibit 39: Employer – Pre-Screening (Business Architecture – Flow 2).....	63
Exhibit 40: Employer/Employee Enrollment – (Business Architecture Employer – Flow 1)	64
Exhibit 41: Employer/Employee Enrollment – (Business Architecture Employee – Flow 2)	65
Exhibit 42: Employer/Employee Enrollment – (Business Architecture Employer/Employee – 3).....	66
Exhibit 43: Customer Support – (Business Architecture Interaction Flow 1)	67
Exhibit 44: Weekly Premium Processing – (Business Architecture Interaction Flow 1).....	68
Exhibit 45: Monthly Premium Processing – (Business Architecture Interaction Flow 2)	69
Exhibit 46: Carrier Processing – (Business Architecture Interaction Flow 1).....	70
Exhibit 47: Carrier Processing – (Business Architecture Interaction Flow 2).....	70
Exhibit 48: Carrier Processing – (Business Architecture Interaction Flow 3).....	71

Exhibit 49: Carrier Processing – (Business Architecture Interaction Flow 4).....	71
Exhibit 50: Carrier Processing – (Business Architecture Interaction Flow 5).....	72
Exhibit 51: Monthly Carrier Processing – (Business Architecture Interaction Flow 1)	73
Exhibit 52: Fed Hub Processing – (Business Architecture Interaction Flow 1)	74
Exhibit 53: Fed Hub Processing – (Business Architecture Interaction Flow 2)	74
Exhibit 54: Fed Hub Processing – (Business Architecture Interaction Flow 3)	75
Exhibit 55: Fed Hub Processing – (Business Architecture Interaction Flow 4)	75
Exhibit 56: Fed Hub Processing – (Business Architecture Interaction Flow 5)	76
Exhibit 57: Fed Hub Processing – (Business Architecture Interaction Flow 6)	76
Exhibit 58: Individual Plan Management – (Business Architecture Flow 1)	77
Exhibit 59: Administrative – End User Security – (Business Architecture Sign Up).....	78
Exhibit 60: Reporting – (Business Architecture Flow 1)	79
Exhibit 61: Reporting – (Business Architecture Flow 2)	79
Exhibit 62: Notice Processing – (Business Architecture Flow 1)	80
Exhibit 63: Online Documents and Notices – (Business Architecture Flow 2).....	81
Exhibit 64: Physical Document Capture – (Business Architecture Flow 3).....	82
Exhibit 65: Development Environment	83
Exhibit 66: Testing Environment.....	84
Exhibit 67: Training Environment	85
Exhibit 68: Client Backup / Recovery Requirements (by host)	86
Exhibit 69: All Network Devices to be Configured.....	86
Exhibit 70: Site Information	87
Exhibit 71: MPLS Circuit End Points	87
Exhibit 72: Physical Server and Virtual Machine VLAN Assignment.....	88
Exhibit 73: Glossary	89
Exhibit 74: Acronyms	103

Revision History

Version	Date	Modified By	Description
1.0	04/25/2013	Scott Cerreta Allan Perry	Initial draft for submission to SOV

DRAFT

1 Introduction

Vermont Health Connect will enable a new solution for Vermonters and Vermont small businesses that will provide simplified access to health insurance at a reduced cost. This project will implement a new technology platform, new software packages, new operational and customer services support functions, and a new public-facing portal as the components of the Vermont Health Benefit Exchange (VT HBE) that will operate in an integrated fashion. This exchange will meet the federally-mandated Affordable Care Act (ACA) requirements and objectives and will be delivered on a timeline that is consistent with the Centers for Medicaid and Medicare Services (CMS) needs.

The Department of Vermont Health Access (DVHA) has contracted with CGI to help ensure that the Vermont Health Connect new solution will be operational and prepared to accept enrollments for the initial Open Enrollment period that begins October 1, 2013. This project will deliver the technology infrastructure that will serve as the marketplace for individuals, families, and small businesses to learn, compare, and purchase private health insurance, calculate any applicable Federal-provided tax credits and/or Vermont provided subsidy, and determine their eligibility for enrollment within Vermont's public health Medicaid plan.

1.1 Business Context

The business goal for the Vermont Health Benefit Exchange is to increase the number of insured by reducing barriers to obtain affordable health insurance. To achieve this business need the Exchange will:

- Help individuals and small businesses identify and purchase affordable coverage
- Increase the number of insured Vermonters by leveraging the use of existing and emerging capabilities in the insurance and information technology industries
- Allow individuals and small businesses to comparison shop, thus facilitating competition among plans on price and quality and make selections that are best for them
- Determine eligibility for participation in the Vermont Health Benefit Exchange, advance payment of premium tax credits, cost-sharing reductions, and Medicaid (under income rules)

1.2 Functional Areas

The functionality of the VT HBE is partitioned into the following six key functional areas:

1. Eligibility and Enrollment

- Employer enrollment in an Insurance Small Business Exchange
- Individual enrollment in a qualified health plan offered through the VT HBE
- Individual enrollment in Medicaid and Children's Health Insurance Program (CHIP)
- Individual appeals and exemptions

2. Plan Management

- Plan certification, recertification, and decertification
- Issuer contracting and integration

3. Financial Management

- Premium determination including premium tax credits, vouchers, and cost sharing
- Plan assessment, reinsurance, risk adjustment, and risk corridors functions
- Individual and issuer reconciliation

4. Customer Service

- Manage responses to information requests and requests for service
- Efficient distribution/management of requests across phone, web, paper, and face to face

5. Communications

- Communications and outreach strategies; content and messaging
- Measurement/reporting of communication effectiveness

6. Oversight

- Federal oversight of Exchange operations
- Insurance Exchange management and operations

1.3 Purpose of this Document

This System Design Document (SDD) describes the State of Vermont's proposed system design solution for a Health Benefit Exchange developed in accordance with the regulations and requirements set forth by the Affordable Care Act (ACA.) Additionally, this solution will be developed and implemented in a way that will help ensure compliance with several government and industry regulatory oversight standards, including those established by the Health Insurance Portability and Accountability Act (HIPAA), Federal Tax Information (FTI), Payment Card Industry (PCI), and the National Institute of Standards and Technology (NIST.)

The SDD describes design goals and consideration and provides a high-level overview of the system architecture. The SDD provides information regarding application components, information models, technology components, security implementation, and information on how these work together. This document serves several purposes including:

- A blueprint for the Vermont Health Benefit Exchange technical solution
- Input for the CMS Detailed Design Review
- Input for further decision making
- A basis for detailed design tasks, development, and testing

This solution design will also establish the initial Services Oriented Architecture (SOA) solution for the State of Vermont. As such, this solution will be establishing several technical capabilities that will result in the need to achieve additional objectives that will also be defined or referenced in this document.

- Input for the State of Vermont Information Technology (IT) Governance policies, procedures, and processes.
- Input for the State of Vermont operational support teams and their associated processes.
- Input for the State of Vermont for potential leverage within other future Vermont healthcare-based applications and the other state functions.

Additionally, at the time of writing this document, the specific requirements for integration with the Federal Hub for the exchange of data with CMS and other Federal agencies continues to be changing. CMS has notified Vermont that the initial set of integration components will be modified to support new requirements; however the specifics and timeline has not been provided.

Consequently, it should be noted that this document has been written with the assumption that future versions will be released and will continue to be updated in future phases, as additional details are clarified concerning business requirements, data exchange specifics, SOA Governance, operational oversight functions, and updates from CMS as additional information becomes available.

1.4 Referenced Documents

The following documents are referenced in this document.

Exhibit 1: Referenced Documents

Document Name	Document Number	Issuance Date
Guidance for Exchange and Medicaid Information Systems	Version 2.0	May, 2011
Exchange Reference Architecture	Version 0.99	March 16, 2011
Collaborative Environment and Life Cycle Governance – Exchange Reference Architecture Supplement	Version 0.91	March 16, 2011
Harmonized Security and Privacy Framework – Exchange TRA Supplement	Version 0.95	March 16, 2011
CMS Technical Reference Architecture – Catalog of Minimum Security Controls for States Supplement	Version 0.1	June 8, 2011

2 Solution Overview

The Vermont Health Benefit Exchange business and functional solution is a fully-integrated technical platform that provides a highly-automated application, and an enrollment and eligibility experience for customers. The ACA's "no wrong door" approach is achieved through a blending of the OneGate, Siebel, and OPA products which supports a streamlined process for Consumers, Navigators, and Brokers.

To meet the ACA Exchange requirements, a selection was made of industry-leading Web-based, commercial-off-the-shelf (COTS) products integrated around a Service Oriented Architecture (SOA)-based Enterprise Service Bus (ESB). The Exchange, through its ESB, will integrate with various outside entities, state and federal systems to satisfy the business goals of operating an e-commerce website offering Qualified Health coverage for Vermont citizens. The Exchange solution architecture and functionality will support both Individual and Small Business capabilities for Vermont. This exchange solution is based on a configurable, COTS-based architecture.

Although there are numerous benefits to this approach, one of the most powerful is the ability it provides the State of Vermont to efficiently leverage resources. For example, rather than having to devote significant project resources to application development efforts, resource efforts can be leveraged to validate state policies and workflows as they are defined and configured. This allows the Vermont Health Benefit Exchange to meet the aggressive timeframe for the initial pilot and deployment to the general public more efficiently and prepares a foundation for the Exchange to evolve as requirements dictate. The Exchange leverages this type of implementation approach as a key advantage as both federal and state legislative policies concerning health benefit exchange are still evolving.

The VT HBE solution provides multiple channels for Vermont's individuals and families to determine their health insurance eligibility through a self-service portal. The VT HBE provides a highly interactive and easy-to-use interface for all applicants (both individuals and employers) and supports the subsequent selection of qualified healthcare plans.

The Vermont Health Benefit Exchange will employ IT system architectures which support the Health Insurance Exchange, Medicaid, and the Children's Health Insurance Program (CHIP) provisions and requirements outlined in the ACA.

The core applications of the VT HBE solution are OneGate, Siebel, and Benaissance (Financial Management) and are explained in the next section of this System Design Document.

2.1 Vermont Health Benefit Exchange Components

The VT HBE will enable Vermonters and Vermont small businesses to provide simplified access to health insurance at a reduced cost. The VT HBE project will implement a new technology platform, new software packages, new operational and customer services support functions, and a new public-facing portal. These components will not only serve as the integrated solution for the VT HBE, but also as the foundation upon which for the State of Vermont (SOV) to build and integrate other state applications.

Enterprise Security – Provides a comprehensive security framework for all components with the solution, including identity management and multi-factor authentication controlling user access. User authorizations will be managed by functional role assignments. The current architecture recommends reuse and extends the security framework available within the VT HBE. The extension will focus on the application user roles. In addition, appropriate encryption and digital signatures will be used to help ensure data exchanges are secure.

Liferay Portal – The Liferay Portal is Java based and runs on any computing platform capable of running the Java Runtime Environment and an application server. It provides a single, secure, and rich user-centered design for VT HBE stakeholder interactions via a Web browser with support for Web 2.0 technologies facilitating collaboration, feedback, interoperability, and information sharing. The VT HBE Portal provides capabilities for public and registered user access compliant with security policies related to authentication, authorization, and channel encryption. Registered users can access their user preferences, check application status, initiate inquiry/correspondence, payments, view transaction status, and look at their current plan/benefits. The Liferay Portal provides the user interface for the VT HBE based on the UX2014 standard provided by CMS. Once the user accesses the VT HBE, data is sent through HTTPS to the Oracle Policy Automation (OPA) and Rules engine to determine access to different functional areas within the VT HBE solution. The Business Rules within the OPA and Rules engine allow VT HBE to determine situations such as when a user is eligible for qualified health plans (QHP), when notifications will be sent to users, and allow users to run reports.

The Liferay portal will also display information from Thunderhead NOW, the notification generation service. Thunderhead NOW sends information to be displayed in the Liferay portal as well as the Siebel CRM Customer Relationship Management (CRM) Modules – Public Sector base, which handles customer-based information such as Help Desk, Email Response, group policies, and Individual coverage.

Over HTTP, the Siebel CRM Modules also provide information to the Oracle Secure Enterprise Search, which also gives information to the Oracle WebCenter to handle content management, document management, and the VT HBE portal.

Business Rules Engine – Oracle Policy Automation (OPA) will be used to generate Business Rules. OPA is a business rules engine that manages external and application-specific business rules. Externalizing business rules from the workflow and application logic provides explicit rule visibility, effective centralized management by business owners, and immediate influence on the solution without incurring any development overhead.

Process Management – The VT HBE solution will leverage a combination of Oracle OPA and Siebel CRM for workflow management. The functionality provided by these components enables the automation of workflows and orchestration of processes associated with eligibility, enrollment, account management, plan and contract management, and financial management processes. Process implementers connect each step of the process to services available through the ESB and assign tasks to specific users.

Enterprise Service Bus (ESB) – In this instance, a combination of Siebel and Oracle ESB / SOA will be used to achieve optimum functionality. The ESB provides the infrastructure for enabling interaction between the various elements of the solution using open standards and interoperability profiles. This infrastructure component is implemented using an ESB supporting discovery of services using the services registry and repository, transformation, and routing of service requests within the enterprise. In ESB architecture, systems and applications interact via messages, which enter and exit service implementations through endpoints. This approach is capable of connecting numerous application endpoints in a “publish” and “subscribe” model which allows for the solution to scale effectively and enables real-time parallel event processing. ESBs combine messaging, Web Services, XML, data transformation, and management to reliably connect and coordinate application interactions. ESB’s eliminate/reduce the need for custom construction of each point of integration. The systems and applications need no awareness of the underlying communication protocols or physical location; they see simple in-boxes and out-boxes. Because of this mapping, services can be upgraded, moved, or replaced without disrupting existing business systems or modifying applications.

Data Management – This component is made up of the structured, semi-structured, and unstructured operational and transaction data repositories. This component comprises the data warehouse, transactional database (user profile, eligibility information, enrollment information, payment information etc.) and the ability to log and monitor transactions. The architecture will provide the capability to develop reports and dashboards for the VT HBE and be delivered via the portal.

Reporting – Oracle Business Intelligence (OBIEE) will be used for report generation. OBIEE provides the capability to generate reports necessary for HIX, State, Federal entities, Employers, and other entities as defined.

Notifications – Thunderhead will be leveraged for communications from the SOV to plan participants, employers, and others. Thunderhead enables the VT HBE to have a high-level of personalization and relevance in communications, with a single engine to manage the delivery of content across multiple delivery channels (for example, print, web, email, SMS, mobile, and social networks).

Data Exchange – This component is being built as part of the SOA architecture to isolate the VT HBE from the external systems. The primary function of the data exchange component is to provide a Plug and Play interface for any external provider who needs to interface with the VT HBE. This helps ensure that external interfaces can be added easily and quickly by following standard interface rules. It provides a secure Web services-based system interface enabling electronic interaction between the VT HBE and the Federal, State, and Insurance Payers. The data exchange layer will also be able to support a batch interface for those systems that require.

1. **Federal Gateway:** This data exchange component will support real-time interface with the Federal Hub to get income and citizenship information. It will also have batch interfaces to support submission of documents to CMS for verification and to accept plan certification information from CMS. It will also perform audit and logging.
2. **Carrier Gateway:** This data exchange component will support both real-time and batch interfaces to numerous Carrier (QHP) systems as part of this solution. It will also perform audit and logging.

Payment Processing – This function will be enabled through a web service integration with Benaissance to execute the VT HBE financial transactions.

Infrastructure – Provides an efficient infrastructure for deploying various components of the solution. The solution could either be deployed in a virtualized infrastructure or in a cloud infrastructure (Infrastructure-as-a-Service) that offers elasticity to meet the varying computing capacity needs for the VT HBE.

Document Management – WebCenter is the software tool that will be used for document management in the VT HBE solution. WebCenter (also known as Oracle Document Management) will be leveraged to store and retrieve documents submitted by the users. This could include a copy of a Birth Certificate, Driver's License, Passport, Utility Bill, Tax Forms etc. to prove citizenship, residency, income, and so on.

2.2 OneGate Design Overview

The platform that OneGate uses is comprised of the following major products:

- Oracle WebLogic
- Oracle Siebel CRM
- Oracle Policy Automation (OPA)
- Oracle Services Oriented Architecture (SOA)/Enterprise Service Bus (ESB)
- Liferay Portal
- Oracle 11GR2 Database

This technology stack is configured to provide the State of Vermont with a platform for supporting Individuals, Small Businesses, Case Workers, Brokers/Navigators, and other stakeholders through an easy-to-use, high-availability online Health Insurance Exchange system.

As previously mentioned, the OneGate design is an accelerator, implemented through configuration steps, allowing policy rules and workflows to be revised by program owners, and using SOA with loosely-coupled interfaces to connect to the State Gateway, Federal Hub, and Insurers.

This section describes the OneGate integrated design in five subsections:

- Functional Design
- Technical Design
- Database Design
- Security

2.3 Functional Design

For more information about the functional design and specific workflows within OneGate, see the Exeter OneGate manuals posted on Ensemble.

2.4 OneGate Technical Design

The OneGate solution leverages Oracle SOA/ESB, Oracle Web Logic, Siebel CRM, Oracle Policy Automation, and the Oracle database to provide self-service portals and integration capability. The Individuals, Employees, Employers, and Brokers/Navigators portals are integral to the OneGate product as well as the Siebel customer relationship management (CRM) call center capability.

The VT HBE system is front-ended by the Oracle WebLogic and Web servers with requests for Liferay portal pages. Oracle SOA/ESB Web services are handled by WebLogic while access to Siebel goes through the web server first then through an adaptor to WebLogic.

The OneGate application features two types of portlets: interview portlets and regular business process portlets. Both portlet types are deployed in Java containers in the WebLogic server and configured within the Liferay portal with associated portal pages used to provide the look and feel. Upon execution of an

interview portlet, the Oracle Policy Automation (OPA) determination engine is invoked and the interview begins. The advantage of using the OPA is that rules can make it easy to alter the interview without changing the configuration of the system or Java coding, and consequently having less costly sustainment.

Exhibit 2: OneGate System Requirements and Software Versions

Tier	Minimum System Requirements	Software
Database	64-bit Oracle Enterprise Linux 5.5 8GB RAM 100GB HD	Oracle Database 11g 11.2.0.1 JDK 7u9
Siebel	64-bit Oracle Enterprise Linux 5.5 8GB RAM 50GB HD	Siebel Business Applications 8.2.2 32-bit Oracle Database Client 11g 11.2.0.1 JDK 1.6+ Oracle WebTier HTTP Server 11.1.1.6
SOA	64-bit Oracle Enterprise Linux 5.5 8GB RAM 50GB HD	SOA Suite 11.1.1.5 JRockit Java JDK 1.6 Oracle WebLogic Server 10.3.5 Oracle Fusion Middleware Repository
Application	64-bit Oracle Enterprise Linux 5.5 8GB RAM 50 GB HD	Liferay 6.1.2 Enterprise Edition JRockit Java JDK 1.6 Oracle WebLogic 10.3.5 OPA 10.4.1

Interview Portlet Design

The OneGate portlets are developed using a Java Model View Controller (MVC) Spring framework with a Hibernate data abstraction layer. The four-tier architecture is implemented as follows:

- Client Tier (Presentation tier or Application tier)
- Web tier, Enterprise JavaBeans Tier (or Business tier)
- Enterprise Information Systems Tier

In the Plan Management java program, the tiers listed above are physically located on the same Java Virtual Machine (JVM) and are developed so that each tier provides a specific type of functionality to the OneGate application.

OneGate Client Tier

The Client tier consists of programs that interact with the user. The Client tier displays a screen and prompts the user for input, and converts the user's response into requests that are forwarded to software on a component that processes the request and returns results to the client program. Java clients can be classified as a Web client, which can be a browser that accesses resources located on the Web tier. The multi-tier clients can access components located on tiers other than the tier where the multi-tier client resides.

OneGate Web Tier

The Web tier accepts requests from other WebLogic servers that were sent using POST, GET, and PUT operations, which are part of hypertext transfer protocol (HTTP) transmissions. The two major components of the Plan Management Web tiers reside on the Web tier and are called by a request from a browser client that operates on the Client tier. The Web tier generates a hypertext markup language (HTML) output stream that is returned to the Web server, which in turn transmits the data to the client.

JavaServer Pages (JSP) is different than a servlet depending on the container that is used. JSP uses custom tags to access the bean.

Enterprise Information Systems Tier

This tier provides a variety of resources and support connectivity to resources, and defines all the elements that are needed to communicate between Java application and non-Java software.

OPA Rule Base Design

Flexibility

The Oracle Policy Automation (OPA) rule base allows the VT HBE to integrate rich, interactive interviews for individual and family application, change of circumstances, and Small Business (SHOP) employer application, into VT HBE onboarding and case-handling processes. This business rule model supports both customer self-service and staff processes. OneGate users are presented with streamlined questions that pertain specifically to them based on their situation, delivering a personalized approach that improves customer experience and satisfaction.

SOA/ESB Composite Design

The OneGate SOA composites are an assembly of services, service components, and references designed and deployed together in a single application within the Oracle SOA/OSB product. Each composite has wiring between the service, service component, and reference enable message communication for processing the information described in XML or other format messages.

The OneGate SOA design includes a mediator service component and a Business Process Execution Language (BPEL) service component, an inbound service-binding component, and an outbound reference-binding component.

The key composite components are as follows:

- Service Components are the building blocks of a SOA composite application. Each service component is hosted in its own service engine container. Messages sent to the service engine are targeted at specific service components. For example, a message targeted for a BPEL process is sent to the BPEL service engine. Service engines that process the message information received from the following service components:
 - ▶ BPEL processes provide process orchestration and storage of synchronous or asynchronous process. You design a business process that integrates a series of business activities and services into an end-to-end process flow.
 - ▶ Business rules enable you to design a business decision based on rules.
 - ▶ Human tasks provide workflow modeling that describe the tasks for users or groups to perform as part of an end-to-end business process flow.
 - ▶ Mediators route events (messages) between different components.
- Services provide the outside world with an entry point to the SOA composite application. The Web Service Definition Language (WSDL) file of the service advertises its capabilities to external applications. These capabilities are used for contacting the SOA composite application components. The binding connectivity of the service describes the protocols that can communicate with the service, for example, Simple Object Access Protocol (SOAP)/HTTP or a Java 2 Platform Enterprise Edition (J2EE) Connector Architecture (JCA) adapter.
- References allow messages to be sent from the SOA composite application to external services in the outside world.
- Wires allow you to graphically connect the following components in a single SOA composite application for message communication:
 - ▶ Services to service components
 - ▶ Service components to other service components

- ▶ Service components to reference

There is a corresponding service engine of the same name for each service component. All service engines can interact together in a single composite.

Siebel CRM Design

The OneGate Siebel HIX specific configuration package has the following components:

- Shell Scripts - shell scripts that are used in the installation process
- iHelp - OneGate seed iHelp XML files
- ADM - Application Deployment Manager XML files that populate OneGate metadata records
- Excel Loader - Microsoft Excel file that populates OneGate metadata records
- Repository - A Siebel repository file (.dat file) that has all the latest Siebel code objects
- Srf - A compiled Siebel Repository file that is used by the Siebel Object Manager
- Logs - Log files generated during the installation process
- Images - Image files
- Css - Cascading Style Sheets (CSS) files
- Swt - Siebel Web Template files

3 Assumptions / Constraints / Risks / Scope

3.1 Assumptions

The following are the assumptions associated to the Vermont Health Benefit Exchange solution:

- Federal Data Services Hub will be implemented and provide the necessary data for verifying eligibility by aggregating data from different federal systems.
- Carriers will use the service interface or a managed file transfer interface for plan rate feeds, enrollments, and exchange of financial information.
- Scalable infrastructure for VT HBE will be provided and maintained by the CGI Cloud services from the Phoenix Data Center (Primary site) and Philadelphia Data Center (Secondary Warm site).
- The necessary data will be provided and no data conversion will be required.
- No legacy system integration is required for compares or conversions, or has been deemed out of scope for this project.
- The OneGate product provides the COTS functionality to meet all federally mandated requirements in a timely fashion to be incorporated and validated the Testing and SOV Acceptance Teams.
- The VT HBE Environment will leverage both Virtual and Physical Hardware environments.
- The following Oracle Products will be established and implemented in the VT HBE enterprise framework:
 - ▶ Oracle Policy Automation
 - ▶ Oracle Identity Manager
 - ▶ Oracle Access Manager
 - ▶ Oracle Virtual Directory
 - ▶ Oracle Internet Directory
 - ▶ Oracle Policy Modeler
 - ▶ Oracle SOA Suite (for example, Enterprise Service Bus, BAM, Orchestrations, etc.)
- The VT HBE will leverage several Siebel modules including but not limited to the following:
 - ▶ Siebel Public Sector CRM Base Option

- ▶ Siebel Health Insurance Base Option
- ▶ Siebel CRM Base
- ▶ Siebel Tools
- ▶ Siebel CRM Web Channel for Customers - up to 15 Objects
- ▶ Siebel Individual Coverage
- ▶ Siebel Group Policies
- Financial processing will be provided by Benaissance that is self-contained within their separate operational environment.

3.2 Constraints

The following are the constraints associated to the VT HBE solution:

- The VT HBE solution has been sized to service Vermont's current population as a basis, and expected growth has been included with ongoing increases in client load. The performance of the database should stay consistent as the data population grows, with proper monitoring and actions that support database best practices.
 - ▶ Specifically, for the initial release it is anticipated that the total potential number of population that may utilize the HBE solution is 65,000 and that the system has been designed to support 400 concurrent users.
- It is expected that the VT HBE environments comply with Federal and Vermont State requirements.
- The VT HBE solution environment configuration should be one supported by the OneGate COTS provider.
- The VT HBE integration approach must work for all carriers involved in the SOV project.

3.3 Risks

The following are the risks associated to the VT HBE solution:

- Federal Data Services Hub implementation is not complete and/or the Federal Hub may have significant operational outage conditions and could negatively impact the VT HBE design, and operational services.
 - ▶ Mitigation: This risk will be monitored closely by the project team and changes to the Federal Hub design or implementation delays will be communicated to the VT HBE stakeholders so appropriate project adjustments can be implemented for successful completion of the VT HBE solution.
 - ▶ Mitigation: The VT HBE solution will be operationally configured in a decoupled approach to enable the necessary system functions to operate on an "alternative mode of operation" in the event that the Federal Hub is not operational at any time. The VT HBE solution will operationally test to determine the status of the Federal Hub throughout the VT HBE operational state. Once a negative operational state is identified, the solution will automatically switch to the alternative mode of operation.
- High-level VT HBE requirements defined may not identify specific functionality required, which could impact the overall scope of the project, which may be uncovered during detailed design and implementation phase of the project.
 - ▶ Mitigation: This risk will be monitored closely and if new requirements are identified during detailed design the project change control process will be followed.
- There are several functional and integration components being developed in parallel that increases risk when they are all brought together.

- ▶ Mitigation: This risk will be monitored closely to help ensure timely completion project dependencies and communication of any implementation delays across component tracks. In addition, the detail testing plan will include scenarios to validate required functional and integration components.
- The introduction of SOA technologies such as ESB, BAM, BRE, Web Services and the general shift towards a real-time, service-based integration between systems could increase the integration risk because it is a departure from the older file-based transfer processes.
 - ▶ Mitigation: This risk will be monitored on an ongoing basis and more detailed risks will be raised and mitigated should the introduction of these technologies cause issues within the VT HBE environment.
- CMS continued changing of requirements and/or specific technical components within the Federal Hub, which may have an impact on the overall scope.
 - ▶ Mitigation: This risk will be monitored closely, and if new requirements are identified during detailed design the project change control process will be followed.
- The VT HBE will be implementing the Exeter OneGate solution, which at the time of writing this document, is new and not currently in production.
 - ▶ Mitigation: The OneGate solution is built upon known fully operational Oracle technologies (Siebel, SOA, and Policy Server) and the open source tool Liferay Portal, and the OneGate specific components only “extend” these well-established tools. Additional testing is planned, including the testing to demonstrate the upgrade of the technical components.
- The introduction of SOA technologies such as ESB, BAM, BRE, Web Services and the general shift toward a real-time, service-based integration between systems could increase the integration risk because it is a departure from the older file-based transfer processes.
 - ▶ Mitigation: This risk will be monitored on an ongoing basis and more detailed risks will be raised and mitigated should the introduction of these technologies cause issues within the VT HBE environment.

3.4 Scope

The following are the Out of Scope items for the initial release of the VT HBE solution:

- The VT HBE solution does not include the Configuration Tool or ongoing SOA processes and procedures that should be implemented to support ongoing SOA operations.
- The VT HBE initial release does not include functionality beyond Federal and State of Vermont requirements unless otherwise accepted through the project change control process.
 - ▶ One specific point of clarification is the Integrated Eligibility requirements, functions, and integration needs that will be addressed within a separate project scope.

4 System Design

4.1 System Design: Functional Layers

The following Vermont Health Benefit Exchange (HBE) diagram breaks down the solution into functional layers providing a high-level overview of the system users, channels, and features.

Functional layer description:

- **People** – The types of system users accessing the VT HBE.
- **Access** – The channels in which system users gain access to the VT HBE.
- **Security** – The solution will provide user and system security that meets all Federal and State requirements.
- **Workflow** – The high-level workflows will be initiated by users while interacting with the VT HBE and each workflow will be made up of several functional components to successfully complete tasks. The solution will leverage system functions across workflows to provide a consistent user experience and minimize implementation cost.
- **Functions** – The system functionality of the Vermont Health Benefit Exchange solution Data. The system includes multiple secure databases for executing transactions on the VT HBE and providing an enterprise foundation for the SOV to leverage and build upon for future applications.

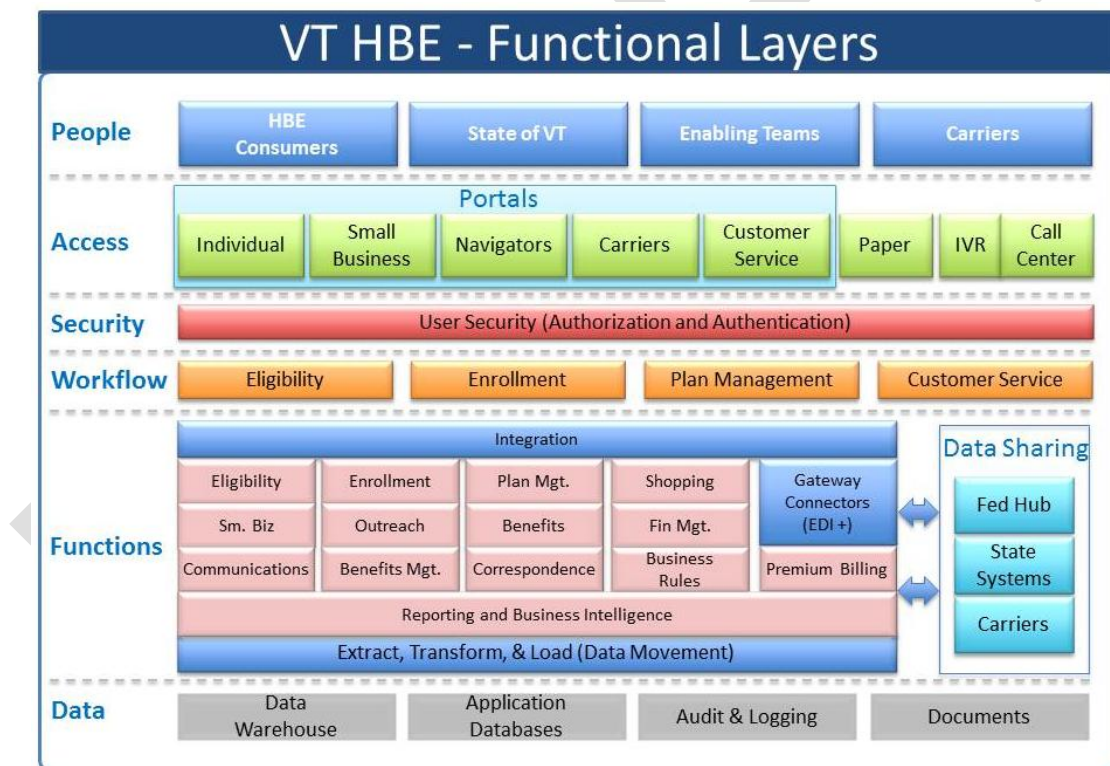


Exhibit 3: Vermont Health Benefit Exchange (HBE) Functional Layers

The VT HBE solution will be hosted in a Government Services Administration (GSA) Cloud environment that complies with FedRAMP for operations, security, and storage of data. Primary operations will be located within the CGI Phoenix Data Center (PDC) and have secondary “warm site” for failover in the CGI Philadelphia Data Center. The solution will be hosted on a three-tiered physical architecture with isolating firewall and load balancers for security and performance. The software solution will be implemented in four-tier logical architecture layers including Presentation layer, Application Layer, Middleware Layer, and database layer.

The Presentation Layer (Web), Application Layer, and Middleware Layer will use virtual environments built upon VMware ESXi hosts. Using virtual machines provides cost-effective utilization of hardware resources by allowing effective balancing of available resources to actual requirements. These virtual servers will be configured to provide a higher-level availability and as localized hardware failure conditions occur fail-over guest machines can be quickly brought online when needed or as load increases during critical operational (for example, open enrollment) time periods.

The Database layer is Oracle-based. The solution will use physical servers for each to provide the highest level of performance and reliability possible.

These components together will help achieve the mission of the State of Vermont to provide all Vermonters with the knowledge and tools needed to easily compare and choose a quality, affordable, and comprehensive health plan, and are explained in part in the next section.

4.1.1 Functional Layer Components

The following table described the components of the Functional Layer.

Exhibit 4: Functional Layer Components

Layer	Component	Functional Description
1	People / Stakeholders	Each Stakeholder group has a set of functions that are accessible to that group. Certain groups may have additional access depending on their role. For example, VT HBE staff and other stakeholders will have different rights depending on their assigned role, caseworker, supervisor, program manager, etc. The roles and access will be managed through Oracle Identity Management and Oracle Access Management.
2	Access / Channels	Channels provide multiple input/output display format types including Web client (http/https), secure email, faxed document, scanned document, fax, paper, and chat. Display format is applied outside the business process services, as a “view” of the content rendered. Separating business services for the content presentation provides reusability of both resource types.
3	Access / Portals	Portals support multiple user communities through a highly configurable portal framework. The OneGate / Liferay public facing portal adheres to the UX2014 usability standards.
4	Integration / Enterprise Service Bus (ESB)	CGI’s business process orchestration is defined in the Integration / Orchestration layer. Components follow the CMS blueprint for functional decomposition (e.g., Enrollment Management, Plan Management, and Financial Management). Based on the Oracle SOA Suite 11g product, the VT HBE ESB will integrate with all other components within the architecture. The ESB provides the standard functionality for message translation, transformation, enrichment, and routing across our solution’s services. The ESB supports open standards and includes out-of-the-box support for approximately 25 different protocols allowing a broad range of federal and State systems to be integrated onto the framework.

Layer	Component	Functional Description
5	Workflow	<p>Some of the major workflow areas of the VT HBE solution are:</p> <ul style="list-style-type: none"> Eligibility <ul style="list-style-type: none"> Plan Management <ul style="list-style-type: none"> Case Management Small Business (SHOP) <p>Siebel CRM Public Sector's workflow capabilities enable automation of specific business policies and procedures such as Eligibility and Case Management. The use of workflow enables commitments to clients to be addressed and issues to be escalated to management automatically. With Workflow, overdue cases and unresolved issues can be automatically escalated so case managers are alerted to problems.</p> <p>In addition, OneGate has developed SOA composites utilizing Oracle SOA Suite 11g, providing out-of-the-box functionality for the Vermont Health Benefit Exchange. For example, customer actions like change of circumstance drive options for VT HBE selections and notifications and immediately alert caseworkers.</p>
6, 7, 8	Service Layers	<p>The Services Layers consist of a set of that provide core VT HBE functionality. The majority of these services are contained within the WebLogic application server.</p> <p>Application Services – This collection of services supplies the fundamental business capability, including plan management, financial management, benefit management, customer service, communication and oversight. These are exposed Web services that are orchestrated through the Oracle SOA Suite 11g. The Orchestration layer serves to translate communication differences between the application services as needed. Communication and orchestration is independent of the source and target application service modules. This complies with MITA solution, as defined by CMS.</p> <p>Technical Services – This group of helper services provides needed system utilities to the VT HBE solution application modules. The end user does not directly interact with this class of modules but does benefit from the resources they provide.</p> <p>Services included are:</p> <ul style="list-style-type: none"> Management of batch data updates or planned processes Centralized logging and system monitoring Caching of data and services to maximize performance Performance Monitoring Common Services <p>Business Rules – The VT HBE facilitates policy rules including MAGI, APTC and CSA (Cost Sharing Assistance) by leveraging the Oracle Policy Automation (OPA) tool.</p> <p>Notice Management – The Thunderhead NOW content management system will handle all forms of public document generation. Rated by Gartner Group as one of the leading solutions in its arena, this technology allows automated creation and assembly of high-volume communications delivered across multiple channels, including print, XML Messaging, Microsoft office documents (Word, Excel), PDF, E-mail, Web, or SMS & MMS for mobile devices.</p> <p>All document templates are XML defined, allowing dynamic change without reengineering.</p> <p>Integration Services – The Integration service components provide secure information exchange capabilities with sources such as the Federal Data Hub, Vermont State Systems, and the carriers. These gateways will support various types of protocols and standards and will support both asynchronous as well as synchronous messaging. Gateways also perform audit and logging.</p>

Layer	Component	Functional Description
10	Data Management	<p>The tools used to manage data are listed below:</p> <ul style="list-style-type: none"> ▪ The VT HBE relational database, running on Oracle 11g ▪ Document and image management through the Thunderhead NOW. ▪ A VT HBE Data Warehouse to enhance reporting capability ▪ Extract, transform, and load of incoming data sets using the Oracle tool ▪ Analytical reporting on program evaluation, business operations and transparency using OBIEE to support continuous improvement and transparency
11	Shared Services	<p>Shared services are centrally provided and can be leveraged across the enterprise. Identity Management system provides services related to identity proofing and user provisioning for the various stakeholder groups that use the VT HBE. Access Management also provides coarse-grained and granular Role-Based Access Control (RBAC) mechanisms for various features and information processed by the Exchange. The Vermont Health Benefit solution will leverage Oracle Access and Identity Manager.</p> <p>Oracle Enterprise Data Quality will be used to achieve the Address Standardization and validation (Oracle Enterprise Data Quality), Enterprise search (Oracle Enterprise Search) that provides the ability to search across systems, and CGI DMS system to process incoming and outgoing mails.</p>
12	Infrastructure	<p>Key infrastructure aspects of the Vermont Health Benefit Exchange solution architecture include:</p> <ul style="list-style-type: none"> ▪ Hosted on CGI Government Cloud ▪ Applications use a modern, N-tier Web architecture and are designed to handle user requests in an event-driven, real-time workflow ▪ Leverages cost-efficient server environments based on Red Hat Linux servers ▪ Servers are deployed with VMware virtual server technology, allowing multiple applications to co-exist efficiently on the same physical servers ▪ The VT HBE is designed for high availability. Hosted in a clustered, load balanced, fault tolerant infrastructure configuration. ▪ Our VM hosting solution allows CGI to provide the dedicated development environment within the requested 30 days of contract approval
13	Security, Privacy, and Compliance	<p>Security and Privacy are mandated for HIPAA, PII, and IRS. Standards help ensure interoperability today and in the future. The basis for sharing components will be adherence to standards. The following standards are part of the proposed Vermont Health Benefit Exchange:</p> <ul style="list-style-type: none"> ▪ MITA, HIPAA EDI / ANSI X.12, NIEM ▪ ADA Compliance / W3C Web Content Accessibility Guidelines (WCAG) ▪ Security Standards (PHI, PII, FTI, PCI, IRS 1075 etc.) ▪ JSR 94 to integrate the rules engine services with business services ▪ UDDI v3 ▪ BPEL 2.0 / BPMN 2.0 to standardize the business process notation for easy portability to other BPM tools if needed for other state's ▪ SOAP 1.1 and 1.2, REST HTTP ▪ XML, FTP / FTPS, TCP/IP, WS-Security 1.0 and 1.1 ▪ Secured Socket Layer (SSL) certificates

4.2 System Design: Logical Architecture

The following diagram identifies the solution components comprising the Vermont (VT) HBE System Design in four layers, including the Presentation Layer, Application Layer, Middleware Layer, and the Data Layer.

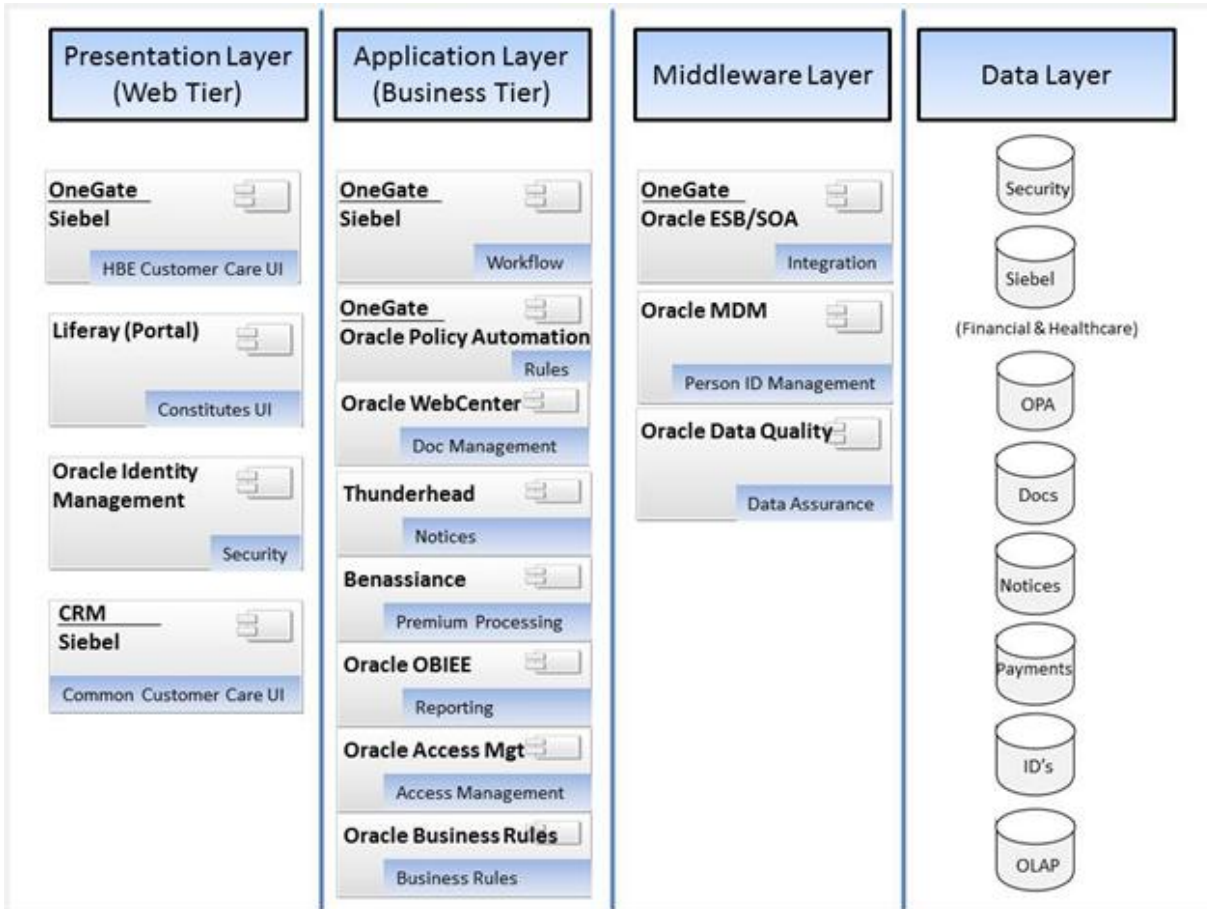


Exhibit 5: Functional Layer Components

4.2.1 Logical Architecture: Presentation Layer

The Presentation Layer or Web Tier provides the new portal capabilities for the SOV to expand end user self-service capabilities. The SOV users will be able to complete the following Self-Service activities through the VT HBE portal:

1. Anonymous browsing of generalized content and obtain high-level cost estimate
2. Create an on-line account
3. Apply for private Insurance
4. Apply for Medicaid Insurance
5. Obtain feedback on application and eligibility status
6. Shop and compare plans
7. View existing plans
8. Pay Premium, one time, and recurring Monthly Payment options
9. View payment history
10. Contact customer service
11. Access reports and notifications

The current SOV systems have limited reporting capabilities. The addition of the VT HBE Portal will enable greater data capture on users for improved analytics and reporting. The Portal also has a robust set of Notification and Reporting capabilities including, but not limited to, Monthly invoicing, Financial notifications, Plan notifications, Benefits confirmation, Plan updates, and AHS communications.

4.2.2 Logical Architecture: Application and Middleware Layers

The Application and Middleware Layers will leverage technology solutions that provide SOA and specifically Enterprise Services Bus capabilities to access the data that will drive the enabling Portal capabilities highlighted above. This follows the direction provided by the Centers for Medicare and Medicaid Services (CMS) that clearly encourages state Medicaid departments to invest in technology solutions that enable streamlined business processes, provide higher degrees of automation, and focus on following industry standards in how systems communicate. Batch interfaces, in which information is sent on a predefined schedule, have given way to “services” that are used to transfer important information to other systems in real-time, as events occur. Instead of holding a group of activities until the end of the day and sending a file of updates to a related system, services allow each activity to be communicated in near real-time to the other system, creating a more synchronized set of systems and reducing lag. This is referred to as an “Event Based Architecture” which is the fundamental approach that will be applied throughout this design and solution, unless specifically described otherwise.

Consistent use of services within an enterprise forms the basis of an event-based service-oriented architecture (SOA), in which systems utilize services to communicate with other systems on an as needed basis. Establishing an SOA in a complex environment, such as the VT HBE, requires an Enterprise Service Bus to manage the services.

The State of Vermont has selected the Oracle SOA Suite of tools as the Enterprise Service Bus (ESB) standard for the VT HBE. Establishing the ESB is only a small part of establishing the SOA that will provide the foundation for future enhancement to the VT HBE and other SOV applications. The most important component of the services architecture is identifying the processes that will participate, defining the services required, documenting the services using industry standard formats, implementing the services, and enabling services that provide the application integration and interoperability the SOV requires. The Services provided by the Application and Middleware Layer will allow the SOV to leverage these services and the ESB framework across the enterprise to reduce cost and implementation timelines.

The middle layers of the System Design also provide the functionality needed to manage both the Federal and State Business Rules in a fashion that is sustainable and scalable to meet the future needs of the SOV. One reason the Business Rules Engine functionality is critical to the operations of an HBE is the complexity of the rules and rule structure and their associated dependencies. The Affordability Care Act (ACA) changed the way Medicaid eligibility is determined, which impacts several key business areas:

- The logic that determines the Assistance Group (AG) has changed to create groupings of individuals based on a tax filing unit. This means that the group of individuals the system is going to evaluate is based on the primary individual and the individuals they expect to declare as dependents on their year's tax filing, rather than on the individuals living in the same household.
- Four new categories of Medicaid have been added (plus an additional category at states' option) and intended to consolidate the overall number of Medicaid categories over a one year timeframe.
- Also, to conform to the "Seven Conditions and Standards" (see "*Definitions*" section) of the Enhanced Funding Requirements, the new eligibility rules for the new Medicaid categories, the determination of the new AGs, and eligibility for the new insurance premium and cost sharing subsidies are brought into a technology neutral standard, outside of the transactional system.

The VT HBE will leverage an SOA-based product that includes a business rules engine. After evaluating the Commercial-off-the-Shelf (COTS) rules engines in the marketplace, the Exeter OneGate solution was deemed the best fit to present the information and apply the rules using the Oracle Business Policy server. The new eligibility rules have been developed in the COTS rules engine, which produces rules in both human and machine-readable formats. From the VT HBE enterprise perspective, any system that needs to make an eligibility determination can call a standard eligibility service exposed by OneGate, which in turn calls the rules engine and returns a standard result.

Point of clarification, this initial VT HBE solution is limited in scope as to how much of the revised Medicaid rules are implemented. Vermont will be initiating a separate project to implement their "Integrated Eligibility" that will fully implement all of the applicable Medicaid rules and programs.

4.2.3 Logical Architecture: Data Layer

The Data Layer of the System Design will provide several secure databases designed to capture the required VT HBE data elements and its operations. The VT HBE will seamlessly integrate with a third-party vendor, Benaissance, that will execute the VT HBE's financial transactions. Throughout the execution of the HBE solution the system will establish unique identifiers for individuals, organizations, and other entities, these identifiers will be tracked and managed using the Oracle Master Data Management (MDM) solution which will provide a foundation to meet the Medicaid Information Technology Architecture (MITA) vision of developing seamless and integrated systems that effectively share Medicaid information. The initial scope of the MDM implementation will be highly constrained and limited to the management of the identifiers, due to the very aggressive delivery timeline.

5 Design Considerations

5.1 Design Goals and Guidelines

Systems developed or enhanced to support functions of the Vermont Health Benefit Exchange will adhere to the following architectural principles when possible:

- Employ Web Services Architecture/Service-Oriented Architecture methodologies for system design and development to help ensure standards-based interfaces to link partners and information at both federal and state levels.
- Employ common authoritative data sources and data exchange services, such as federal and state agencies or other commercial entities.

- Employ open architecture standards (non-proprietary) for ease of information exchanges.
- Use Service-Oriented Architecture (SOA) concepts for developing the architecture.
- Use NIEM, NIST, HL7 and other standards for information modeling and exchange wherever possible.
- Conform to HIPAA's rules and regulations and respect all best practices concerning PHI.
- Use standards-based business rules and a technology-neutral business rules repository.
- Enable the business rules to be accessible and adaptable by other states.
- Use a standard technology-neutral Business Rule Management System (BRMS) for managing the business rules.
- Build in Performance Measurement and Reporting to collect system performance measures on a regular basis to help ensure quality, integrity, accuracy, and usefulness of functionality and information.
- Provide reporting capabilities that will allow the State of Vermont to analyze key data points.
- Provide the capability to easily add measures to the collection process.
- Provide reporting of measures in both real-time and as reports (event and time-driven).
- Help ensure systems are highly available and respond in a timely manner to customer requests.
- Offer configurable system performance parameters, including:
 - ▶ Use of performance measurement to adjust system parameters (that is, priorities).
 - ▶ Redundant capabilities (for example, portal, phone lines, hardware).
 - ▶ Load balancing.

5.2 Architectural Strategies

1. System is based on Service Oriented Architecture (SOA) principles and should address reuse, granularity, modularity, and interoperability.
2. Leverage virtualization, cloud computing, and managed hosting.
3. The solution should maximize the use of open standards-based components within the solution.
4. Interfaces will be developed using best practice standards.
5. The services are loosely coupled units of functionality. The functionality is agnostic of the business process and capable of being leveraged and reused by multiple processes.
6. Follow Federal and Industry standards for accessibility, messaging, and security.
7. Isolate business rules from programming logic. The categories of the rules identified are:
 - ▶ Eligibility rules for different programs (Medicaid, CHIP, MAGI etc.)
 - ▶ Plan premium calculation rules
 - ▶ Small Business specific employer/employee verifications rules
 - ▶ Financial rules, determine contribution amount, process Advance Payment Tax Credit (APTC) data received from IRS etc.
8. Will support the capacity to exchange data electronically so that multiple programs can be managed through a single application.
9. Design standardized interfaces to support consistent, efficient, and transparent exchange of data elements between federal programs and states.
10. Employ a modular, flexible approach to systems development, including open interfaces, and isolated components that can be more easily upgraded, maintained and shared over time.

11. Design will be flexible to provide real-time feedback on eligibility, plan options, and cost.
12. Focus on the consumer to simplify and reduce the time necessary for an individual to enroll in a health plan.
13. Enable reuse of the proposed Health Exchange functional solution, integration, and technical components where possible.
14. Enable a secure delivery platform to build trust between the various organizational entities.
15. Simplify ongoing operational support needs.

5.3 Architectural Drivers

The architecture is driven by business and technological objectives:

- General Business Drivers
 - ▶ Access and share business information faster and more effectively
 - ▶ Information is accessible as needed for each business function
 - ▶ Ability to act on changing business and legislative environment
 - ▶ Accommodate business growth and expansion
 - ▶ Accommodate existing information technology assets
 - ▶ Expose business services to interested parties
- General Technology Drivers
 - ▶ Provide a reliable, scalable, and stable solution
 - ▶ Simplify on-going maintenance and support functions
 - ▶ Simplify integration with other / existing system during the initial release and future releases
 - ▶ Implement reusable technologies in support of current solution needs and potential future enterprise initiatives
 - ▶ Leverage new network computing architectures, particularly those based on web services standards
 - ▶ Use COTS package applications where applicable
 - ▶ Displace obsolete and outdated technologies

5.4 Architectural Goals

The following are the primary goals for the software architecture:

- **Quality:** Support implementation of the business processes and services correctly and consistently
- **Intuitive:** Enable designs and APIs that are consistent, coherent, and clear
- **Ease of maintenance:** Enable easy implementation of future enhancements and changes
- **Security and Confidentiality:** Align with all applicable security policies at the Department and State levels including Personally Identifiable Information (PII) related confidentiality requirements
- **Reliability:** Reduce application downtime, application outages, and errors that directly affect users
- **Modularity:** Support de-coupling of components through implementation of function-based units accessible through defined application program interfaces
- **Extensibility:** Support future expansion by using configurable and encapsulated components that can be replaced with little impact
- **Reusability:** Support component and service-based reuse for future projects
- **Flexibility:** Support flexible and distributed deployment flexibility

The following table lists the main architectural goal characteristics and their descriptions:

Exhibit 6: Main Architectural Goal Characteristics

Acronym	Definition
Availability	Characteristic of a system providing for maximization of the time the system is available to its users.
Extensibility	Characteristic of a system supporting reduction of effort while introducing significant modifications to the system.
Interoperability	Characteristic of a system allowing for interaction with external systems irrespective of their technological platform of implementation.
Maintainability	Characteristic of a system reducing the effort needed to maintain the system in the typical usage patterns and expected life cycle.
Manageability	Characteristic of a system supporting monitoring, system configuration, and remote detection of performance-related events and failures.
Performance	Characteristic of a system allowing for production of intended results under specified load and within specified response times.
Portability	Characteristic of a system supporting migration from one underlying technology platform to another with a minimum of required changes to the system itself.
Reliability	Characteristic of a system determining its functioning with acceptable and prescribed levels of failure.
Reusability	Characteristic of a system supporting use of specific artifacts in systems or applications other than the system of origin.
Scalability	Characteristic of a system allowing for increasing the load on the system (in terms of for example, concurrent users, programs) without affecting the basic elements of the system.
Securability	Characteristic of a system providing for authentication of users and authorization of users in accessing specific resources of the system.
Serviceability	Characteristic of a system supporting repairs and updates with a minimal impact on system availability.
Usability	Characteristic of a system describing how easy it is for users to perform functions supported by the system.

5.5 Development Methods and Contingencies

The following section describes the development methods and contingencies.

5.5.1 Introduction

There is a critical need for a common development framework that can be used by IT practitioners to address the creation and management of systems in a consistent and effective manner. The SOV has requested, based on CMS requirements, the VT HBE project leverage the use of a Waterfall methodology to manage the overall development lifecycle. The VT HBE project may overlap certain waterfall activities or execute multiple development streams to help ensure the highest quality delivery by the federally mandated implementation date. The following restrictions may apply:

- The Requirements must be approved prior to the beginning of construction (Prototyping is allowed for the clarification of the requirements and design and the prototypes may be evolved into components of the product)
- The design and construction must be complete prior to the beginning of formal testing
- Formal testing must be complete prior to production implementation

This Waterfall approach allows for certain aspects of the development lifecycle to be initiated concurrently and allows for some rapid development of specific solution components. This approach is limited only by physical reality of software development (for example, it is not possible to install software that has not yet been constructed), the availability of team members to perform the tasks, and the restrictions mentioned above. Some benefits of this approach are:

- The client business environment is changing rapidly and some requirements are not fully known in a timely fashion and this approach allows time for requirements to be finalized before a change is required.
- The user interface needs experimentation. To optimize the effectiveness of the user interface, a new type of application may need to experiment with several approaches to optimize the effectiveness of the user interface.

In order to enable a true loose coupling among the solution components supported by a Service Oriented Architecture (SOA), we need application and integration frameworks. Another key element of the development framework is the use of a Model Driven Architecture that allows the generation of development artifacts from UML models. The benefits of SOA are:

- The generation of software artifacts inherently compliant with the architecture and system design.
- Increases developer productivity and consistency, maintainability, and quality of software artifacts.
- Supports traceability of generated software artifacts to models and supports impact analysis to determine effects of changes to system models.
- Supports true abstraction of the architecture from the underlying implementation thereby enabling changes and/or upgrades to the implementation in the future without losing knowledge built into the model.
- Decouple:
 - ▶ Consumers from Providers
 - ▶ Interfaces from implementations
 - ▶ Business rules from application logic
- Provide system “discoverability” through metadata
- Define and utilize canonical message and data structures
- Practice component-based development
- Use those components to build services through orchestration
- Provide SOA transparency through BAM

These benefits align closely with the SOV vision for the VT HBE solution to provide an enterprise foundation for future applications to build off of in the future. For example, some of the SOV goals for the VT HBE solution are:

- The Implementation of a best of breed market solution that can be expanded to support enterprise needs that are loosely coupled.
- Integration-based solution that enables data access between technical components and external functions driven by a Services Oriented Architecture (SOA) approach and tools.
- Enable a highly reliable solution that provides confidence in the operations teams and the citizens of Vermont.
- Provide a secure solution that ensures access, operations, and delivery of data supports a complex combination of compliance needs HIPAA, FTI, PCI, and NIST that are necessary for a state government solution to operate a healthcare solution.
- Drive leverage and reuse. Enable the ability to share appropriate business functions, materials, and components within the VT HBE solution and to other additional solutions/enterprise.

- Operational independence. Ensure that each of the operational components can operate separate from the other components within the VT HBE solution to simplify the support and maintenance functions.

Contingencies are broken into two fundamental sections; development contingency and operational contingency.

5.5.2 Development Contingency

The VT HBE solution is based fundamentally on the well-known tool set from Oracle applications and architecture with a set of add-on extensions from a company (Exeter), the company that developed OneGate.

The initial development contingency has already been enacted, as a preventative measure, in the form of professional consulting services from Oracle and Exeter. In addition, the development team is engaged with other VT HBE state-based solutions that are using similar tools to further reduce the number of unknowns. The project plan and team have brought the testing team on board early in the development process to help ensure that all test conditions are identified and appropriate desired business and technical test results are achieved. The testing team will be engaged with the development team throughout the development activities. The State of Vermont Department of Information and Innovation (DII) have provided significant staffing, that is above and beyond the core development staffing, to support the discovery and definition of detailed technical aspects that would negatively impact the delivery schedule. To further reduce the development issues a series of delivery releases is planned; A) stand up initial baseline technology, B) perform initial prototyping on functionality, C) verify integration between components are operational, D) execute an extensive set of testing.

5.5.3 Operational Contingency

The overall design of the VT HBE solution is based on the approach that the solution can operate within and take advantage of a High Availability infrastructure that will support and resolve the majority of local (within primary site) operational failures with minimal impact on the end user. If a significant issue arises that would require the initiation of the secondary “warm site” in Philadelphia, the secondary site will be configured as a “mirror” to the primary site with access to the common information and recent processed information, up to 30 minutes. This warm site will be configured to be operational within a four (4) hour time period. In the unique scenario that both Primary and Secondary sites are not available for operations, the Disaster Recovery plan will describe how operational teams will respond.

5.6 State of Vermont SOA Principles Summary

Principles form the core values of architectural decision making for an organization. The SOV SOA principles are derived from The Open Group Architecture Framework (TOGAF) principle catalog as well as the Oracle Enterprise Architecture Framework (OEAF).

Principles are general rules and guidelines, intended to be enduring and seldom amended that inform and support the way in which an organization sets about fulfilling its mission.

In their turn, principles may be just one element in a structured set of ideas that collectively define and guide the organization, from values through to actions and results.

It may be that the Architecture Principles are documented using a wiki or as an intranet rather than a text-based document. A more effective solution would be to use a licensed TOGAF tool that captures this output.

Each of the SOV principles include a Principle Name, Statement, and Rationale that provides guidance concerning how the principle should be applied.

Exhibit 7: SOA Principles Acronyms

Acronym	Definition
ACA	Affordability Care Act
BRE	Business Rules Engine
CI	Configuration Item
CM	Configuration Management
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial Off the Shelf Software

Exhibit 8: Descriptive Names of the SOA Principle

Name	SOA Principle
Statement	The Statement should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organization to the next. It is vital that the principles statement be unambiguous.
Rationale	The Rationale should highlight the business benefits of adhering to the principle, using business terminology. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. Describe situations where one principle would be given precedence or carry more weight than another for making a decision.

The following core SOA Principles will be applied for the VT HBE project to refer to as a guide during the design review, development, and implementation of the overall solution.

Exhibit 9: Core SOA Principles

Name	Statement	Rationale
Service re-use	Existing services should always be considered first when creating new SOA solutions.	Re-use before buy before build to decrease cost and complexity.
Standard Service Contract	Services share standardized contracts. Services within the same inventory are in compliance with the same contract standards.	<p>To enable services with the meaningful level of the natural interoperability within the boundary of service inventory which reduces the need for data transformation.</p> <p>To allow the purpose and capabilities of services to be more easily and intuitively understood.</p>

Name	Statement	Rationale
Service Loose Coupling	Services are loosely coupled. Service contracts impose low consumer coupling requirements and are themselves decoupled from their surrounding environment.	Re-use before buy before build to decrease cost and complexity.
Service Abstraction	Service contracts should only contain essential information and information about service is limited to what is published in service contracts.	To enable services with the meaningful level of the natural interoperability within the boundary of service inventory which reduces the need for data transformation. To allow the purpose and capabilities of services to be more easily and intuitively understood.
Service Autonomy	Services exercise a high level of control over their underlying runtime.	This promotes an environment in which services and their consumers can be adaptively evolved over time with minimal impact on each other.
Service Discoverability	Services are supplemented with communicative meta-data by which they can be effectively discovered and interpreted.	To keep the quantity and details of contract content concise and balanced and prevent unnecessary access to additional service details.
Service Description	Descriptions shall be adequate to support consumer decision to use the service.	To increase the service runtime reliability, performance, and predictability. To increase the amount of control service has over its runtime environment.
Service Harvesting	Solutions should be reviewed for harvesting re-usable services.	Services should be positioned as highly discoverable resources within the enterprise.
Service monitoring	Service contracts adherence should be monitored. Metrics should be gathered and available.	Help ensure consumers have adequate information to decide whether the service is appropriate for their objectives. This may include: Service Meta-data - Policy - Contracts - Funding model (current and projected) Helps support consumers re-using existing services
Service policy enforcement	Service design and run-time policies should be enforced.	Existing solutions are the best source for re-usable services with the least development and maintenance costs. New solutions should consider harvesting services during initial development and on an ongoing basis.
Service security	Services contracts and descriptions should be reviewed for conformance to organization security requirements with identified security best practices and support of objectives.	To help ensure correct service delivery. To detect service contract violations. To feed service and SOA solution governance. To support consumers choosing a service with appropriate metrics.
Comply with EA	The SOA services and solutions should comply with the enterprise architecture (if one exists).	To ensure high-quality services. To help ensure conditions are met that have been expressed to achieve stated goals.

Name	Statement	Rationale
SOA governance must promote the alignment of business and IT	The SOA governance program should support the business and IT drivers. Business and IT stakeholders must participate in governing and enforcing the organization's SOA program.	To help ensure correct security levels and risk levels.
Conform to organization's governance	SOA governance activities shall conform to Business, IT, & EA governance principles and standards.	To help ensure that the SOA solution and service fulfills the long-term goals of the organization.
SOA Reference Architecture is required	An SOA Reference Architecture provides a set of architectural patterns, standards, and best practices for use in developing SOA solutions.	SOA is intended to drive flexibility and agility for the business and IT. Failing to govern to foster that alignment will reduce the benefits of service-oriented approach.
Provider & consumer contracts	Contracts should exist between service providers and consumers. Contracts may be dictated by one Party.	The organization governance procedures are part of the strategy of the organization and should be a part of SOA governance as well.
Service metadata	To enable decisions and descriptions relating to services and their contracts to be stored in a well-known location, including relationships among services and their associated artifacts.	Use of the approved architectural artifacts, from the SOA RA, will reduce project risk and lower costs, by reducing the number and complexity of design activities in the project
Identified governance stakeholders	Stakeholders shall be identified and accept responsibility for the governance process(es).	To help ensure the correct delivery of service.
Tailor SOA governance processes	SOA governance processes should be tailored based on objectives, project scope, and risk.	Understanding of the purpose of the service. Business continuity impact analysis. Root cause analysis.
Automate SOA governance processes	It should be possible to automate the SOA governance processes.	To help ensure proper execution of governance. To communicate SOA governance value. To communicate appropriate SOA governance processes and procedures.

5.7 Development Tools

The following section provides a description of the tools used to enable the VT HBE implementation throughout the Software Development Lifecycle (SDLC). The following section outlines the description of how each of the products will be integrated and leveraged to establish end-to-end configuration control. The selected development tools for the implementation of the VT HBE integration and configuration are listed below.

Exhibit 10: Development Tools

#	Tool	Description
1	ALMComplete	This application lifecycle management tool furthers the collaborative process helping teams communicate more effectively. It combines the capabilities of two integrated modules, QAComplete and DevComplete, plus support ticket management and contact management capabilities. Document sharing, team calendars, interactive dashboards, burn-down charts, knowledge bases and threaded discussions.

#	Tool	Description
2	QTP	HP QuickTest Professional software provides functional and regression test automation for software applications and environments. Part of the HP Quality Center tool suite, HP QuickTest Professional can be used for enterprise quality assurance.
3	LoadRunner	HP LoadRunner is the industry standard for application performance testing. The load testing tool helps you prevent issues by detecting bottlenecks and to obtain an accurate picture of end-to-end system performance before going live.
4	Web Inspect	HP WebInspect is an automated and configurable web-application security-testing tool that mimics real-world hacking techniques and attacks, enabling you to thoroughly analyze your complex web applications and services for security vulnerabilities.
5	Ensemble	Internal (CGI) document repository (Issue, Change, Risk, Collaboration, Doc Repository).
6	Toad	Toad provides a simple, consistent way to build, manage, and maintain databases.
7	jProfiler	JProfiler's intuitive UI helps you resolve performance bottlenecks, pin down memory leaks and understand threading issues.
8	CA Erwin	CA Erwin Data Modeler is an industry-leading data modeling solution that provides a simple, visual interface to manage your complex data environment.
9	Justinmind Prototyper	With Prototyper, you can draw highly interactive wireframes in minutes using its extensive gallery of components and interactions.
10	XML Spy	XML Editing Tool
11	Liferay	Liferay Portal, the market's leading independent portal product.
12	JAWS	JAWS is used for ADA Compliance verification and Usability Testing.
13	Thunderhead NOW	Simple Correspondence.
14	soapUI Pro	Web services test tool; supports automation of web services inspection, invocation, simulation, mockup, functional, load, and compliance tests.
15	Java PDF417, QR Code Generator	This tool set provides functionality to generate barcode images in 1D and 2D barcodes.
16	Splunk	Splunk is a fully featured, powerful platform for collecting, searching, monitoring and analyzing machine data.
17	AccVerify	AccVerify software is provided by HiSoftware as a content-aware compliance solutions for the Web that detect private or confidential data and report on violations to help ensure compliance with regulatory and other internal policies. This tool will be used to execute the 508 Compliance Check.
18	ATSM	Test Automation and Regression, Case Loading and Support.
19	Data Masker	Test and Development Data creation and manipulation.
20	CGI SWAT	Development tool for Agile development and sprint management.
21	Checkstyle	Development tool for Coding Standards (JAVA).
22	Cobertura	Development tool for Code Coverage (Java).
23	CSSAnalyzer	Development tool for Usability Testing Tools.
24	Eclipse	Development tool for coding (Java IDE).

#	Tool	Description
25	FindBugs	Development tool for applying Coding Standards (JAVA).
26	Javadoc	Development tool for Documentation (Java).
27	JavaNCSS	Development tool for Code Metrics (Java).
28	Jenkins/Hudson	Development tool for Continuous Integration (Server).
29	Junit	JUnit is a simple, open source framework to write repeatable tests. JUnit executes regression tests as part of the release process which greatly helps continuous integration process.
30	Maven	Development tool to help perform code builds (Build Tool).
31	Quartz	Quartz is a full-featured, open source job scheduling service that can be integrated with, or used alongside virtually any Java application - from the smallest stand-alone application to the largest e-commerce system. Quartz can be used to create simple or complex schedules for executing tens, hundreds, or even tens-of-thousands of jobs; jobs whose tasks are defined as standard Java components that may execute virtually anything you may program them to do.
32	Selenium	Web application record/playback tool used for regression testing of the user interface.
33	SLF4J	The Simple Logging Facade for Java or (SLF4J) serves as a simple facade or abstraction for various logging frameworks
34	SONAR	Development Tool for Coding Standards (JAVA) (Code Quality Metrics).
35	Apache ANT	Apache ANT is open source java-based tool which allows automating build management activities. Maven may be leveraged as an alternative to ANT.
36	TortoiseSVN	TortoiseSVN is open-source revision control software for Windows. TortoiseSVN provides an easy user interface for accessing Subversion.
37	SpringSource	Alternative Java IDE. SpringSource is a popular application development framework for enterprise Java. Developers use Spring to create high performing, easily testable, reusable code without any lock-in.
38	Eclipse IDE	Oracle provides an Eclipse distribution package, Oracle Enterprise Pack for Eclipse (OEPE) that includes a variety of plug-ins that are useful and necessary to develop some of the Oracle Middleware components. The current version, suitable to development of the SOA 11.1.1.6 Suite, is OEPE 11.1.1.8.0, which is based on Eclipse 3.7.1 (Indigo). OEPE is essential for Oracle Service Bus (OSB) development and very useful for database, Web Tier, and WebLogic (WLST) development. Because OEPE is a contemporary version of Eclipse, it seems a good candidate for standardization as the primary Java-based stack development IDE. Additional plug-ins can be added to OEPE for extended development capability.
39	Oracle JDeveloper IDE	JDeveloper is a Java IDE, with basic capabilities similar to Eclipse. All developers who will be creating orchestrated services and business processes will use the JDeveloper IDE. Most other development will be done on Eclipse or other appropriate IDE.
40	Oracle BPM Composer	BPM Composer is a web-based development and documentation tool for Oracle BPM processes and rules. The current version of Composer is not a suitable replacement for the JDeveloper BPM Studio. If Composer is used into HBE, it will likely only be used as an interface to specific administrators or technical analysts, and only to make limited changes such as modifying a business rule.

#	Tool	Description
41	Oracle Data Modeler	Oracle Data Modeler (ODM) is a no-cost development tool used primarily for logical and physical database design. Some of the uses of ODM for HBE development are to design new and customized OLTP tables, reverse-engineer database schemas for inspection and documentation, create and publish models as documentation artifacts, create and manage database deployment scripts, etc.
42	Subversion	Subversion is used for management and control of software development assets. Subversion is an open source product. It provides sophisticated version control, parallel development, and the 47 capabilities needed to create, update, build, deliver, reuse, and maintain business-critical assets.

The following are the details and list of the current file types for each configuration category:

Exhibit 11: Controlled Software Category File Types

#	Controlled Software Category - Application	File Type
1.	Enterprise Java Beans (EJB)	.java
2.	EJB Deployment Descriptors	.xml
3.	Plain Old Java Objects (POJO)	.java
4.	JUnit Test Files	.java
5.	Java Servlets	.java
6.	Application Configuration Files	.xml
7.	Property files	.properties
8.	Java Server Pages (JSP)	.jsp
9.	HTML Files	.html
10.	Cascading Style Sheets (CSS)	.css
11.	JavaScript	.js
12.	Images	.gif, .jpeg
13.	Application Deployment Descriptors	.xml
14.	Third-Party JAR files	.jar
15.	Java Enterprise Archive	.ear
16.	Web Archive	.war
17.	XMS Schema Definition	.xsd
#	Controlled Software Category - Script	File Type
18.	Apache ANT Build Files	.xml
19.	Property Files	.properties
20.	Shell Scripts	.sh
21.	Third-party JAR Files	.jar

6 General Testing Approaches

6.1 Integrating and Testing with the Federal Hub

- Complexity in the implementation of our communication infrastructure requires:
 - Validate the handshaking ability between physical networks. Confirm, via the use of SoapUI, that the XSD's the Fed's provide us are viable and that security is in place and dependably functional
 - Confirm, via the use of SoapUI, that message content, utilizing CMS test data, provides expected results
- Once we achieve the previous levels of validation, we would continue to exercise the SoapUI utility to inform our ongoing development efforts of SOA composites, again following a gradual progression:
 - Achieve the same level of communication reliability that the SoapUI utility is providing
 - Implement Oracle SOA Suite Mediators to do the message validation and mapping

6.2 Integrating and Testing with Carriers

The preferred method of transmission is web services. Web services provide improved reliability, tracking, problem resolution, and monitoring. File transfers are slow, and their content not programmatically discernible. For example, errors have to be identified and responded to manually.

The internal processing for Carrier integration will be an event-driven model. Highlights of the model include:

- Internal provisioning of employer and employees through the VT HBE solution.
- As carrier specific transactions are identified (such as the creation of employers, adding employees), the internal processing will occur.
- Transactions (e.g. 834) will be created as if web services will be used for processing.
- If the Carrier Exchange Agreement identifies batch SFTP as the transport method, then we will queue the transactions, and pass these as files. For this business use case we will need to hold the employee transactions until the employer record creation has been verified.
- These two paths will provide an Enterprise solution that is both flexible and scalable.

7 System Architecture

The following diagram represents the high-level architecture of the VT HBE solution.

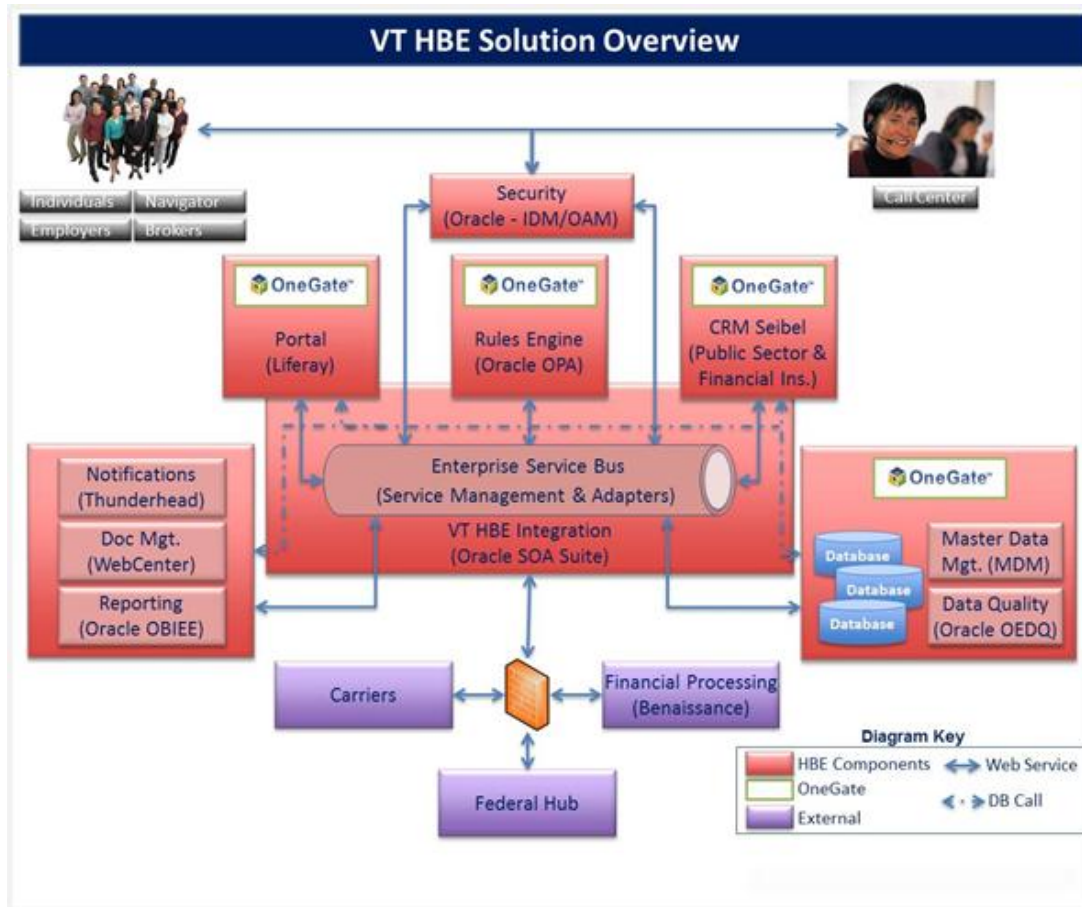


Exhibit 12: VT HBE Solution Overview

7.1 Design Patterns

Design patterns are commonly defined as time-tested solutions to recurring design problems. These patterns represent solutions to common problems in software development. Design patterns have two major benefits. First, they provide a way to solve issues related to software development using a proven solution. The solution facilitates the development of highly-cohesive modules with minimal coupling. They isolate the variability that may exist in the system requirements, making the overall system easier to understand and maintain. Second, design patterns make communication between designers more efficient. Software professionals can immediately picture the high-level design in their heads when they refer to the name of the pattern used to solve a particular issue when discussing system design. These patterns have been used successfully by developers in their respective fields, and therefore, the pros and cons of the pattern (as well as implementation issues) are known beforehand. All design patterns are reusable and can be adapted to particular contexts.

There are a number of design patterns which will be used in the design and development of the Vermont Health Benefit Exchange. The most significant design patterns are listed below:

7.2 SOA Architectural Patterns

The Canonical Schema Bus SOA architectural pattern is the basis of the system integration design. The Canonical Schema Bus pattern is a composite of several SOA design patterns, primarily:

Enterprise Service Bus (ESB) pattern

The ESB pattern is a composite pattern that provides an additional layer of connectivity and abstraction. ESB is characterized by the application of some essential patterns:

- Asynchronous Queuing
- Event-Driven Messaging
- Intermediate Routing
- Policy Centralization
- Reliable Messaging
- Rules Centralization
- Service Broker

Canonical Schema pattern

Services that use similar data use common schemas, thus reducing transformation requirements that increase development effort, design complexity, and runtime performance overhead.

Standardized Service Contract pattern

A fundamental tenant of SOA is to adopt a normalized approach to developing and publishing services. The Vermont Health Benefit Exchange web services conform to the Standardized Service Contract pattern by providing WSDL, XSD, and WS-Policy descriptions for every exposed service.

The Contract Centralization pattern states that services can only be accessed according to the service contract, thereby eliminating “back doors”. Contract Decoupling also applies, which means that the contract is not directly associated to the implementation, therefore the implementation of the service could be changed without affecting the contract itself or the consumers of the service.

7.3 Model – View – Controller Pattern

As with most web applications, the VT HBE is also built using the MVC design pattern. This pattern helps us in developing solutions that are loosely coupled and thus more flexible.

The VT HBE architecture will implement a Model-View-Controller (MVC) architecture pattern where presentation, business logic, and persistence are decoupled. An MVC separates design concerns (data persistence and behavior, presentation, and control), decreasing code duplication, centralizing control, and making the application highly maintainable and extensible. The user interface simplifies user “actionable events”, supports the majority of the modern browsers and complies with the overarching requirements of accessibility (Section 508), usability, and user support.

The Model-View-Controller (MVC) pattern is the suggested solution for web-based applications. MVC has been used very effectively in GUI-type applications. By applying the MVC design pattern to a J2EE application, you can separate the data access logic from the data presentation logic. You can also build a flexible and easily extensible controller that controls the whole flow of the application. The following figure depicts the MVC architecture.

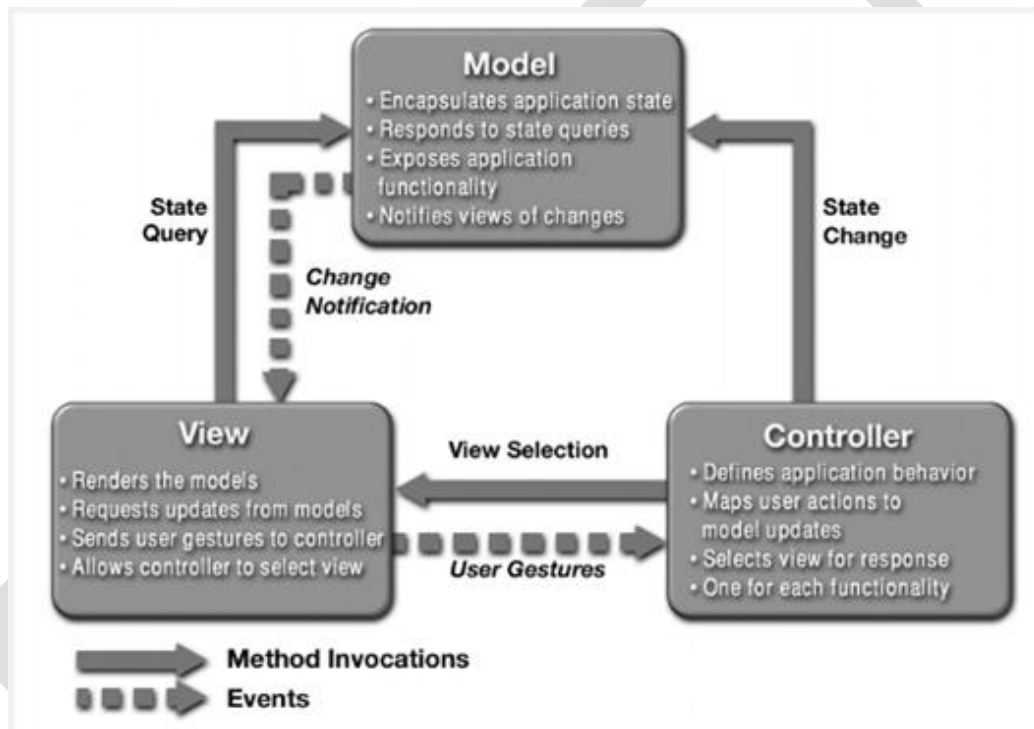


Exhibit 13: MVC Architecture

The MVC architecture can be mapped to a multi-tiered enterprise application as follows:

All enterprise data and the business logic to process the data can be represented in the MODEL.

The VIEW can access the data through the model and decide on how to present them to the client. The VIEW must ensure that the presentation changes as and when the MODEL changes.

The CONTROLLER can interact with the view and convert the client actions into actions that are understood and performed by the MODEL. The CONTROLLER also decides on the next view to be presented depending on the last client action and results of the corresponding MODEL action(s).

Some of the benefits of MVC architecture include:

- MVC architecture is suitable for a highly-interactive system that requires extensibility, maintainability, and multiple user views.
- MVC decouples presentation, user interaction, and system model.
- Presenting multiple views for multiple data sets is made easy because of the decoupling. This also makes it much easier to enable support for new types of clients (web, pda).
- Using this architecture minimizes code duplication.
- By separating the presentation from model and overall application flow, this architecture enables division of developer responsibilities, and thereby, produces faster development cycles.

7.4 Other Design Patterns

Exhibit 14: Other Design Patterns

Pattern	Description
Front Controller	Uses controller as the initial point of contact for handling a request. The controller manages the handling of the request, including invoking security services such as authentication and authorization, delegating business processing, managing the choice of an appropriate view, handling errors, and managing the selection of content creation strategies.
View Helper	A view contains formatting code, delegating its processing responsibilities to its helper classes, implemented as JavaBeans or custom tags. Helpers also store the view's intermediate data model and serve as business data adapters.
Session Façade	Uses session bean as a facade to encapsulate the complexity of interactions between the business objects participating in a workflow. The Session Facade manages the business objects, and provides a uniform coarse-grained service access layer to clients.
Web Service Broker	Use a Web Service Broker to expose and broker one or more services using XML and web protocols.
Transfer Object	Uses transfer Object to encapsulate the business data. A single method call is used to send and retrieve the Transfer Object. When the client requests the enterprise bean for the business data, the enterprise bean can construct the Transfer Object, populate it with its attribute values, and pass it by value to the client.
Data Access Object (DAO)	Uses Data Access Object (DAO) to abstract and encapsulate all access to the data source. The DAO manages the connection with the data source to obtain and store data.

7.5 Hardware Architecture

The Vermont Health Benefit Exchange IT infrastructure will leverage the CGI Government Cloud. Cloud sites are located in the Phoenix Data Center (PDC) and the Philadelphia Data Center (SDC). Vermont's setup is comprised of five separate operational specific environments. Note that this version of the SDD only covers the first two-boldded items:

- **PDC**
 - ▶ Development-Integration
 - ▶ System Integration Test (mirror of Production)
 - ▶ Staging (mirror of Production)
 - ▶ Production
- **SDC**
 - ▶ Disaster Recovery (limited mirror of Production)

The Hardware Architecture section of this document provides an overview of the VT HBE environments and network connections. There are a total of six VT HBE environments, of which three are considered Non-Production environments that consist of Development, Test, and Training. Each of the Non-Production environments will be fully functioning environments, but do not require any physical servers and the overall environment size is smaller than the Production Environments. The remaining three environments are considered Production equivalent environments that consist of Staging, Production, and Disaster Recovery. The Production environment configuration utilizes Physical servers to help ensure the best possible performance and the Staging environment will be mirror image of the Production environment.

Development Environment (Non Production Configuration)

The Development environment is used to develop and unit test the application for each of the technology areas. This development environment allows collaboration of development that actually takes place on developer workstations.

Test Environment (Non Production Configuration)

The Test environment is used to conduct functional and technical test for the components that have been constructed and unit tested in the development environment. This dedicated environment enables testers to confirm the application meets business functional requirements. Depending on the specific test activity taking place, this environment is set up for the test team to verify and validate the functionality of the application.

Training Environment (Non Production Configuration)

The training environment is a dedicated environment that allows users to perform hands-on exercises during training delivery.

Staging Environment (Production Configuration)

The Staging environment provides an area to the end users to validate the components and verify functional accuracy and completeness of the application. This environment supports not only the end-user functionality, but also the back-end functions such as batch processing, interfaces, and information delivery. This environment acts as a staging platform prior to promoting any changes to the production environment. The architecture of the pre-production environment mirrors the setup of the production environment with less capacity in regard to server count and storage capacity. As a best practice for CM only after a change has been verified in the pre-production environment is it migrated to the live production environment.

Production Environment (Production Configuration)

The production environment serves as the live environment of the application.

Disaster Recovery (Production Configuration)

The Disaster recovery environment serves as a warm failover environment for the Production environment. The architecture of the Disaster Recovery environment mirrors the setup of the production environment with less capacity in regard to server count and storage capacity.

7.6 Network Diagram

The following diagram provides an overview of the VT HBE Wide Area Network.

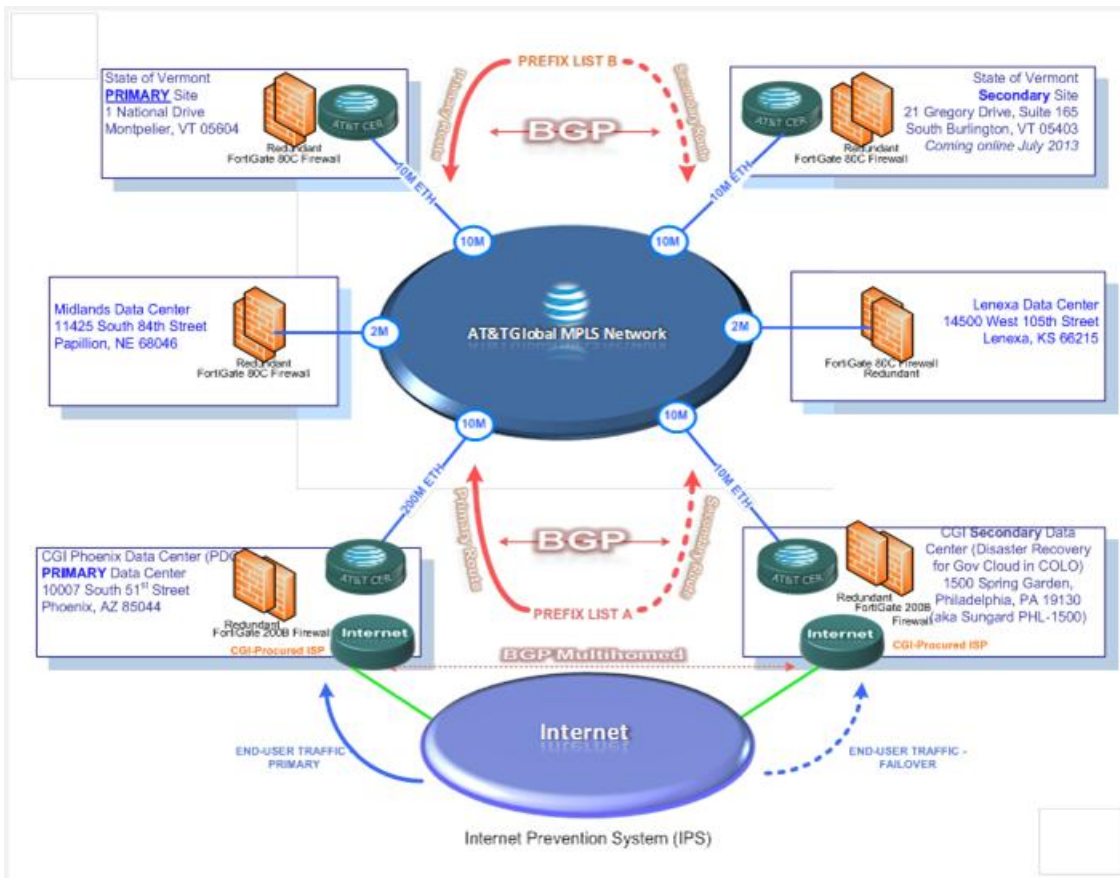


Exhibit 15: VT HBE Wide Area Network

Exhibit 16: Environment Definitions

Environment	Area	Activities	Comments
Development - Integration	Development	<ul style="list-style-type: none"> Unit Testing of modules Unit automation 	Purpose: Verify that each functional or technical component performs its actions as required. Each development stream will perform Individual coding efforts and unit testing in their own development environment and then integrate their code enhancements/changes into the Integration environment.
	Project Tools	Support project activities: <ul style="list-style-type: none"> Subversion Microsoft Visual Studio Grid Control 	Purpose: Supports project functions including software version control (Subversion), performance monitoring, etc.
	Test	<ul style="list-style-type: none"> Integration Testing of components from N Iteration White box Functional Testing Black and Gray box Regression Testing Batch Processing Performance Testing (unique virtual instance) Security Testing (unique virtual instance) 	Purpose: Verify that Individual components work together to perform business steps, processes or functions as required. Once development code changes have been unit tested and integrated with the main COTS Integration environment where integration and COTS functional testing will be performed by the development and testing staff, the CGI testing team will create and utilize stubbing techniques to mimic communication from other interfaces not developed. End-to-end testing, performance testing, security, and usability will take place in parallel during the final iterations of System Integration Test.
System Integration Test	System Test	<ul style="list-style-type: none"> Release Test Module connectivity test End-to-End Test Data Structure Validation Operational Readiness Deployment Procedure Testing 	Once the VT HBE has passed through the various test phases, the test environment is used to practice migration strategies and perform final testing activities against actual production data before General Availability to the public. The CGI project team members and VT HBE representation will review release changes, test results, risks, and production migration plans before each actual release to the Vermont public.
	Rules Configuration Test	Policy Change Testing	This environment may be set aside for the VT HBE team to perform rules configuration testing based on policy or other exchange changes.
	Emergency Fix Test	<ul style="list-style-type: none"> Critical defect testing Regression testing 	The Emergency Fix environment will mimic the production environment and be accessible by the CGI and State test team to help ensure urgent fixes are retested properly before promotion to production.
Staging	Staging	Production Staging	Release management
Production	Production	Live production (PHX)	Purpose: Provides operational capability.
Disaster Recovery	Disaster Recovery	Standby-Business Continuity (PHL)	Purpose: This is the failover “warm” continuity of operations site for live production environment.

- Web / Presentation
- Application / Middleware
- Database Service

7.7 Non-Production Environment Configuration

HEALTHCARE PLATFORM

Health Benefits Exchange View

Non-Production Environment(s) Dev, Test, Training, etc.

2/4	CGI VM 2VCPU w/4GB RAM
4/8	CGI VM 4VCPU w/8GB RAM
8/8	CGI VM 8VCPU w/16GB RAM
12/32	CGI VM 12VCPU w/32GB RAM
30N GB	CGI Storage in GB (DB & Apps) COTS

Web Server Zones

Application Server Zones

Database Server Zones

Exhibit 17: Non-Production Environment Configuration

7.8 Production Environment Configuration

The following diagram provides an overview of the Production environment configuration.

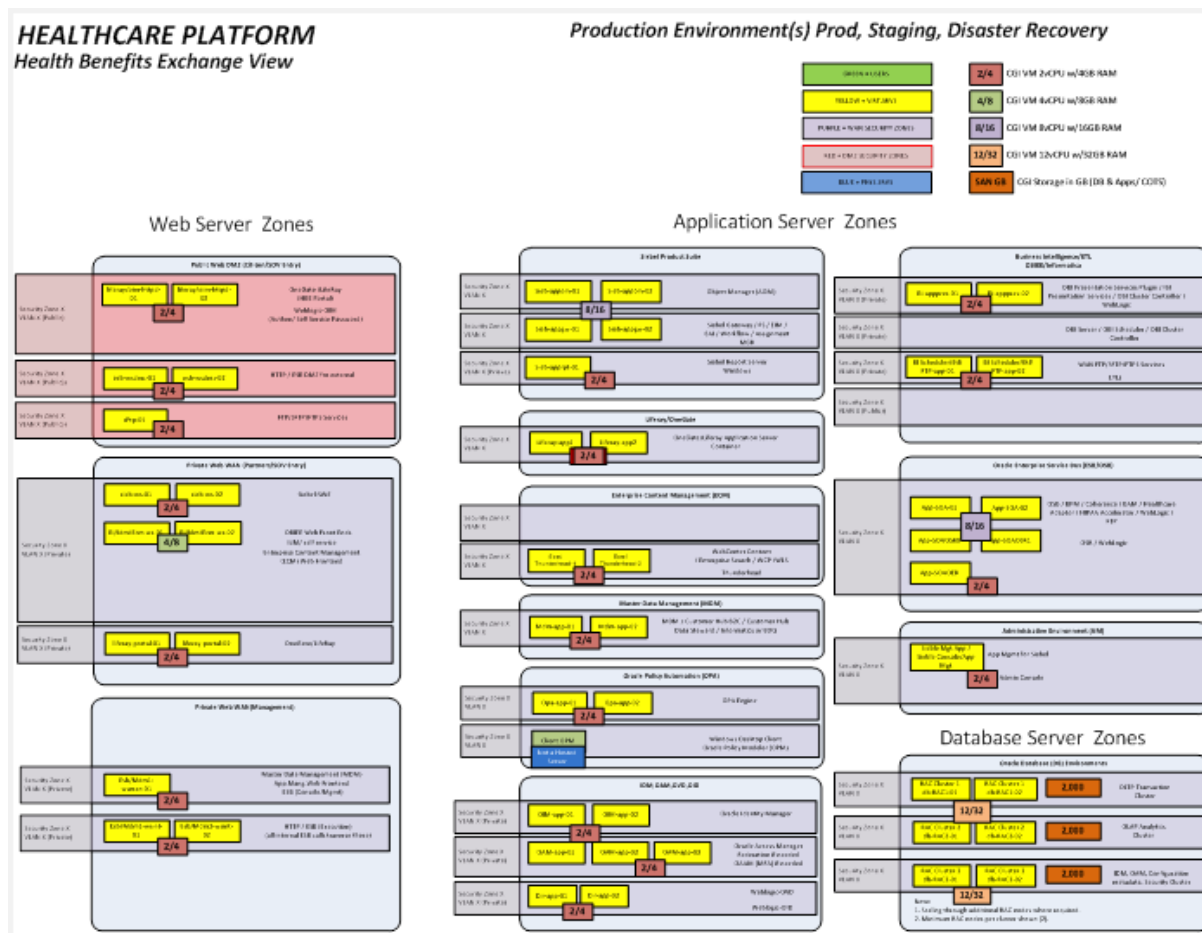


Exhibit 18: Production Environment Configuration

7.9 vCloud integration

The CGI Government Cloud will act as Infrastructure as a Service (IaaS) providing the VT HBE a single provider virtual datacenter (vDC) and an organizational virtual (operational) datacenter (vDC) for each of the environments.

7.10 Database Services and Storage

Each environment has a requirement for Oracle services. Due to high transaction volume, Oracle services will utilize RedHat Enterprise physical servers. Oracle encryption will be required on certain portions of the data stores to support Vermont and CMS security requirements.

Each function will utilize active/passive server pairs leveraging within the Phoenix Data Center (PDC) with comparable servers in the Philadelphia Data Center (SDC) Disaster Recovery (DR) environment. Oracle Data Guard will provide the necessary synchronization (active ↔ passive and DR site).

7.11 Security Hardware Architecture

Using the FIPS 199 system categorization process, VT HBE has been identified as having a system security level of Moderate. This categorization provides a basis for identifying a baseline set of security controls (identified in NIST SP 800-53) that are tailored based on CMS guidelines and customer specific security requirements. Additional security controls or modification of the baseline security controls is performed as a result of a risk assessment during the security control allocation phase of the NIST Risk Management Framework (RMF). To begin addressing these security controls, VT HBE will utilize the CMS technical reference architecture and implements a defense in-depth security posture using multiple zones of operation with each zone containing a set of security mechanisms providing protection, access control, and monitoring.

7.12 Additional Infrastructure Requirements

The follow table lists other various infrastructure requirements, as outlined in the VT HBE contract.

Exhibit 19: Other Design Patterns

Feature	Controls
Hosting Infrastructure	<p>Tier 1 Storage Area Network</p> <p>Redundant servers—multiple servers running in parallel using failover clustering for non-stop operations.</p> <p>Automated monitoring and alerting—Server, network, and storage health continuously monitored by automated tools to detect error conditions and alert engineers via pager to correct problems before an outage occurs. Incidents automatically escalated to take corrective action before Service Level Agreements (SLAs) are impacted.</p> <p>Server automated hardware fault reporting—Diagnostic data automatically uploaded to EMC hardware support when failures occur to dispatch technicians with the required parts for onsite repair.</p> <p>Application Performance Monitoring</p> <p>24x7 support—Our hardware vendors provide with on-site response support 24x7 in less than four hours.</p> <p>Vendor SLAs—We have SLAs with our vendors to provide rapid response to support requests.</p>
Network Connectivity	<p>Two telecommunication carriers—connectivity to data centers is provisioned by two different telecommunications carriers.</p> <p>Resilient local access—SONET ring provides redundant network loop at the primary data center; Alternate data center has carrier POPs.</p> <p>Multi-Protocol Label Switching (MPLS)—has high survivability due to its fully meshed nature.</p> <p>Redundant network components—All Local Area Network (LAN) components within the data centers are redundant with automatic failover.</p> <p>Automated alerting—Notifying engineers automatically of high priority incidents via pager ;</p> <p>Automatic escalations occur to take corrective action before SLAs are impacted.</p>
Data Center	<p>Redundant systems—N+1 redundant cooling, power, and telecommunications.</p> <p>Backup power—Uninterruptible Power Systems (UPS) prevent power spikes, brownouts and surges. Two diesel generators provide power in the event of a utility power outage. On site fuel is approximately 7,000 gallons, which can sustain the building for 10 to 12 days.</p> <p>Automated monitoring—Extensive monitoring process of network, servers and applications to detect problems, often before they affect availability and to support capacity-planning services to accurately distribute and accommodate load.</p>

Feature	Controls
Application	<p>The proposed Technical Architecture leverages a Java EE application server implementation, leveraging the Oracle WebLogic Application Server.</p> <p>Within the Java EE platform, the solution supports a SOA-based implementation with web services exposed for consumption within an enterprise service bus (ESB), a mechanism that manages access to applications and services (especially legacy versions) to present a single, simple, and consistent interface to end-users via Web- or forms-based client-side front ends.</p> <p>With this ability, we can upgrade, move, or replace solution components without disrupting existing business systems or modifying applications. Our solution uses the next generation and powerful Oracle Service Bus (OSB), a part of the Oracle SOA Suite that is highly scalable, supports open standards, and can plug and play along with various application servers.</p>
Data Management	<p>Data Management services include the various structured and unstructured data repositories that support the VT HBE system's business services. The transactional and analytical database for this solution use Oracle 11g with high availability as well as Clustered SQL Server.</p>

7.13 Descriptions of Operational/System Environment and Special Considerations

The Vermont Health Benefit Exchange (VT-HBE) system is a collection of online applications delivered as Software-as-a-Service in a cloud computing environment. In this delivery model, CGI is responsible for all of the service delivery layers including; infrastructure (that is, hardware and software that comprise the cloud infrastructure); data security, and service management processes (that is, the operation and management of the infrastructure and the system and software engineering lifecycles). This section provides a high-level overview of the CGI Cloud GSS.

The operational system environment for the VT HBE resides entirely within the virtualized environment of the CGI Infrastructure as a Service (IaaS) "Cloud" defined by the GSA FedRAMP authorization boundary. The authorization boundary for CGI's IaaS Cloud GSS includes type declarations for web hosting services whose controls agencies may reference in their major application authorization package. The CGI IaaS Cloud also includes infrastructure to manage many but not all of the security controls required to achieve an authority to operate (ATO) for a major application. The authorization boundary includes tenant-specific boundaries that CGI establishes for each new tenant in the CGI Data Centers supporting the CGI IaaS Cloud. The boundary also includes the CGI IaaS Cloud general support system (GSS) which services all tenants in the CGI IaaS Cloud.

CGI provisions each tenant with six network zones implemented with virtual Local Area Networks (VLANs) by default in which they may provision web hosting services. These zones include a web, application and data zone at each of the CGI Data Centers. The tenant is also provisioned with their own dedicated Virtual Private Network (VPN) zone through which they can connect to their network zones and can access the CGI IaaS Cloud management portal. The VPN zone is routed across all of CGI's data centers supporting the federal cloud. Access into the VPN zone is granted using a Secure Socket Layer (SSL) VPN initiated from the CGI IaaS Cloud public facing website. The CGI IaaS Cloud public website is available over the Internet. This SSL VPN leverages Active Directory and RSA On-Demand tokens to provide access into a tenant's VPN zone and is only intended for administrative access to a tenant's environment.

7.14 Applicable Laws or Regulations: VT HBE Security

The following are the laws and regulations that affect the system:

- 42 U.S.C. 300, Patient Protection and Affordable Care Act, 2010
- 44 U.S.C. 3541, Federal Information Security Management Act, 2002
- 5 U. S. C. 552, Freedom of Information Act, 1967
- 5 U. S. C. 552a, Privacy Act, 1974
- 18 U. S. C. 1030 (a) (3), Fraud and related activity in connection with computers
- 38 U. S. C. 218, Security and law enforcement on property under the jurisdiction of the Administration
- 38 U. S. C. 3301, Confidential nature of claims
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-18, Guide for Developing System Security Plans
- NIST SP 800-27, Draft, Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30, Draft, Rev A, Risk Management Guide for Information Technology Systems
- NIST SP 800-34, Rev 1, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-37 Rev1, Guide for Applying the Risk Management Framework to Federal Information Systems
- NIST SP 800-42, Guideline on Network Security Testing
- NIST SP 800-53r3, Recommended Security Controls for Federal Information Systems
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-61, Computer Security Incident Handling Guide
- NIST SP 800-64, Security Considerations in the Information System Development Life Cycle
- Public Law (PL) 99-474, The Computer Fraud and Abuse Act of 1986
- PL 93-502 - Freedom of Information Act 1974

7.15 Rules of Behavior: Security

Rules of behavior are still under development for the VT HBE; however current policies and procedures within the cloud are based on NIST 800-53 regulations and include the following:

- **Password construction / maintenance** – Passwords are created and maintained in the CGI Cloud accordance with the password policy; Passwords are changed every 90 days.
- **Changing system data** – System data is maintained by authorized users in accordance with the controls under the AC, AU, SA, SI, and CM control objectives.
- **Searching databases** – Database access is based on the concept of “least privilege” access; audit logging and monitoring assist the oversight of database user operations, file integrity and unauthorized changes.
- **Divulging information** – Personnel are to be trained on handling PII and FTI and complete ROB and acknowledgements that limit us.
- **Working at home** – The VT HBE has not determined an appropriate Work at Home model.
- **Dial-in access** – Dial in access is restricted through specific secure channels with appropriately secure computing resources.

- **Assignment and limitation of system privileges** - As described, privileges are maintained by authorized users in accordance with the controls under the AC, AU, SA, SI, and CM control objectives.
- The consequences of non-compliance clearly states the exact behavior expected of each person. Specific consequences are under development.

7.16 Review of Security Controls

The security controls for the CGI Cloud supporting the VT HBE were reviewed in 2011 as part of the GSA FedRAMP Accreditation process, and are reviewed independently by third-party audit annually.

8 Security Controls Detail and Comment

The SSP and SPR coupled together provide the comprehensive control requirements that must be documented for the protection of all data received, stored, processed, and transmitted by the health insurance exchanges and data services hub for implementation of the ACA legislation. Security controls common to both CMS and IRS requirements are documented in the SSP. Security controls specific to the protection of FTI or requirements above the common control baseline must be documented in the SPR. Together, the SSP and SPR form the description of the controls in place to protect all data contained in health insurance exchange and data services hub systems – both FTI and non-FTI.

Please refer to the *D-24 System Security Plan* document for Security Controls Details and Comments. This document contains specific information regarding VT HBE security policies governing Access Control, Audit and Accountability, Certifications, Configuration Management, as well as Identity Management and the tools involved.

9 Other Hardware Protection and Security Measures

The network Infrastructure design for the VT HBE environments will have dedicated security zones and firewall policies to promote isolation from other applications within the data center. Redundant security components such as firewall devices, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) will be configured to protect HBE environments from potential security attacks.

9.1 Security Devices

The network Infrastructure design will be configured so that all network traffic in the form of data packets to access the VT HBE application for all environments will traverse through secured firewall security devices. The firewall security device setup/configuration will be similar between both the Primary Data Center (Phoenix) and Secondary Data Center (Philadelphia), with the exception that the Primary Data Center will have redundant firewall devices. There will be two firewall devices each for the Production environment and the rest of the test environments configured in the Primary Data Center for redundancy so there will be an automatic fail over to another device should there be problems.

Following the firewall, the network traffic in the form of data packets will then traverse through another level of Intrusion Detection Services (IDS)/Intrusion Prevention technology (IPS) security devices to protect against any unwanted traffic using deep packet inspection. As packets pass through the IPS, they are inspected to determine whether they are legitimate or malicious. This is another security protection, and its placement protects the IPS/IDS from having to inspect unnecessary traffic that will be dropped by the firewall.

Following the IDS/IPS, depending upon the environment the user is trying to navigate, the network traffic in the form of packets will be routed to that environment network zone as explained below. Each network

zone will be configured to have its own, dedicated Virtual Local Area Network (VLANs) so they are further secured and can communicate with one another avoiding any traffic communication issues.

9.2 Security Zones

Security zones are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts and block any traffic that has not been explicitly allowed. Any routing between the zones will have to traverse the firewall and, to keep with security policies, each zone is allocated its own VLAN.

There will be three security zones configured per environment including:

1. External Zone
2. Application Zone
3. Database Zone

9.2.1 Security Zones – External Zone

The External or Web Zone is a demilitarized zone (DMZ) where the external accessible Web/application servers will be configured. In this zone, the configuration will further be designed to have two layers, one for external and the other for internal traffic. This layer three security zone is utilized as a gateway for the load balancer. Network load balancing will be made available on servers in the Web Tier for both external and internal user traffic. Load balancers will be used for distributing load across the Web nodes. Traffic is then sent to multiple hosts from the load balancer as it sees fit in order to keep the traffic load shared among the hosts.

The servers in this zone will be allowed communications using firewall configurations from and to other zones using specific ports per servers.

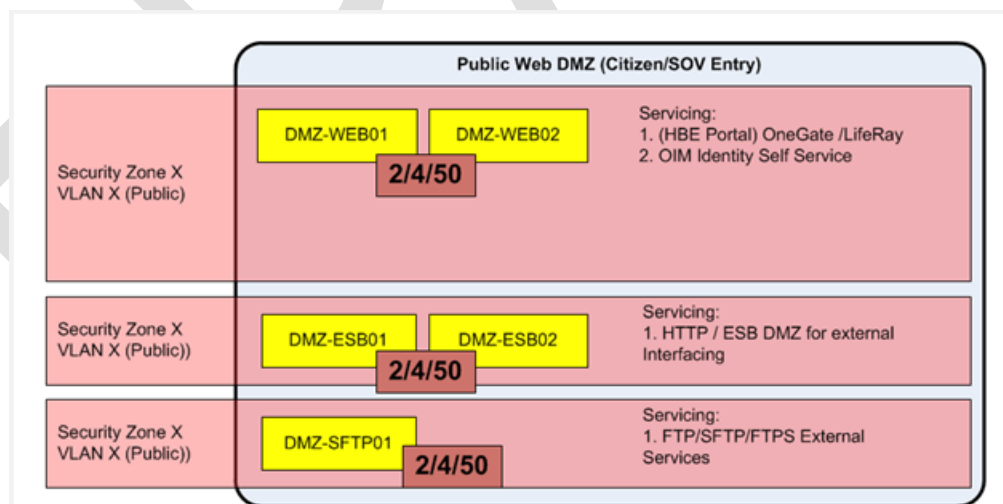


Exhibit 20: External Zone

9.2.2 Security Zones – Application Zone

The Application Zone is an internal zone where those application tier/layer components will be configured that cannot be accessed from the Internet users. These additional security measures are designed such that the servers in this zone are not going to be exposed from Internet users.

The servers in this zone will be allowed communications using firewall configurations from and to other zones using specific ports per servers. An example of the Application Security Zone for both Oracle and WebLogic is shown below:

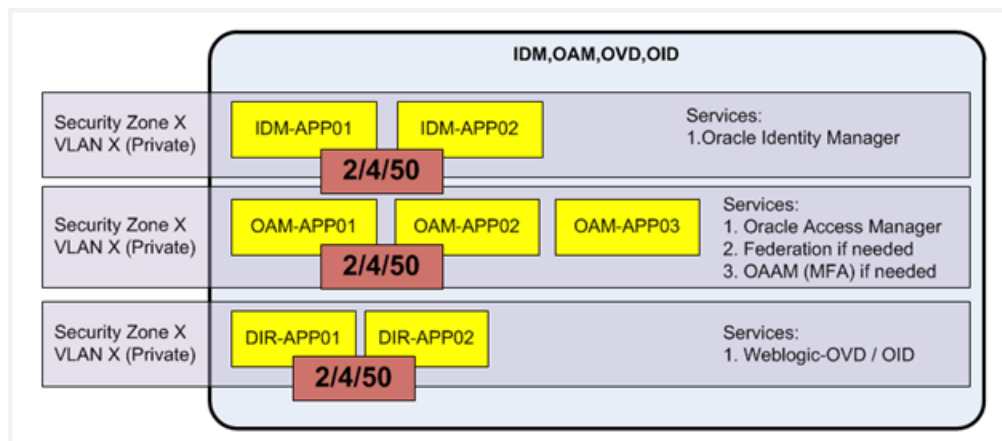


Exhibit 21: Application Zone

9.2.3 Security Zones – Database Zone

The Database Zone is an internal zone where those database tier/layer components will be configured that cannot be accessed from the Internet users. These are additional security measures designed such that the servers in this zone are not going to be exposed by Internet users.

The servers in this zone will be allowed communications using firewall configurations from and to other zones using specific ports per servers. A sample of a Database Security Zone is shown in the figure below:

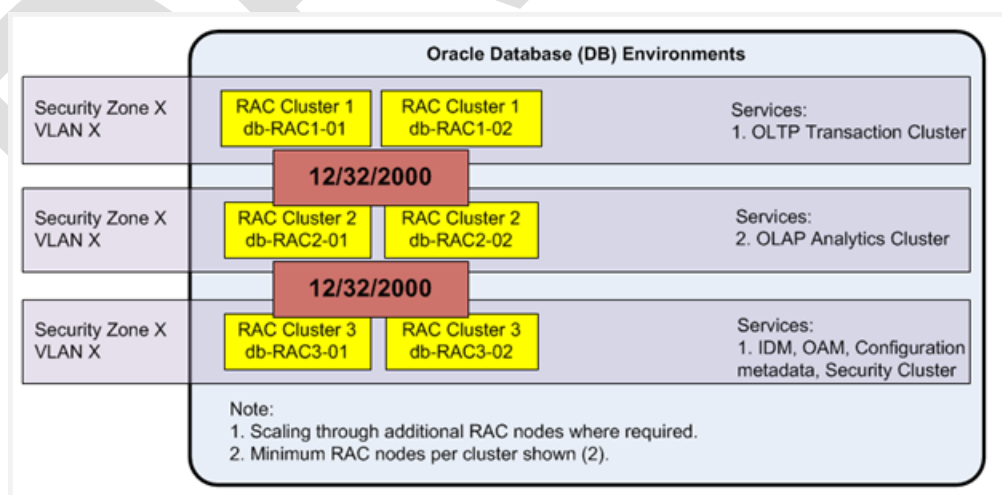


Exhibit 22: Database Zone

10 Performance Hardware Architecture

The Vermont Health Benefit Exchange hardware is tuned for optimum performance and scalability. Load balancing and server farms are employed on all levels of the system to spread the load across multiple servers. The Production and Non Production databases are clustered to provide high availability, redundancy, scalability, and security as follows:

1. **High availability (HA)** – The environment will be designed to be highly available by setting up;
 - a) Virtual environments using OVM (Oracle Virtual Machine) technology
 - b) Physical database servers using Oracle RAC (Real Application Cluster)
2. **Redundancy** – Redundant networking security devices such as routers, firewalls, and network load balancers will be setup to promote reliability
3. **Scalability** – Additional computing resources will be added to the infrastructure as required
4. **Security** – Network will be setup using multiple security zones. One security zone per environment will be configured with firewall rules to provide controlled access to a specific zone

The infrastructure described above, along with the items described in the next section will result in optimal hardware reliability and performance.

10.1 Architectural Performance Guidelines

1. Segregate application services and installs (minimize running everything on 1 server)
2. Clearly define security boundaries between users, web (dmz,WAN), application and database zones.
3. Design for quick and predictable vertical and horizontal scaling.
4. Vertical scaling through more CPU, memory, disk space, and a virtual infrastructure
5. Horizontal scaling through load balanced web, application and database instances
6. Segregate database workloads based on usage. OLTP (Transactional), versus OLAP (Star Schema) versus Other (Security)
7. All interactions between autonomous applications will utilize Enterprise Service Bus for data access.

10.2 Software Architecture

The Software Architecture is primarily a system of layered containers, the foremost of which is WebLogic Server (WLS), providing classical High Availability (through clustering), Security support, and Configuration and Operational Management services. There are numerous WLS instances in the OneGate system – an Administration Server that serves as a primary director, and several Managed Servers that provide specific areas of support, including SOA Server, WebCenter, IDM and others. There is, in fact, an instance of a Managed Server supporting most Oracle system components.

The Managed Servers provide a wide array of tools for support of their respective portion of the overall solution software; providing tools for monitoring, configuration, loading, and unloading of executable components and tracking performance and loading.

Layered on top of these underlying infrastructure components are the application layers noted earlier in this document: Presentation, Middleware, and Data.

From an application server perspective, the primary component is the Liferay Portal. Liferay is based on an MVC pattern through its use of JSP's for providing page content and Portlet support. Additionally, it supports an Inversion of Control (IoC) pattern implementation through its use of the Spring Framework. The primary toolsets needed for development and maintenance are:

- Eclipse for maintenance and coding of JSP's and Spring code
- SQL Developer for database and stored procedure development and maintenance
- Subversion for code control
- Maven for automated build management

There is also a presentation layer provided by Siebel, though Siebel is an exception to the general Oracle approach of layered containers. It does not directly rely on a Managed Server, and interface development and maintenance is provided for within the product itself.

Middleware is an essential layer in the OneGate system, as well as more generally in the overall VT HBE solution. We divide the VT HBE solution into two fundamental logical layers – Internal and External. Internal consists of the OneGate system, while external is a completely custom layer providing interfaces to external partners for the VT HBE (for example, Carriers, CMS, Premium Processor, and SERFF). A fundamental architectural premise in the VT HBE system is that all communication to the external world be routed through the external integration layer; so, for instance, no Liferay or Siebel functional module would ever directly integrate to a Carrier or communicate to a CMS service – all would be directed through the external integration layer.

Both internal and external middleware rests primarily on the Oracle SOA Suite, and an underlying Oracle Service Bus implementation. The primary tool of development, maintenance and deployment is Oracle's JDeveloper.

The middleware layer (specifically SOA Suite-based composites) will utilize another SOA Suite product – the Oracle Business Rules (OBR). This product provides for both table-based and hierarchical rules configuration that can be carried out dynamically, without needing to redeploy code. The OBR will provide a repository for business domain experts to dynamically configure business-driven operational rules for the OneGate application systems.

OBR is not the only rules repository – there is also a significant rules foundation provided in another Oracle product – Oracle Policy Automation (OPA). This product represents another departure from the Oracle WLS-based architecture and is very much a stand-alone system in the same vein as Siebel. Similar to Siebel, OPA rules modeling takes place within the system itself, in its own IDE called Oracle Policy Modeler (OPM). The expression of the rules, within OPM, actually occurs in a Microsoft Word or Excel document structure.

Other Oracle systems providing application software support are:

- IDM
- WebCenter Content
- OBIEE
- MDM

These are described elsewhere in this document, but configuration and solution deployment for all of these are provided in precisely the same fashion as noted above – configuration is carried out through managed server pages and any coding customization, as appropriate, is handled through JDeveloper.

The following table provides a list of Software being utilized for the VT HBE solution.

Exhibit 23: Software Utilized for the VT HBE Solution

Tier	Web/App/DB Zones from Visio	Application
Web	Public Web DMZ (citizen/SOV Entry)	OneGate /Liferay (HBE Portal)
Web	Private Web WAN (Partner/SOV Entry)	Siebel-SWE
Web	Private Web WAN (Partner/SOV Entry)	Oracle - OBIEE Web Front Ends; OneGate /Liferay
Web	Private Web WAN (Management)	Master Data Management (MDM) App.Mang.Web Frontend
Web	Private Web WAN (Management)	Oracle WebCenter Capture - Index/Scan/Commit, Forms/Barcode recognition server and Import server components
App	Siebel Product Suite	Siebel - Object Manager AOM
App	Siebel Product Suite	Siebel Gateway / FS / EIM / EAI / Workflow / Assignment MGR
App	Siebel Product Suite	Siebel Report Server Windows
App	Liferay/OneGate	OneGate/Liferay Application Server Container
App	Enterprise Content Management (ECM)	Thunderhead Web Center Content
App	MDM	Master Data Management (MDM)
App	Oracle Policy Automation (OPA)	OPA Engine / Windows Desktop Client / Oracle Policy Modeler (OPM)
App	IDM, OAM, OVD, OID	Oracle Identity Manager (OIM) / Oracle Access Manager (OAM)
App	IDM, OAM, OVD, OID	Oracle Access Manager (OAM)
App	IDM, OAM, OVD, OID	WebLogic; Oracle Internet Directory (OID)/ Oracle Virtual Directory (OVD)
App	Business Int/ETL/OBIEE	OBI Presentation Services Plugin / IBI Presentation Services / OBI Cluster Controller / WebLogic
App	Oracle Enterprise Service Bus (ESB/OSB)	OSB / BPM / Coherence / BAM / Healthcare Adaptor / HIPAA Accelerator / WebLogic / FTP
App	Oracle Enterprise Service Bus (ESB/OSB)	OSB / BPM / Coherence / BAM / Healthcare Adaptor / HIPAA Accelerator / WebLogic / FTP
App	Oracle Enterprise Service Bus (ESB/OSB)	OSB / BPM / Coherence / BAM / Healthcare Adaptor / HIPAA Accelerator / WebLogic / FTP
App	Administrative Environment (AM)	App Mgmt for Siebel
Database	Oracle Database (DB) Environment	OLTP Transaction Cluster
Database	Oracle Database (DB) Environment	OLAP Analytics Cluster
Database	Oracle Database (DB) Environment	IDM, OAM, Configuration metadata, Security Cluster
App	Administrative Environment (AM)	Subversion - Code Repository
App	Administrative Environment (AM)	Build Server

10.3 Security Software Architecture

The VT HBE technical architecture is compliant with Federal Enterprise Architecture Framework (FEAF), and aligns well with the DHHS CMS Guidance for Exchange and Medicaid Information Technology (IT) Systems and Medicaid Information Technology Architecture (MITA).

These industry and federal guidelines promote the use of key standards that are also supported with Technical Architecture such as SOAP, XML, UDDI, WSDL, BPEL, SAML, and NIST security standards.

Exhibit 24: Technical Architecture Capabilities and Features

Representative Technical Architecture Capabilities	Technical Architecture Features
Web services and adherence to key frameworks and standards	<ul style="list-style-type: none"> FEAF, MITA, and SCEA frameworks and standards Open standards such as SOAP, XML, UDDI, WSDL, BPEL, SAML and NIST security OTech standards and guidelines for flexibility in on-premise hosting should the State desire an alternative to Cloud Computing implementation Messaging formats such as HIPAA 834 and 270/271
Scalability and optimized resource utilization	<ul style="list-style-type: none"> Multi-tiered architecture Clear separation between presentation, application, and database tiers enable horizontal and vertical scalability Virtualization Clustering solutions
Communication, Data, and Process Integration	<ul style="list-style-type: none"> Use of ESB for reliable communication channels and protocols for integration Synchronous and asynchronous communication operations
Fault Tolerance	<ul style="list-style-type: none"> Redundancy to minimize single points of failure Use of redundant components Failure detection Recovery and bypass mechanisms built into the solution Auto-reconfiguration to minimize downtime
Fault Avoidance	<ul style="list-style-type: none"> Use of highly reliable solution components containing data loss

10.4 Functional Activity Logging

The Vermont Health Benefit Exchange System will record and maintain a log of certain functional activity.

Each application component will create its own logs, and a composite service will collect, collocate, and correlate all activities performed by each user and functional activities performed by the System on behalf of each user.

The activity logs will contain records of system usage (logins); user activity (pages viewed, data entered and actions taken); user interaction patterns such as use of decision tools, filters and sorts; services invoked; data exchanged; and the like. The logging service will add meta-data such as activity origination, timestamp, and actor ID to facilitate correlation and audit reviews.

10.5 Technical Monitoring, Logging, and Auditing

Auditing requirements include the standard Government Cloud offering, as well as additional, more granular audit trails resulting from the design phase. The auditing and monitoring solution highlights include:

- Conform to a standard process for generating, transmitting, storing, analyzing, and disposing of security log data.
- Routine log analysis for identifying security incidents, policy violations, fraudulent activity, and operational problems.
- User-friendly audit trail to capture a history of certain transactions processed by the system.
- Utilize security features such as role-based access controls and auditing of administrative actions to provide an accountability audit trail among the administrators.
- Configure monitoring tools to alert assigned automation system administrators to address processing failure.

10.6 Other Security Measures

Software used in the Vermont Health Benefit Exchange goes through strict evaluation for security and is tested to meet the security standards of both the State of Vermont and CGI before it is purchased. In addition to these evaluations, CGI employs the following security architecture software installed on CGI servers:

- **Eavesdropping resistance:** The information systems utilize eavesdropping resistant protocols to make it impractical for an attacker to carry out an off-line attack where he/she records an authentication protocol run then analyses it on his/her own system for an extended period, for example by systematically attempting to try every password in a large dictionary, or by brute force exhaustion.
- **Password Guessing Resistance:** The information system protects against password guessing by requiring use of high-entropy passwords and limiting the number of unsuccessful authentication attempts, or by controlling the rate at which attempts can be carried out.
- **Hijacking Resistance:** The information system uses an authentication and transfer protocol combination which is resistant to hijacking if the authentication is bound to the transfer in a manner that prevents an adversary capable of inserting, deleting, or rerouting messages from altering the contents of any information sent between the claimant and the relying party without being detected.
- **Verifier Impersonation Resistance:** The information system uses a secure authentication protocol that is resistant to verifier impersonation if the impersonator does not learn the value of any token when acting as the verifier.
- **Man-in-the-middle Resistance:** The information system uses authentication protocols that are resistant to a man-in-the-middle attack when both parties (e.g., claimant and verifier) are authenticated to the other in a manner that prevents the undetected participation of a third party.

10.7 VT HBE User Authentication, Authorization, and Account Management

This section describes the VT HBE application's user authentication, authorization, and account management design using Oracle Identity and Access Management solution. The Oracle Identity Management suite is comprised of tools that collectively offer identity and access management capabilities to the VT HBE. These solutions are described in the following table.

Exhibit 25: Oracle Identity and Access Management Solution Tools

Oracle Identity & Access Management Solution	Description
Oracle Universal Directory (OUD)	<ul style="list-style-type: none"> ▪ The user authentication repository for the VT HBE ▪ It stores user's basic profile along with security attributes (e.g., password, access roles)
Oracle Identity Manager (OIM)	<ul style="list-style-type: none"> ▪ Used for user account management operations (e.g., create, add, disable) ▪ Assigns user account policies during account operations ▪ Single point of control for the user repository (security) of the VT HBE
Oracle Access Manager (OAM)	<ul style="list-style-type: none"> ▪ Enforces user authentication and authorization to the VT HBE application screens ▪ Enforces account policies (for example, session timeout, account lockout) ▪ First line of defense for user authorization (that is, determines access to VT HBE screens) to the HBE application
Oracle Adaptive Access Manager (OAAM)	<ul style="list-style-type: none"> ▪ Works in collaboration with OAM to enforce authentication to the VT HBE application screens ▪ Enforces multifactor authentication for a privileged user accessing the VT HBE application screens

10.8 Logical Design: Access and Identity Management

This section provides the logical design view of VT HBE's identity and access management solution that is comprised of Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM) and Oracle Internet Directory (OID). All the process steps for Oracle Identity Manager and Oracle Identity Manager SOA are background processes that get executed on their respective servers.

10.9 Logical Architecture for User Account Management

Oracle Identity Management solution's tool is used for managing users that have access to the VT HBE application. The user account management processes include account management actions such as creating users, creating organizations, updating user profiles, updating organization profiles, enabling users, disabling users, and changing passwords.

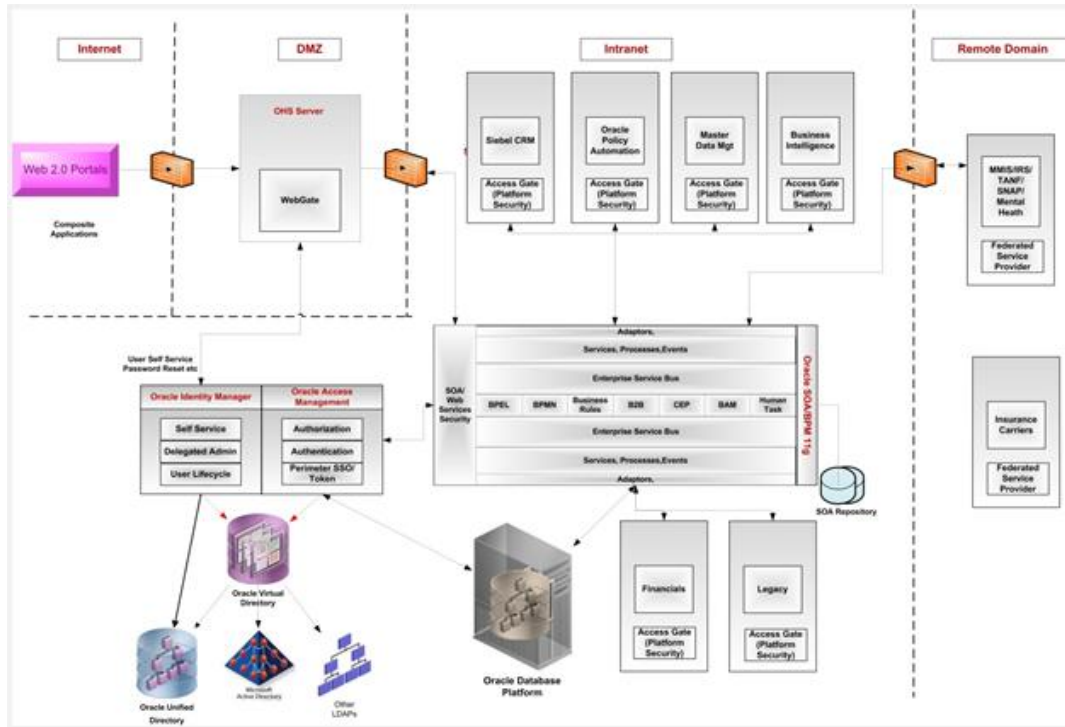


Exhibit 26: User Authentication & Authorization: Solution Overview

The components shown in the figure above are described in the following table:

Exhibit 27: User Account Management: Components

No.	Component	Utilized For:
1.	OIM	<ol style="list-style-type: none"> User registration and maintenance for the following set of users: <ol style="list-style-type: none"> Internal External System accounts Managing and enforcing password policy for the VT HBE application
2.	Oracle Universal Directory (OUD)	<ol style="list-style-type: none"> Serving as the LDAP based authentication user store for the VT HBE application Persisting: <ol style="list-style-type: none"> VT HBE application user profile VT HBE application user authentication credentials VT HBE application user authorization
3.	OIM Database	<ol style="list-style-type: none"> Storing OIM access policies and password policies Storing OIM approval/provisioning/schedulers configurations
4.	OID Database	<ol style="list-style-type: none"> Serving as the backend data store for OID Persisting user details (such as attributes and group membership) in Relational Database Management System format

No.	Component	Utilized For:
5.	OIM API Package	1. Providing a Java-based application programming interface (API) package that externalizes key OIM functions that can be invoked from the HBE application for user management scenarios
6.	OAAM	1. Working in collaboration with OAM to provide multifactor authentication services for privileged users
7.	OAAM Database	1. Storing OAAM user store for the VT HBE application 2. Policy and metadata store for OAAM
8.	Oracle Virtual Directory	1. Oracle Virtual Directory provides Internet and industry-standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.
9.	Lightweight Directory Access Protocol (LDAP)	1. LDAP is a standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate.

10.10 Logical Architecture for User Authentication and Authorization

OAM and OAAM are the tools from the Oracle IDM solution that are used for authentication and authorization for users who will access the VT HBE application. The user authentication processes include validating user credentials, authorizing users to the VT HBE application screens, enforcing multifactor authentication, managing session timeouts and inactivity timeouts.

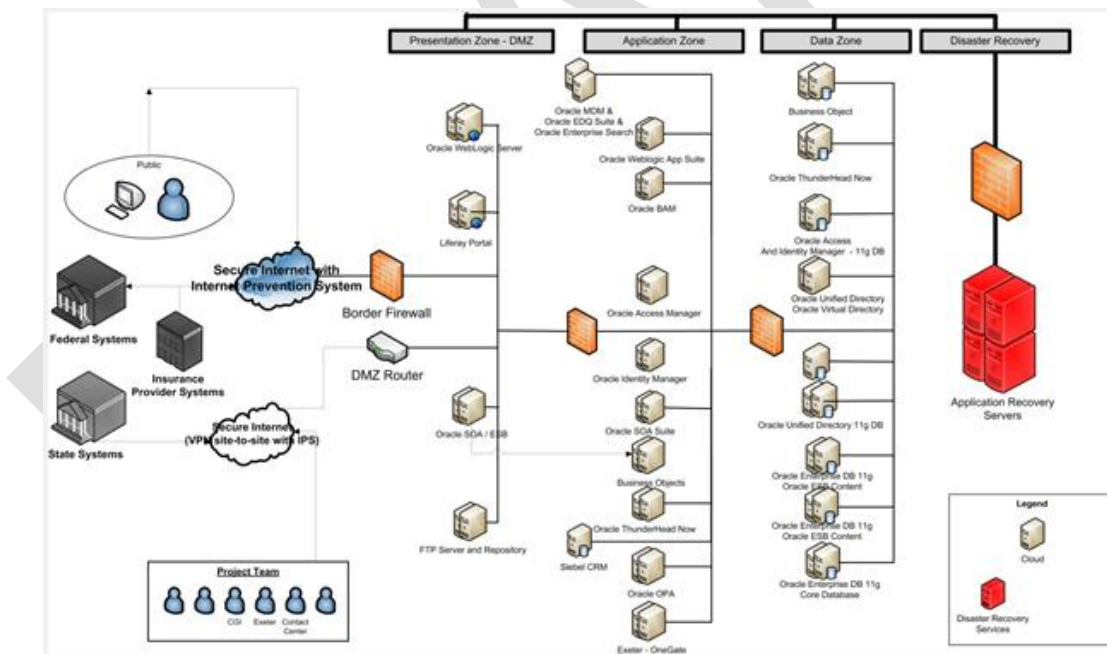


Exhibit 28: User Authentication & Authorization: Components by Tier

The functions of each component depicted in the preceding Figure are described in the following table:

Exhibit 29: Component Features

No.	Component	Utilized For:
1.	OAM	<ul style="list-style-type: none"> ▪ Authenticating and authorizing users ▪ Identifying user's role and group membership ▪ Enforcing password policy ▪ Providing advanced status flags such as Reset Password, Password Expired, User Locked, and others
2.	ODU	<ul style="list-style-type: none"> ▪ Serving as the LDAP based user store for the VT HBE application ▪ Providing credential validation and user details retrieval functionality
3.	OAM Agent	<ul style="list-style-type: none"> ▪ Intercepting Web requests and enforcing access management policies for authentication and authorization ▪ Communicating with OAM on SSL port with message encryption using webserver specific encryption keys
4.	OAM Database	<ul style="list-style-type: none"> ▪ Persisting policies and configuration details for OAM server ▪ Persisting protection scheme details for the VT HBE application screens for authentication and authorization
5.	OID Database	<ul style="list-style-type: none"> ▪ Persistent layer for OID ▪ OID maps LDAP based structure to relational database objects in the OID Database
6.	OAAM	<ul style="list-style-type: none"> ▪ Supporting primary and multi-factor authentication by working in collaboration with OAM
7.	OAAM Database	<ul style="list-style-type: none"> ▪ Storing OAAM user store for the VT HBE application ▪ Policy and metadata store for OAAM
8.	SOA for OIM	<p>Workflow-based provisioning is a key feature of Oracle Identity Manager that enables you to automate the business processes that manage user access in an organization. Oracle Identity Manager leverages services enabled and managed by Oracle Service-Oriented Architecture (SOA) Suite to provide an interactive environment to request, approve, and manage user access. Oracle SOA Suite provides the back-end services and management capabilities required to implement SOA.</p> <p>Oracle Identity Manager makes use of the following components of the SOA Suite:</p> <ul style="list-style-type: none"> ▪ BPEL Process Manager, which provides the end-to-end solution for creating and managing business processes ▪ Human Workflow, which manages the lifecycle of human tasks, including creation, assignment, deadlines, expiration, and notifications ▪ Oracle Business Rules, which allows you to define complex business rules to support request assignment, process selection, and approver resolution

10.11 Performance Software Architecture

Software used by the Vermont Health Benefit Exchange goes through strict evaluation for performance. In addition to this evaluation, CGI also employs the following performance tools into its architecture:

- Load Balancing to help ensure that performance is continuously at a high level on the Application and Web Servers.
- Server clustering via Rack Clusters to help ensure that the database servers will deliver high performance.
- Performance Monitoring software is included in the Service Layer of the VT HBE Solution.

11 Records Management

The Records Management Plan (“HBE RMP”) provides the records management strategy and approach for the CCHIO Federal Exchange project, including the scope, goals, and objectives. The RMP details how the records will be organized, maintained, and monitored. It further details the methodology for records management that will be employed during the entire project life cycle. The information in the RMP provides the basis for communication and common understanding among project team members and other stakeholders. The RMP forms the basis for an agreement between all project teams and stakeholders associated with the VT HBE project. At a minimum, the RMP will include the following elements:

- Overview
- Accountability
- Integrity
- Protection
- Compliance
- Availability
- Retention
- Disposition
- Transparency

The RMP is to be established under guidance from the CMS Records Management Officer (Office of Strategic Operations and Regulatory Affairs (OSORA)/Issuances and Records Management Group) so that the RMP is in line with Federal records management regulations as well as CMS policies and procedures.

11.1 Internal Communications Architecture

For more information, see section 7 *System Architecture*.

11.2 System Architecture Diagram

For more information, see section 7 *System Architecture*.

12 Data Design

The Vermont Health Benefit Exchange data design is based on industry standard principles and guidelines that focus on storing and maintaining quality and complete information in a highly efficient and secured way. Summarized below are some of the data design principles that have been applied to the VT HBE databases:

- **Operational requirements**

Operational requirements are needed to be met by a database in order to effectively support an application when operational. Though it typically may be expected that operational requirements are automatically met by a DBMS, in fact it is not so in most cases: To be met a substantial work of design and tuning is typically needed. This is typically done by specific instructions/operations through special database user interfaces and tools, and thus may be viewed as secondary functional requirements (which are not less in important than the primary requirements).

- **Availability**

A database should maintain needed levels of availability, that is, the database needs to be available in a way that a user's action does not need to wait beyond a certain time range before starting the execution upon the database. Availability also relates to failure and recovery from it. Upon failure

and during recovery normal availability changes and special measures are needed to satisfy availability requirements.

- **Isolation between users**

When multiple users access the database concurrently the actions of a user should be uninterrupted and unaffected by actions of other users. These concurrent actions should maintain the database's consistency (that is, keep the database from corruption).

- **Recovery from failure and disaster**

All computer systems, including DBMSs, are prone to failures for many reasons (both software and hardware related). Failures typically corrupt the database, often to the extent that it is impossible to repair it without taking special measures. The DBMS should provide automatic recovery from failure procedures that repair the database and return it to a well-defined state.

- **Data independence**

Data independence pertains to a database's life cycle. It strongly impacts the convenience and cost of maintaining an application and its database, and has been the major motivation for the emergence and success of the Relational model, as well as the convergence to common database architecture. In general the term "data independence" means that changes in the database's structure do not require changes in its application's computer programs, and that changes in the database at a certain architectural level do not affect the database's levels above. Data independence is achieved to a great extent in a contemporary DBMS, but it is not completely attainable, and achieved at different degrees for different types of database structural changes.

- **Security**

Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers, and the associated network links) against compromises of their confidentiality, integrity, and availability. It involves various types or categories of controls, such as technical, procedural/administrative, and physical.

Many layers and types of information security control are appropriate to databases, including:

- Access control
- Auditing
- Authentication
- Encryption
- Integrity controls
- Backups
- Application security
- Scalability

Scalability is the capability to manage resources to yield a linear (ideally) increase in service capacity. The key characteristic of a scalable database is that additional load only requires additional resources rather than extensive modification of the database itself.

12.1 Data Objects and Resultant Data Structures

The following main categories of data will be collected, and stored or transferred from outside sources:

- Employers – Employer data, Employer, and Employee plan data
- Account – ID and Passwords for the public-facing component of the Health Benefit Exchange and knowledge based challenge questions, answer choices, and correct answers
- Household – Relationships between household members

- Person – General person information such as demographics, citizenship, and contact details
- Income – Income information about a person
- Expenses – Expense information about a person
- Insurance – Current insurance information
- Premium – Billing, Premium Pay, Premium Pay history, Pay profile
- Plan info – Information related to active/non-active individual benefit programs

Note: The above is a high level list of data categories and is not all inclusive at this point in time.

The data to be gathered for the purpose of the VT-HBE project will be mutually exclusive data, numeric, relative and absolute measure count. Hence, the data types will be nominal (belonging to a definable category), ordinal (the values can be counted), primitive, and measure (relative values).

12.2 File and Database Structures

Refer to deliverable *D-19 Database Design Document* for information about the File and Database Structures.

12.3 Database Management System Files

Refer to deliverable *D-19 Database Design Document* for information about the Database Management System Files.

12.4 Non-Database Management System Files

Refer to deliverable *D-19 Database Design Document* and *D-20 Data Management Plan* for information about the Non-Database Management System Files.

13 User and Machine Readable Interface

13.1 Inputs

Exhibit 30: User and Machine Readable Inputs

Record Content	Format	Input Method	Source
Single Streamlined Application (SSAp)	Paper	Manual completion of paper form	Applicant (individual or small employer)
	Image of paper (above)	Scanner	Applicant
	Electronic	Manual input to web page	Applicant, Broker, Service Rep
Enrollment Application	Electronic	From SSAp	See above
Eligibility determination – Medicaid, use of Exchange	Electronic	System Interface System determination	CMS, Exchange
Official document used to verify SSAp	Paper	Scanner (original returned to supplier)	Applicant

Record Content	Format	Input Method	Source
data and/or eligibility			
	Electronic	System upload	Applicant or broker
Enrollment in QHP or other disposition by carrier or Exchange	Electronic	System Interface System determination	Carrier Exchange
Correspondence – Outbound, including Notices and Notifications	Paper (sent to recipient)	Electronic	Exchange System
	Electronic (email)	Electronic	Exchange System
Evidence or suspicion of Fraud, Waste, Abuse (FWA)	Electronic or paper	Personal computer or Exchange system	Exchange staff, other authorized sources
Eligibility determination – APTC, CSR	Electronic	System Interface	Federal Data Services Hub (FDSH)
Submission of Initial Payment by Individual	Electronic	Manual input to web page	Individual applicant
Monthly Payment by Employer	Electronic – CR/DR card, ACH or check image	Manual input to web page	SHOP applicant – employer
Correspondence – Inbound, other than general inquiries	Paper	Scanner	Account holder
	Electronic	Email or Exchange web page	
Service-center incidents (calls or emails)	Electronic	Service Center manual input and incident recording, or email	Exchange CRM
Invoice to carrier or employer	PDF (paper or electronic medium)	Electronic	Exchange System
Reconciliation of invoice and payment	Electronic	System interface, electronic and manual entry into Exchange system	Exchange system, employer system, carrier system
Appeal	Electronic	Manual input to web page or Service Center manual input and incident recording	Applicant or broker
Complaint	Electronic	Manual input to web page or Service Center manual input and incident recording	Applicant or broker
General Inquiries, telephonic	Electronic	Recording of calls to Service Center	Telephone calls

Record Content	Format	Input Method	Source
General Inquiries, data	Electronic	Email or Exchange web page	Account holder
General Inquiries, paper	Paper	Scanner	Account holder
Stakeholder feedback	Electronic	Manual input to web page or Service Center manual input and incident recording	Any external stakeholder
Login credentials	Electronic	Manual input to web page	System user
QHP definition	Electronic	System Interface	SERFF
Provider Directory	Electronic	System Interface	Vendor
Federal Tax Information	Electronic	System Interface	Federal Data Services Hub (FDSH)

13.2 Outputs

The high-level operational scenarios in the *Operational Scenarios* section provide an overview of how data will flow through the VT HBE solution.

Operational Scenarios

13.3 Scenario 1: Pre-Screening Individual

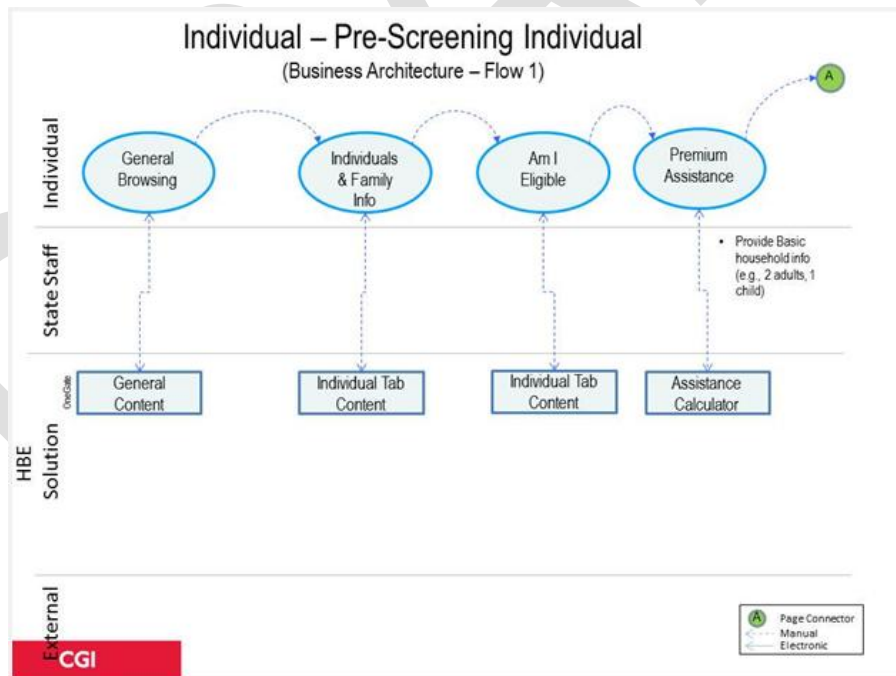


Exhibit 31: Pre-Screening Individual (Business Architecture – Flow 1)

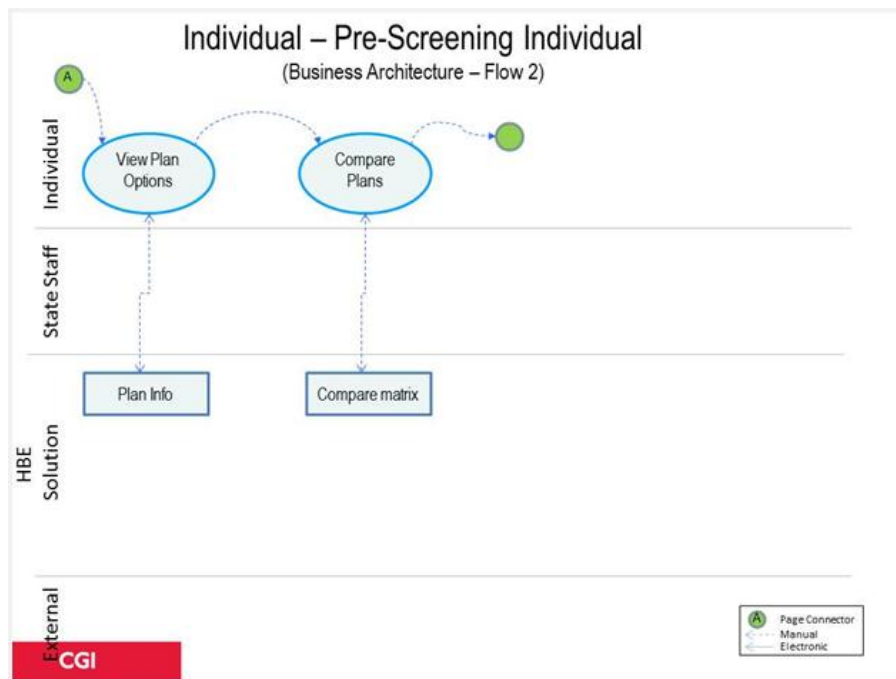


Exhibit 32: Pre-Screening Individual (Business Architecture – Flow 2)

13.4 Scenario 2: Individual Enrollment

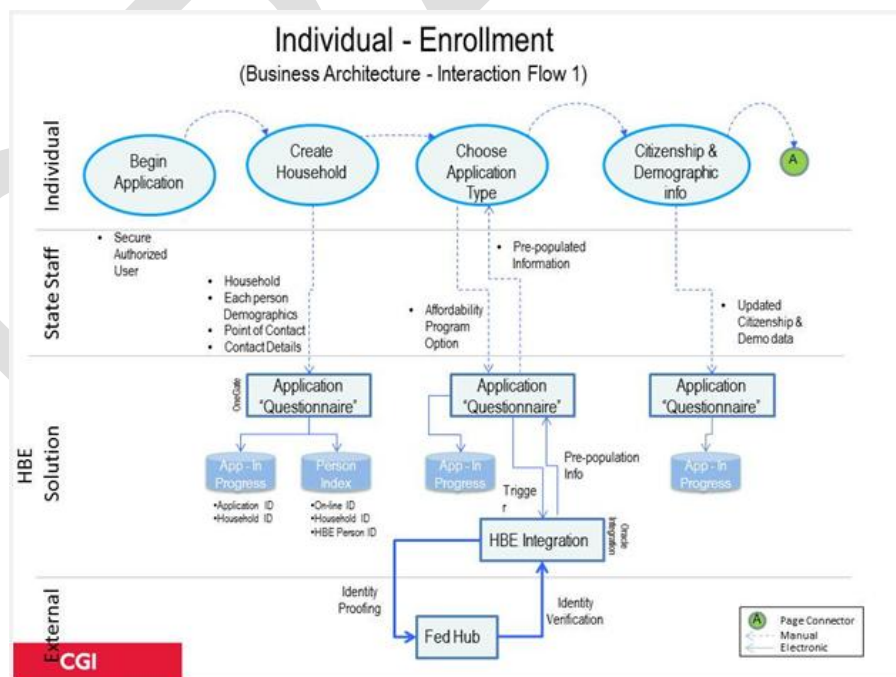


Exhibit 33: Individual Enrollment (Business Architecture – Flow 1)

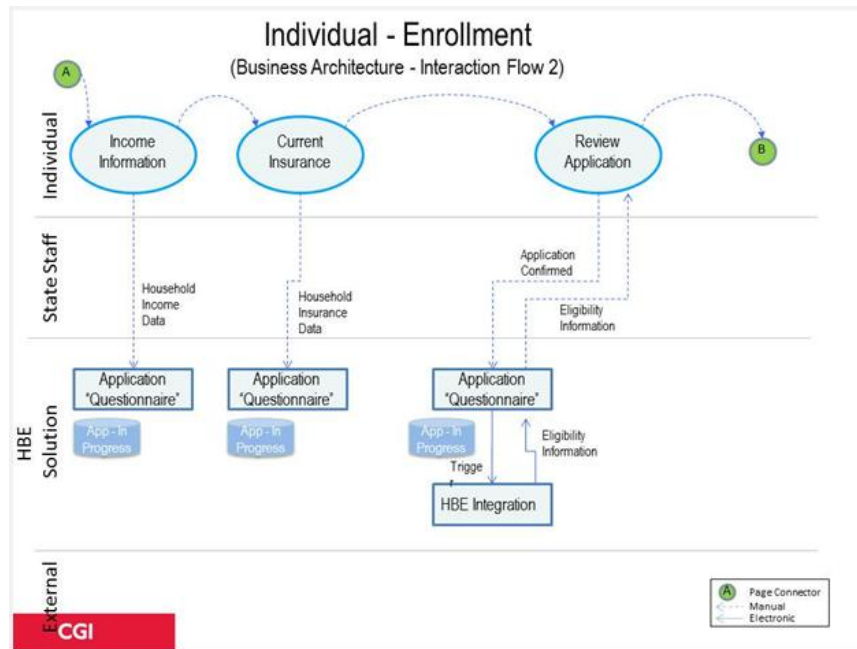


Exhibit 34: Individual Enrollment (Business Architecture – Flow 2)

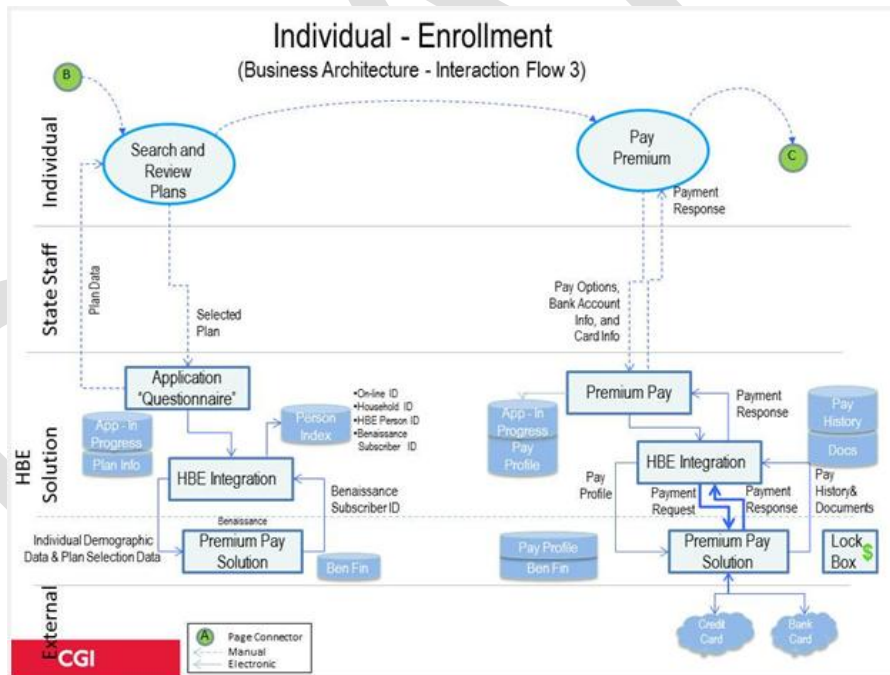


Exhibit 35: Individual Enrollment (Business Architecture – Flow 3)

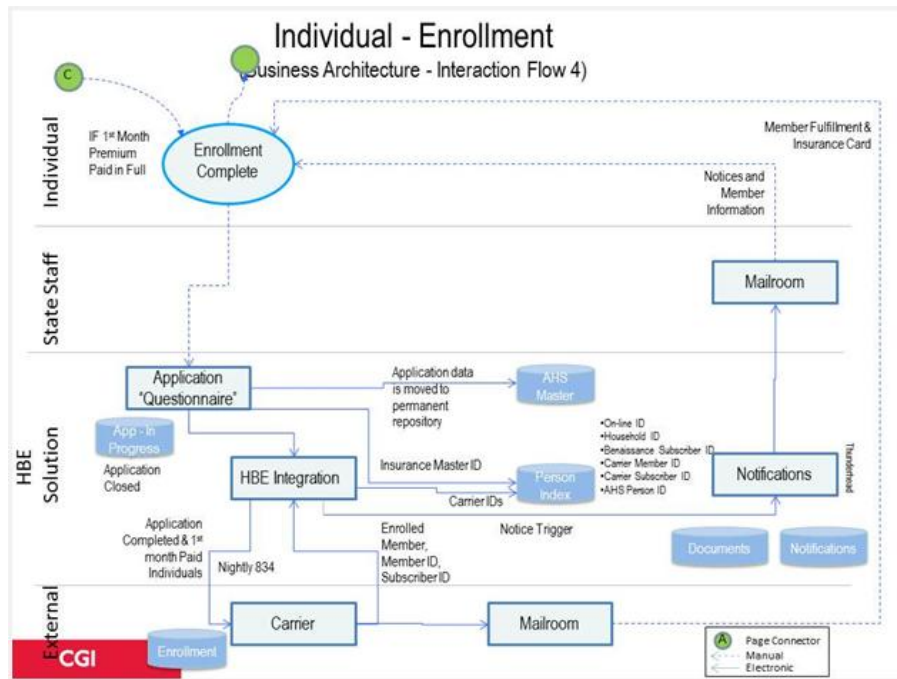


Exhibit 36: Individual Enrollment (Business Architecture – Flow 4)

13.5 Scenario 3: Individual - On-going Payments

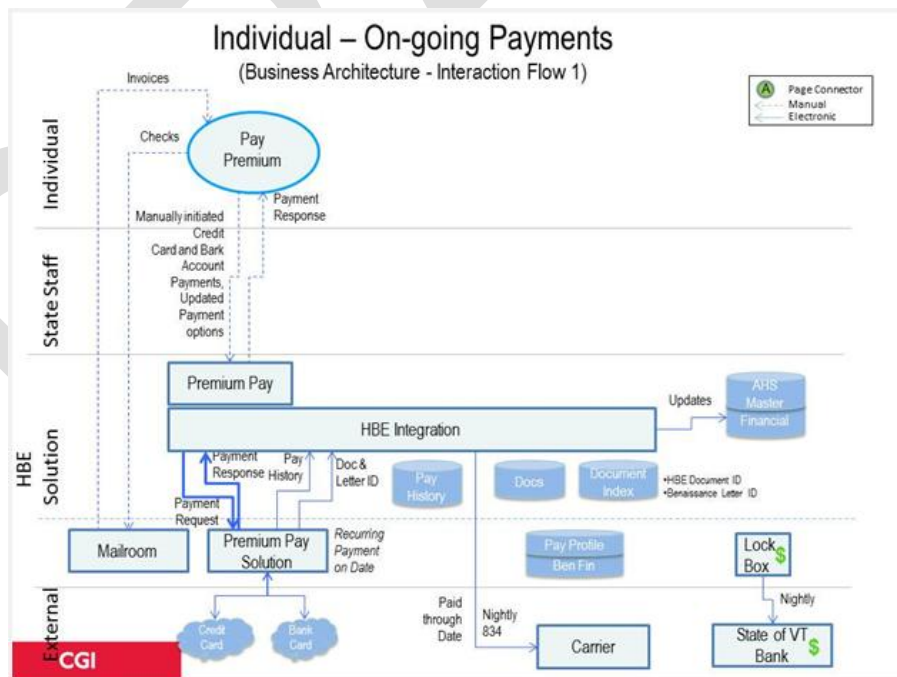


Exhibit 37: Individual On-going Payments (Business Architecture – Flow 1)

13.6 Scenario 4: Employer – Pre-Screening

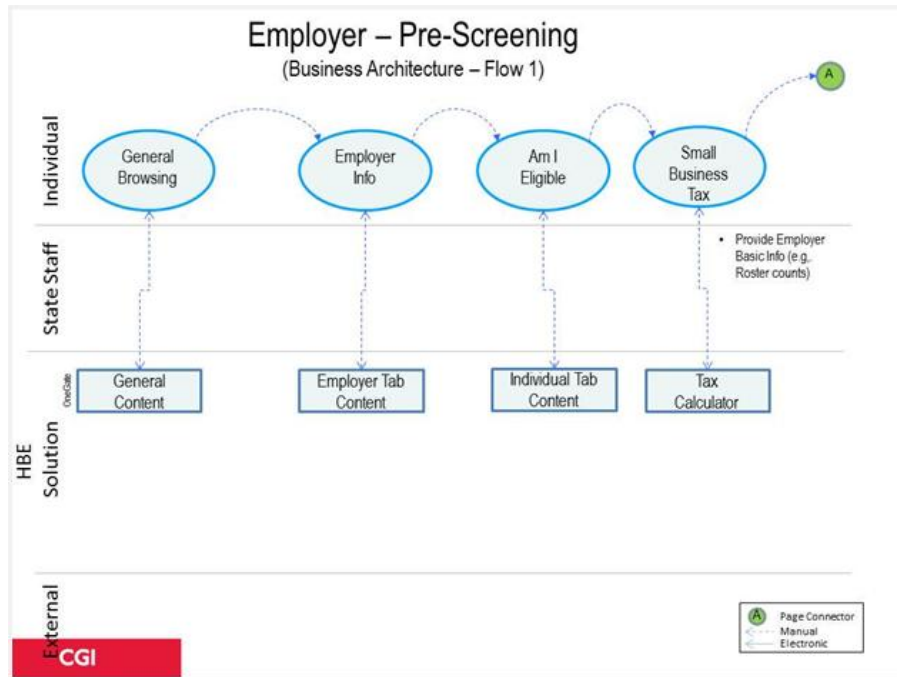


Exhibit 38: Employer – Pre-Screening (Business Architecture – Flow 1)



Exhibit 39: Employer – Pre-Screening (Business Architecture – Flow 2)

13.7 Scenario 5: Employer / Employee Enrollment – Employer Side

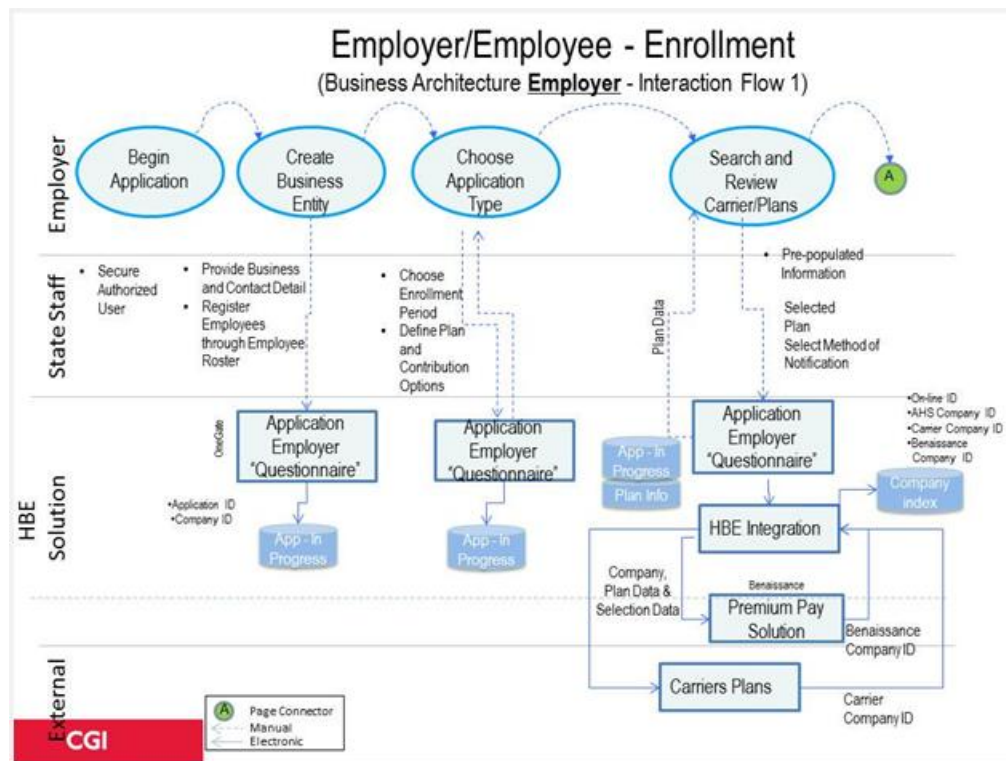


Exhibit 40: Employer/Employee Enrollment – (Business Architecture Employer – Flow 1)

13.8 Scenario 5: Employer / Employee Enrollment – Employee Side

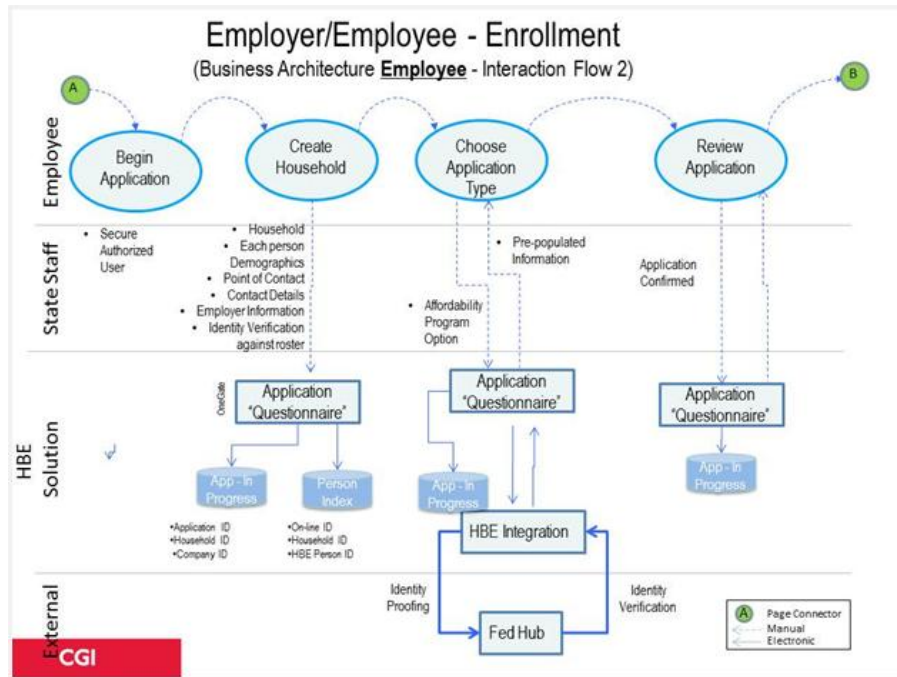


Exhibit 41: Employer/Employee Enrollment – (Business Architecture Employee – Flow 2)

13.9 Scenario 5: Employer / Employee Enrollment

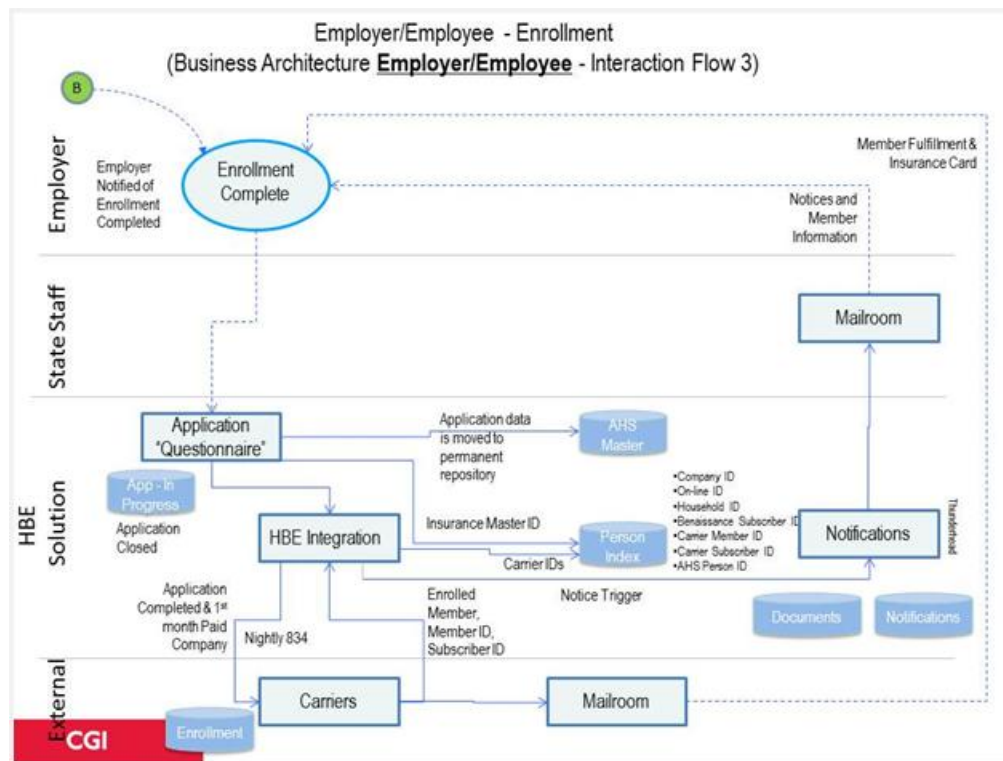


Exhibit 42: Employer/Employee Enrollment – (Business Architecture Employer/Employee – 3)

13.10 Scenario 6: Customer Support

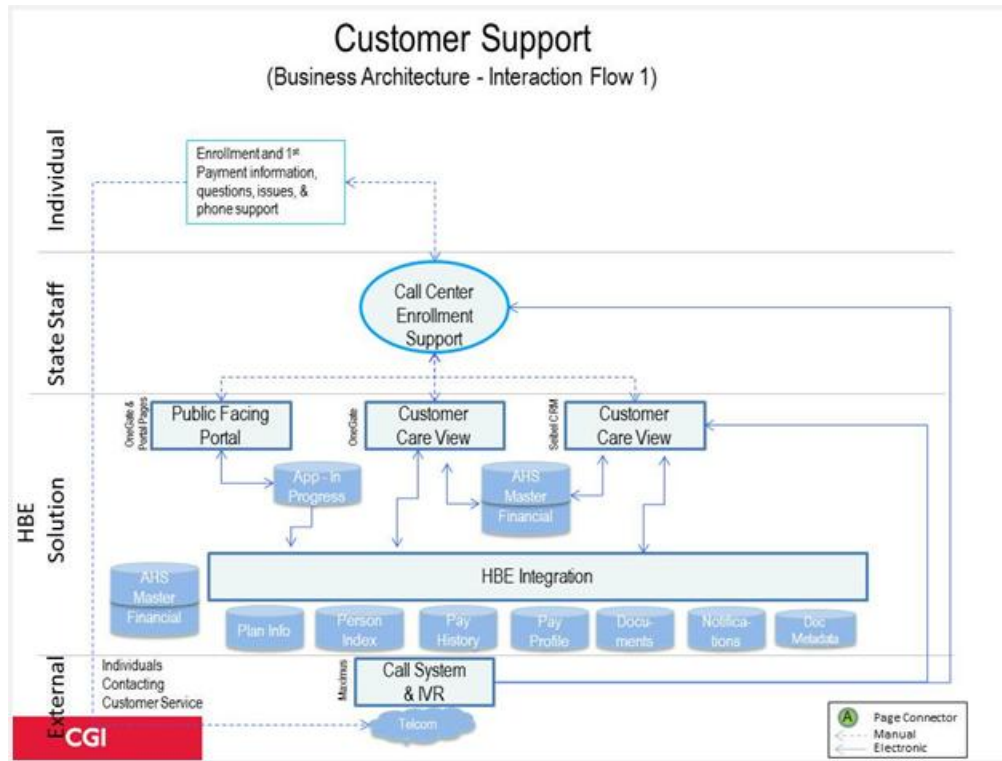


Exhibit 43: Customer Support – (Business Architecture Interaction Flow 1)

13.11 Scenario 7: Weekly Premium Processing

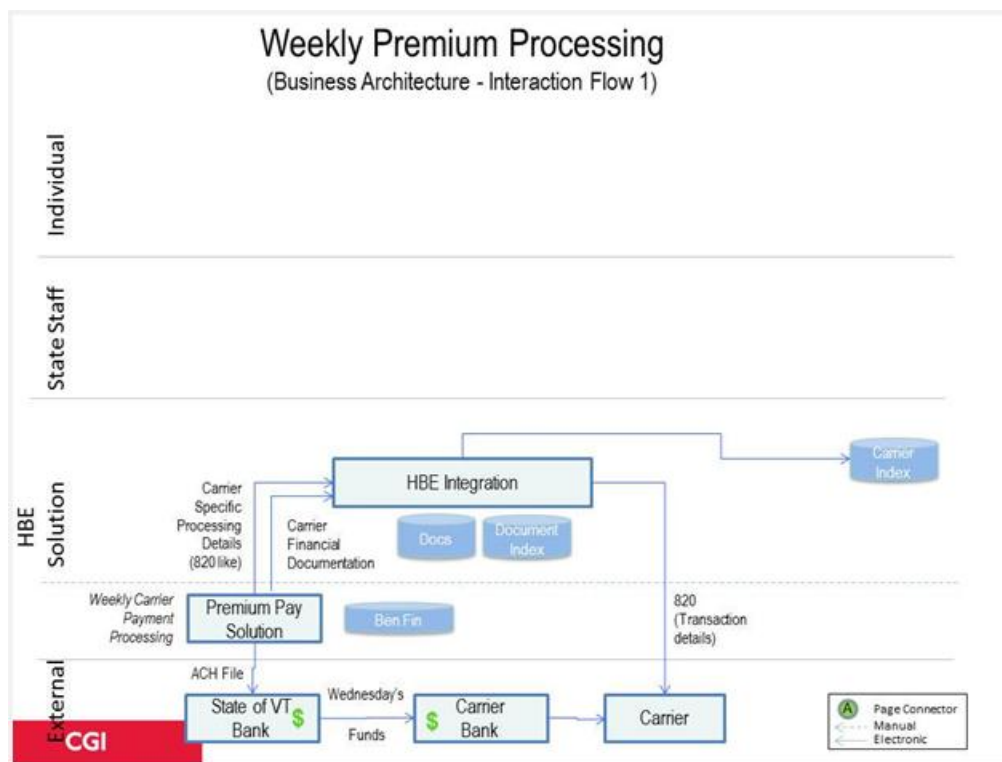


Exhibit 44: Weekly Premium Processing – (Business Architecture Interaction Flow 1)

13.12 Scenario 8: Monthly Premium Processing

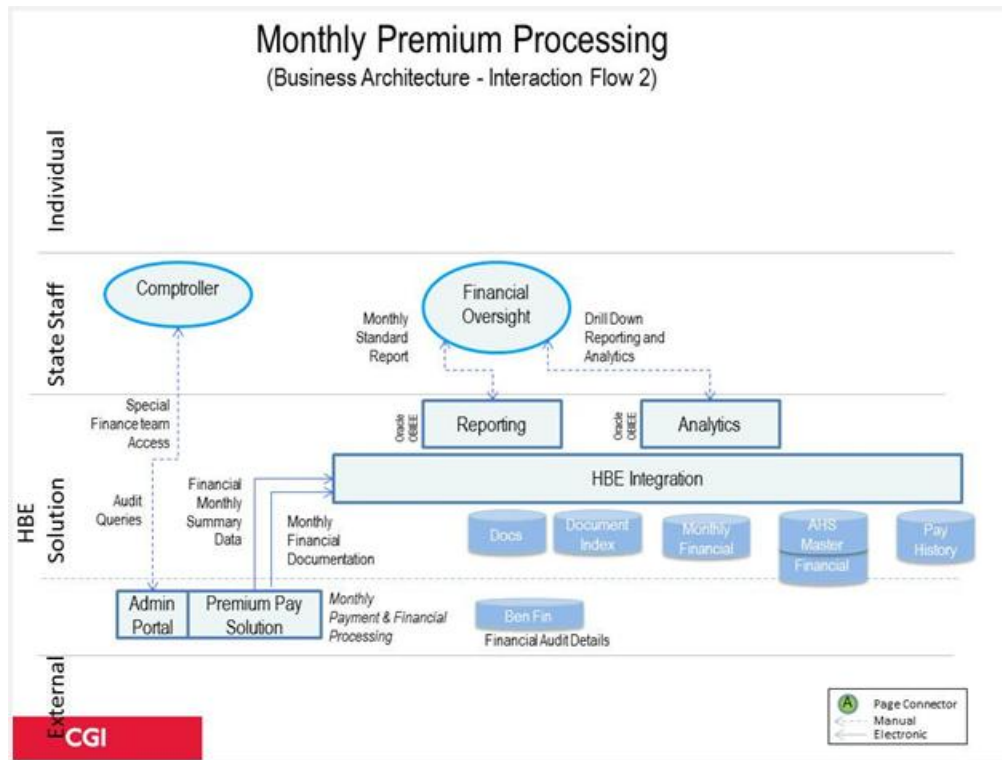


Exhibit 45: Monthly Premium Processing – (Business Architecture Interaction Flow 2)

13.13 Scenario 9: General Carrier Processing

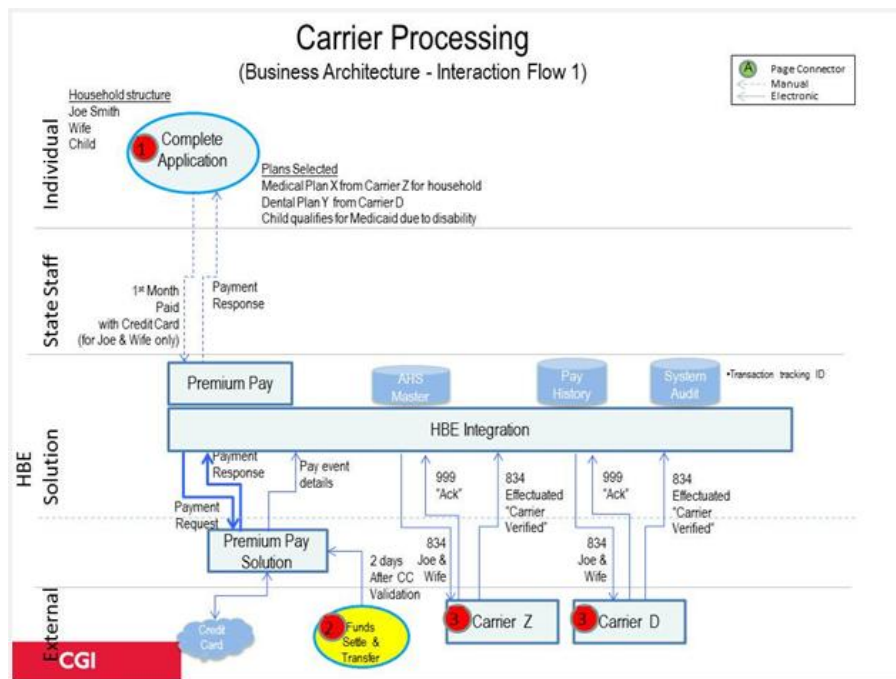


Exhibit 46: Carrier Processing – (Business Architecture Interaction Flow 1)

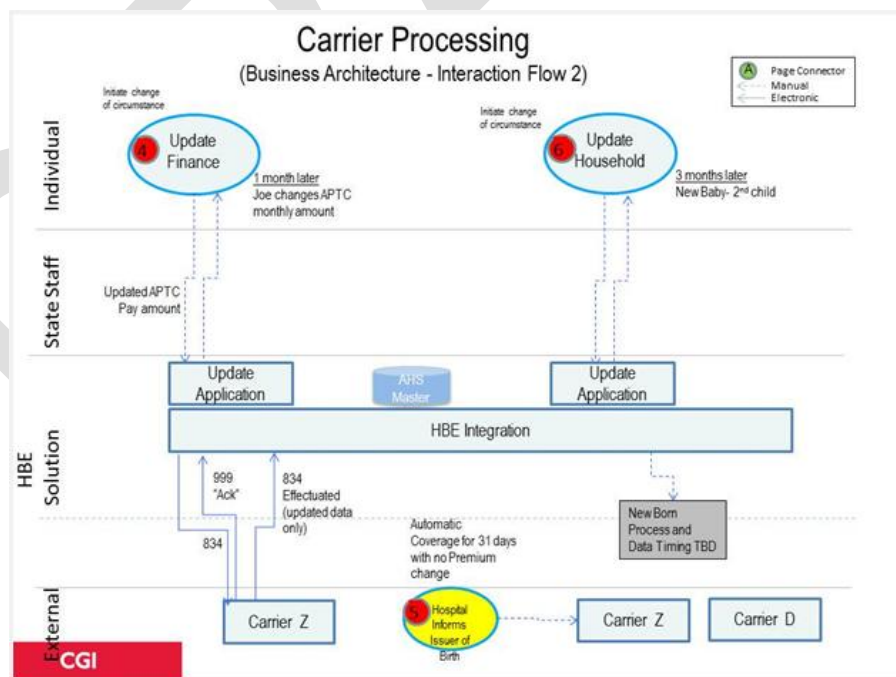


Exhibit 47: Carrier Processing – (Business Architecture Interaction Flow 2)

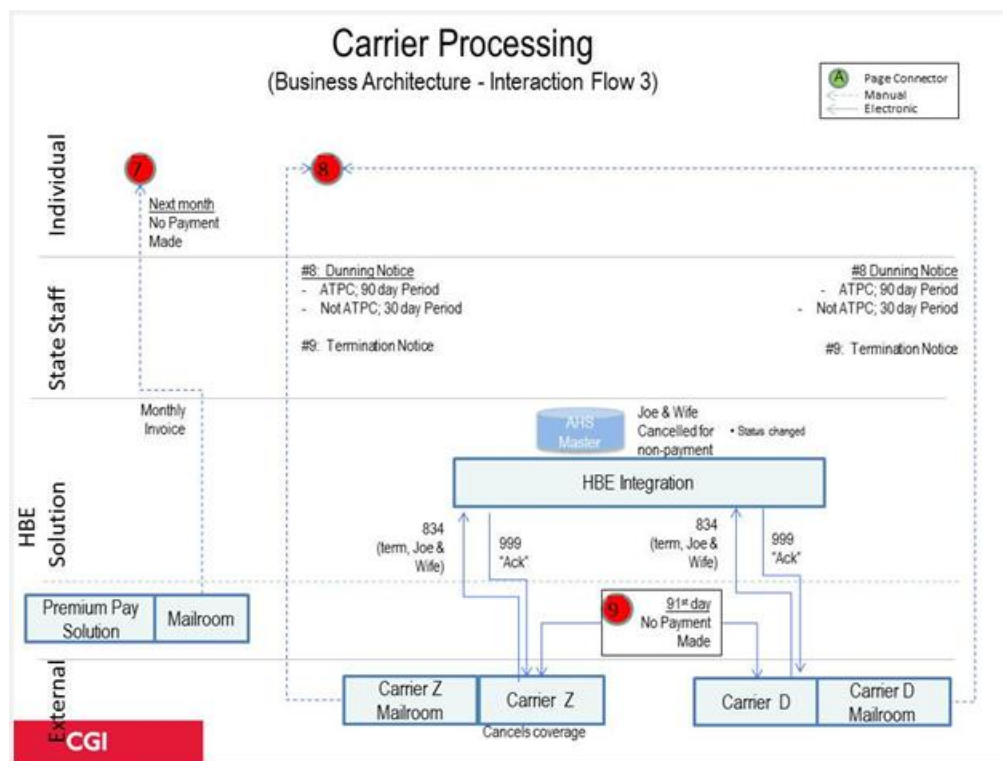


Exhibit 48: Carrier Processing – (Business Architecture Interaction Flow 3)

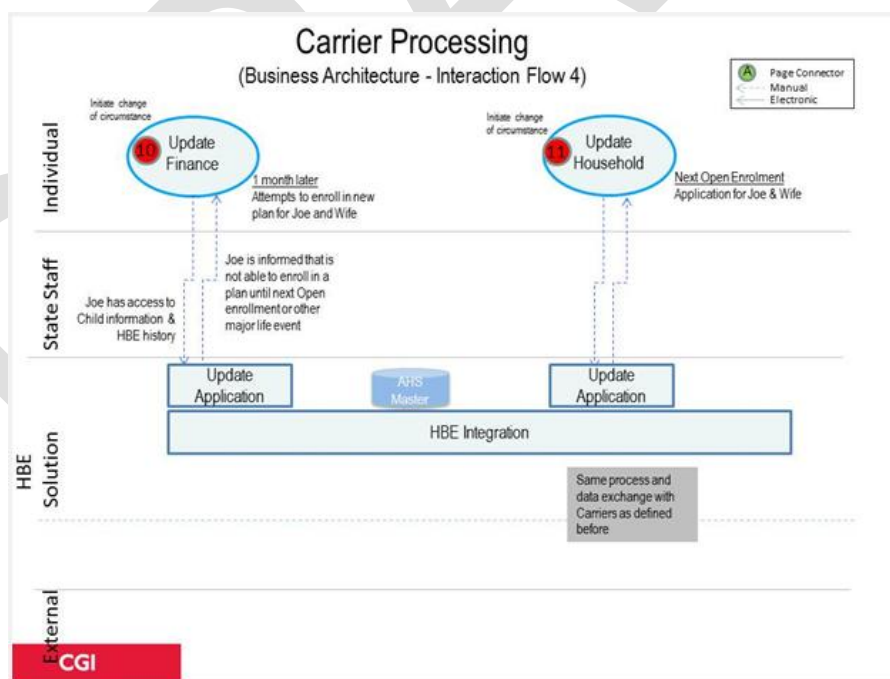


Exhibit 49: Carrier Processing – (Business Architecture Interaction Flow 4)

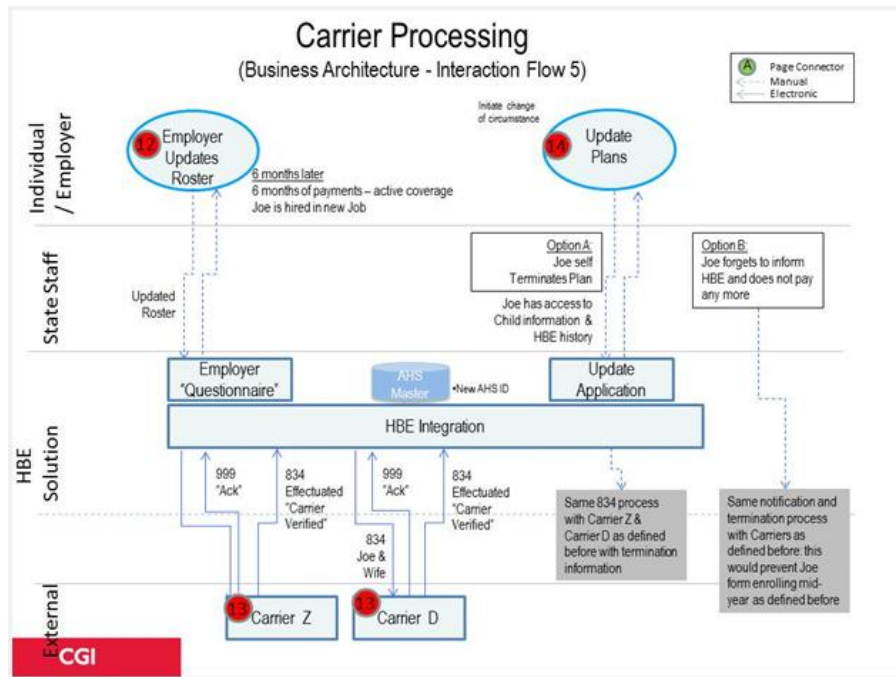


Exhibit 50: Carrier Processing – (Business Architecture Interaction Flow 5)

13.14 Scenario 10: Monthly Carrier Processing

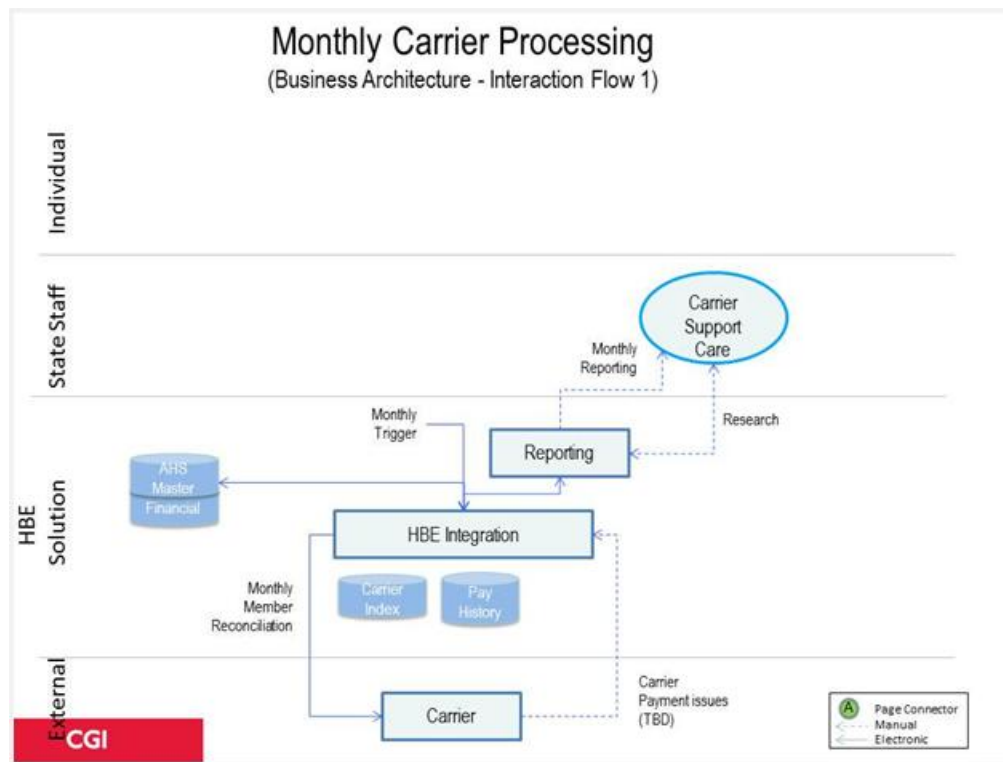


Exhibit 51: Monthly Carrier Processing – (Business Architecture Interaction Flow 1)

13.15 Scenario 11: Federal Hub Processing

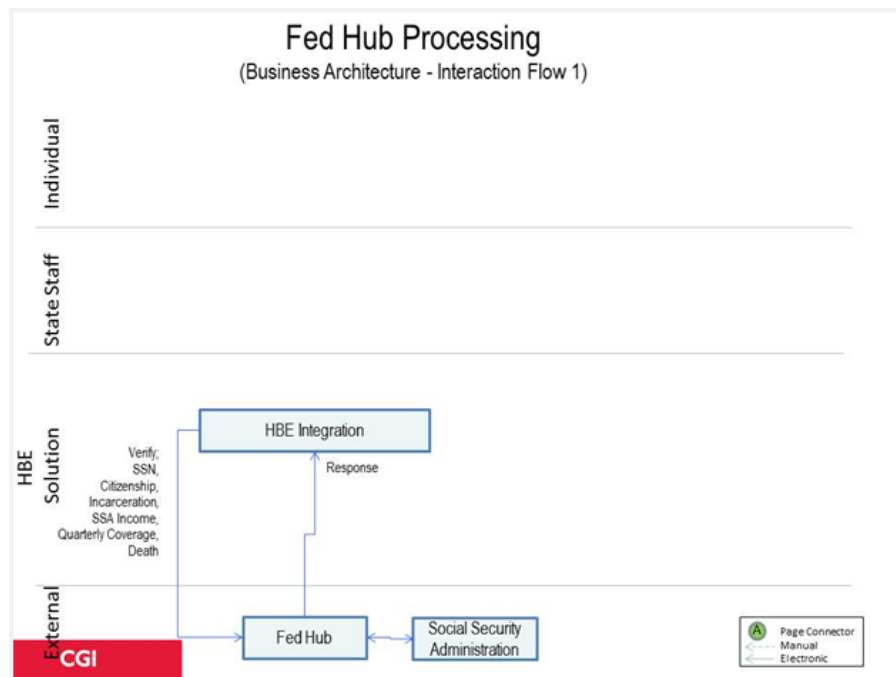


Exhibit 52: Fed Hub Processing – (Business Architecture Interaction Flow 1)

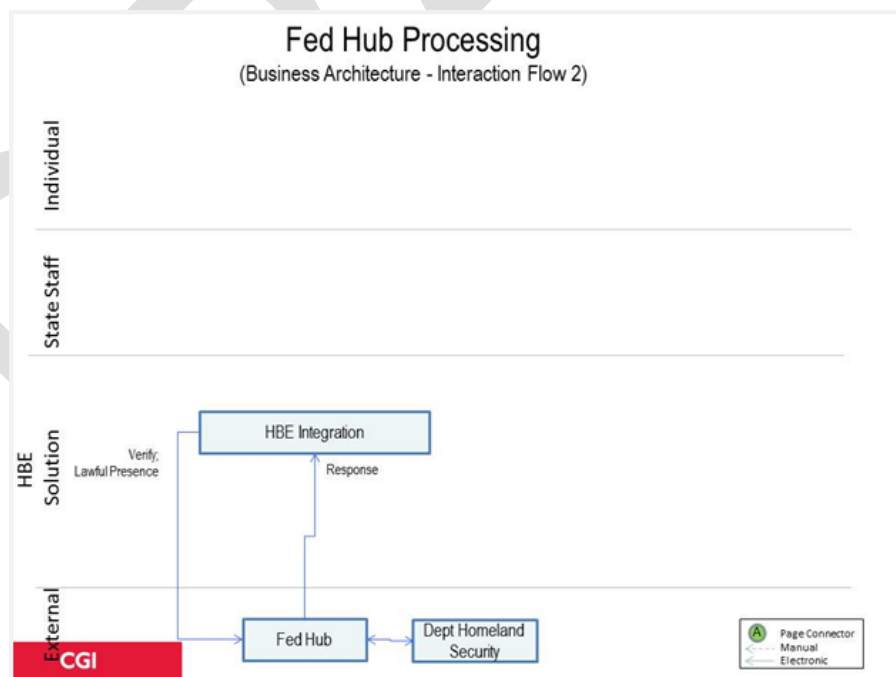


Exhibit 53: Fed Hub Processing – (Business Architecture Interaction Flow 2)

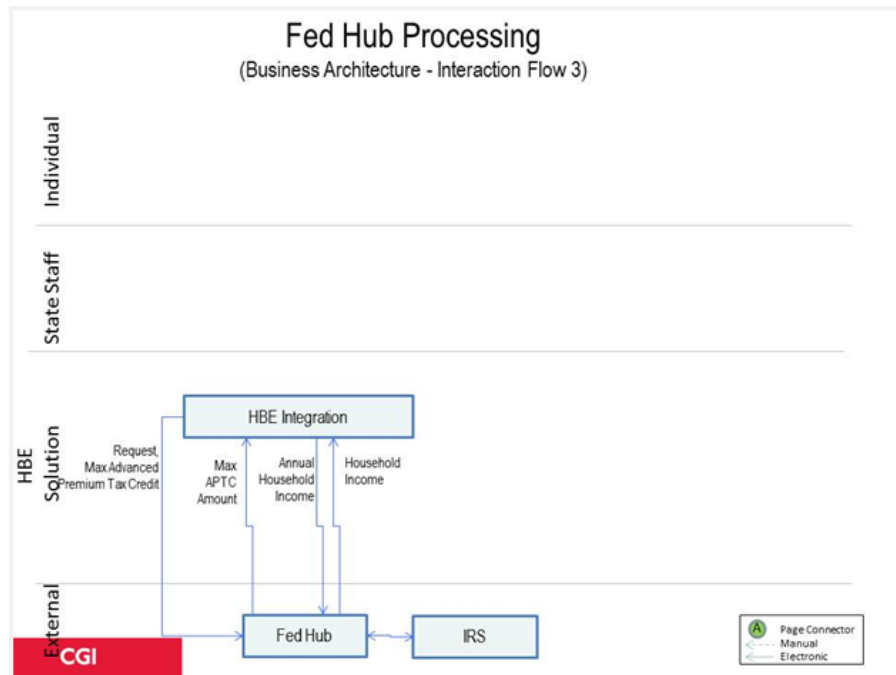


Exhibit 54: Fed Hub Processing – (Business Architecture Interaction Flow 3)

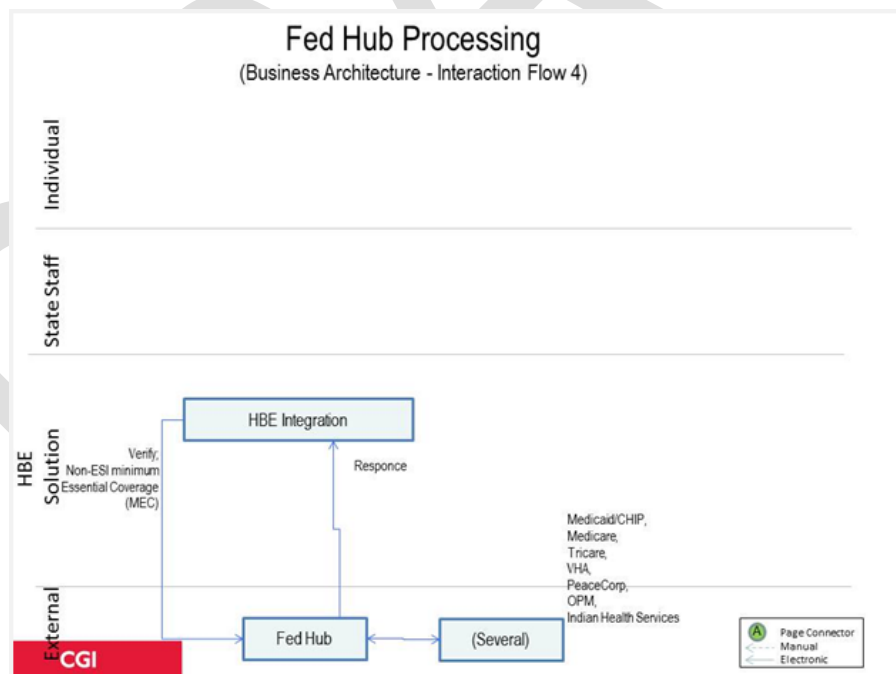


Exhibit 55: Fed Hub Processing – (Business Architecture Interaction Flow 4)

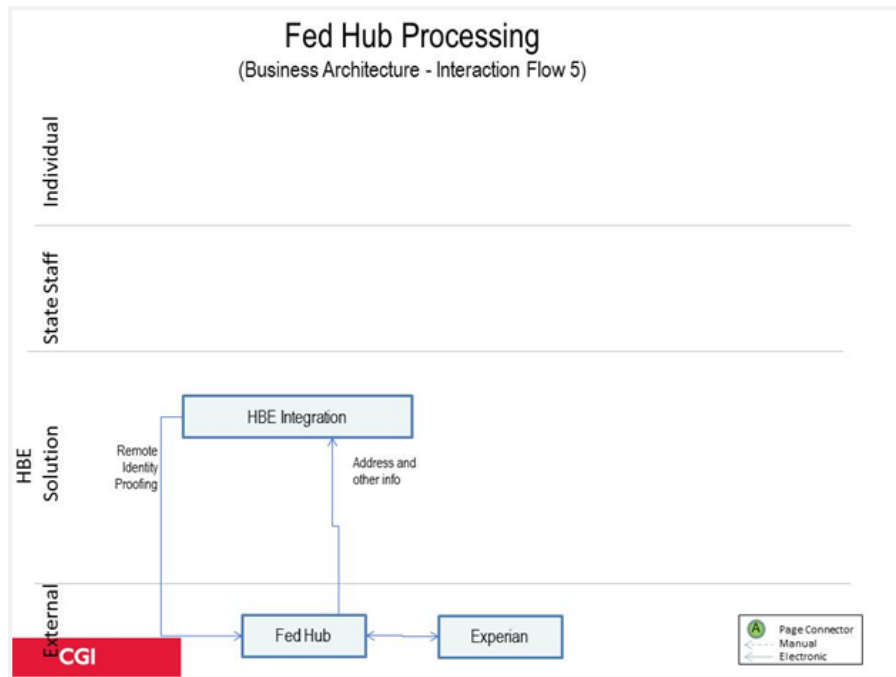


Exhibit 56: Fed Hub Processing – (Business Architecture Interaction Flow 5)

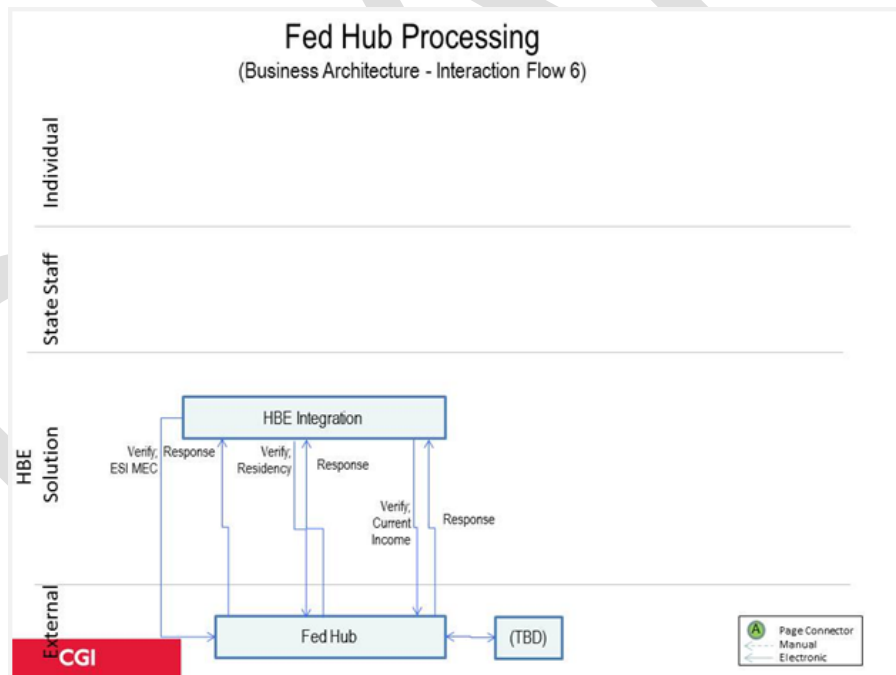


Exhibit 57: Fed Hub Processing – (Business Architecture Interaction Flow 6)

13.16 Scenario 12: Plan Management

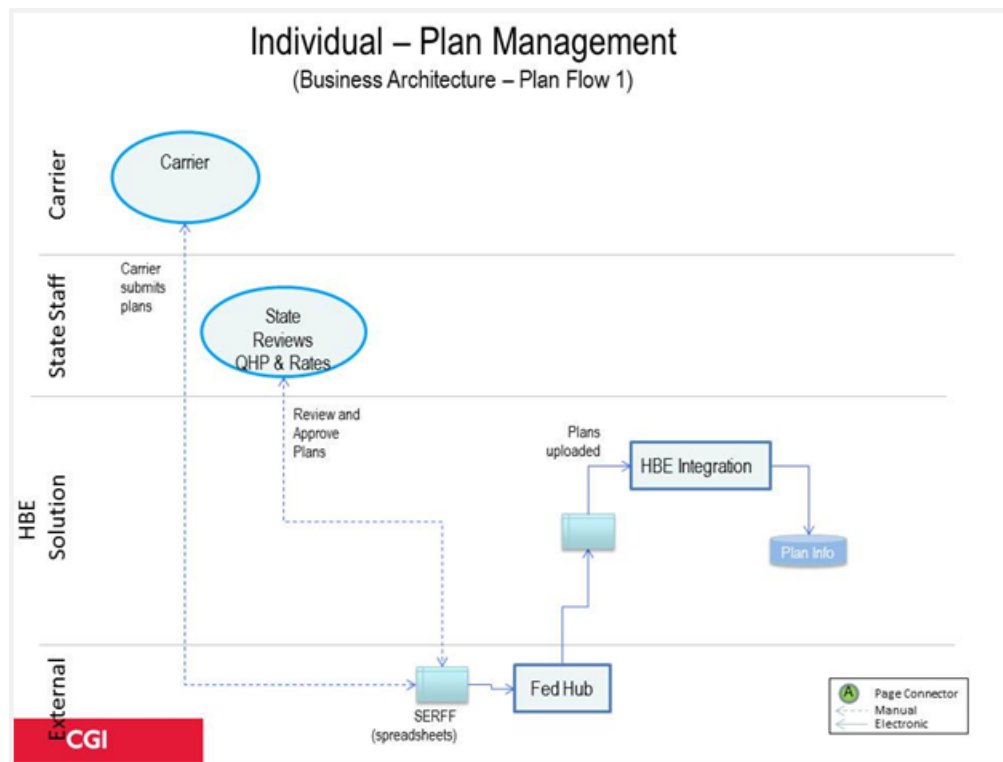


Exhibit 58: Individual Plan Management – (Business Architecture Flow 1)

13.17 Scenario 13: Administrative – End User Security

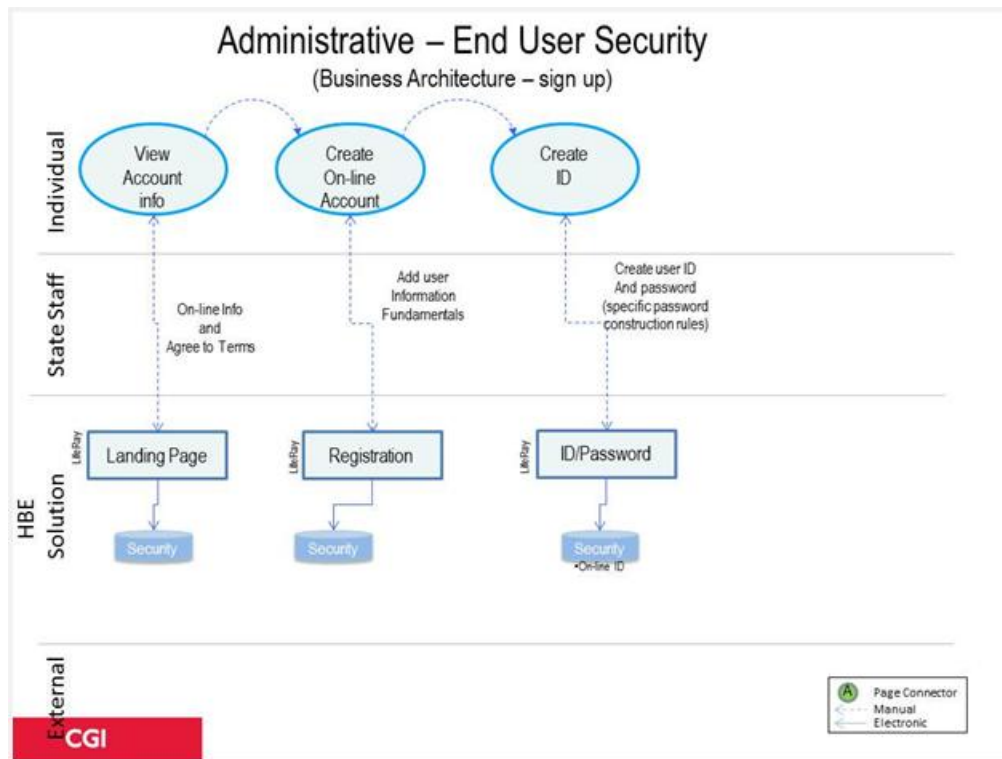


Exhibit 59: Administrative – End User Security – (Business Architecture Sign Up)

13.18 Scenario 14: Reporting

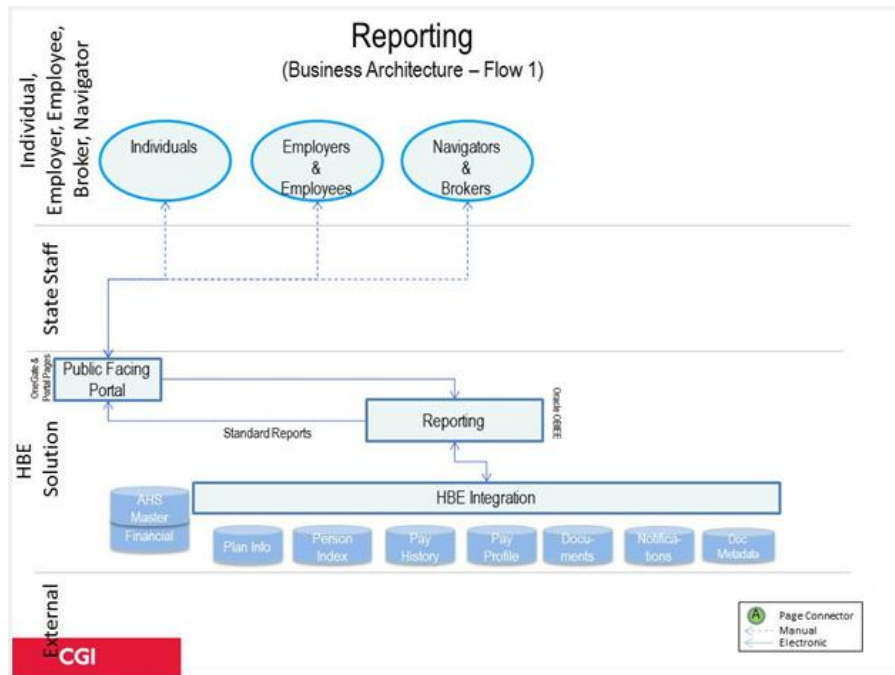


Exhibit 60: Reporting – (Business Architecture Flow 1)

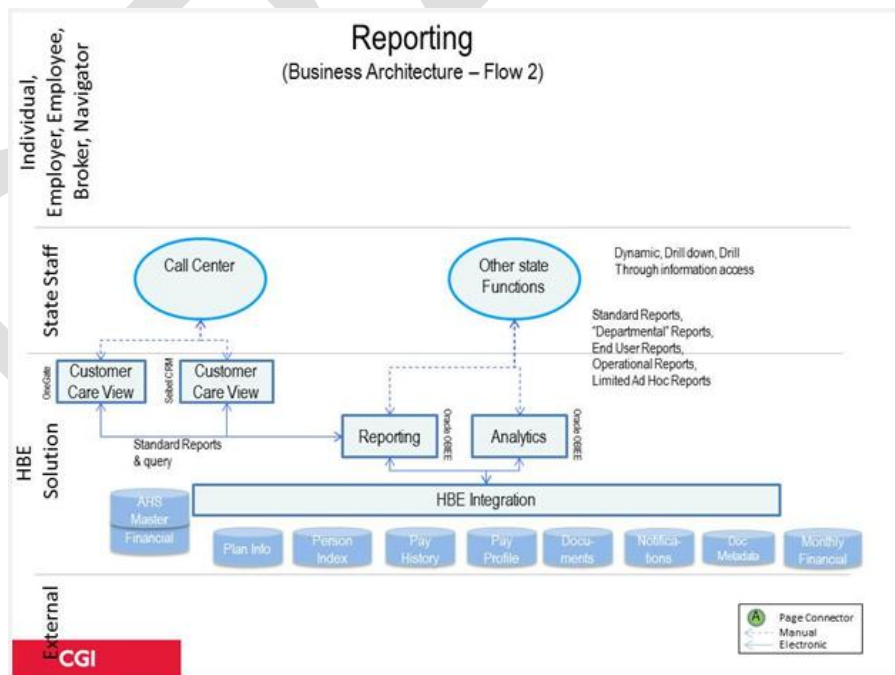


Exhibit 61: Reporting – (Business Architecture Flow 2)

13.19 Scenario 15: Notice Processing

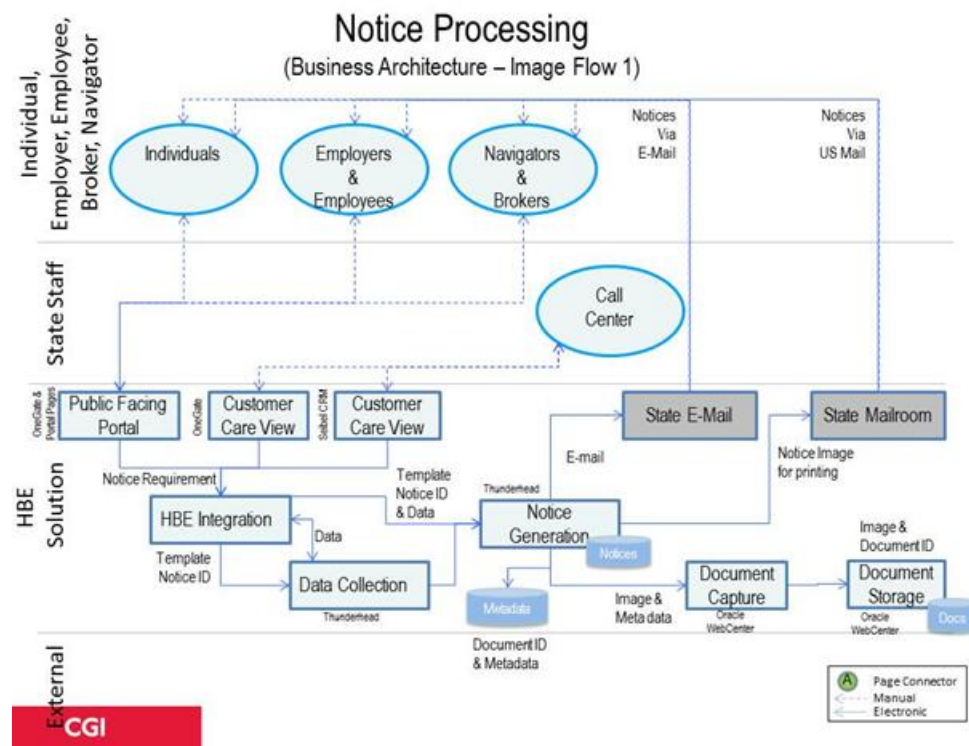


Exhibit 62: Notice Processing – (Business Architecture Flow 1)

13.20 Scenario 16: On-line Documents and Notices

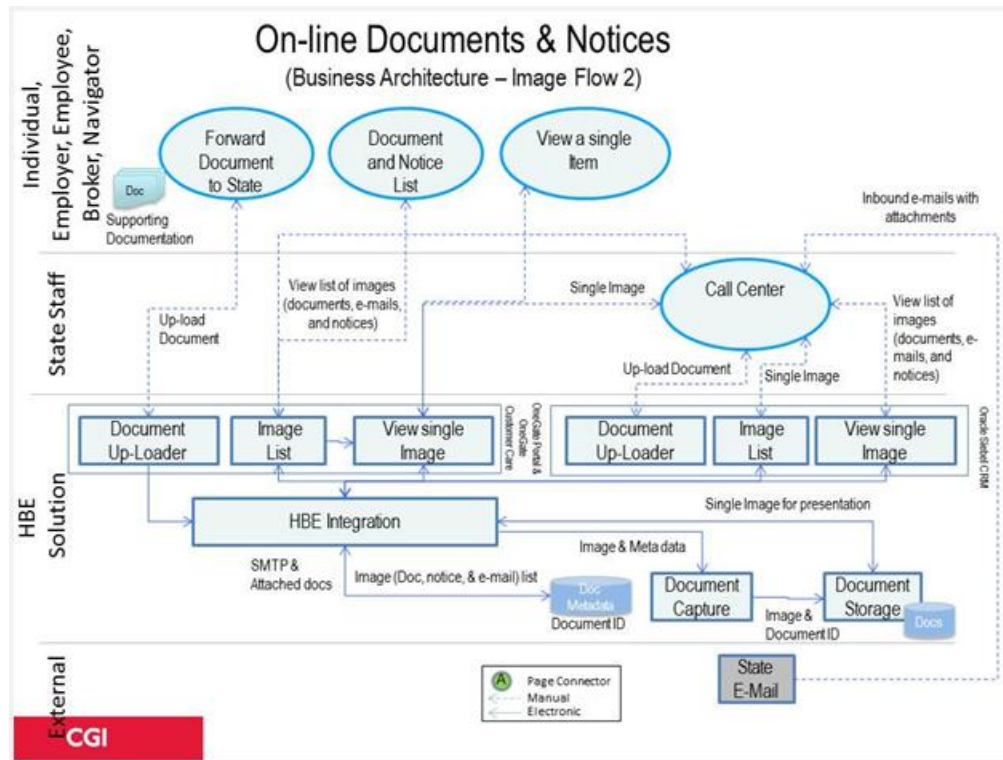


Exhibit 63: Online Documents and Notices – (Business Architecture Flow 2)

13.21 Scenario 17: Physical Document Capture

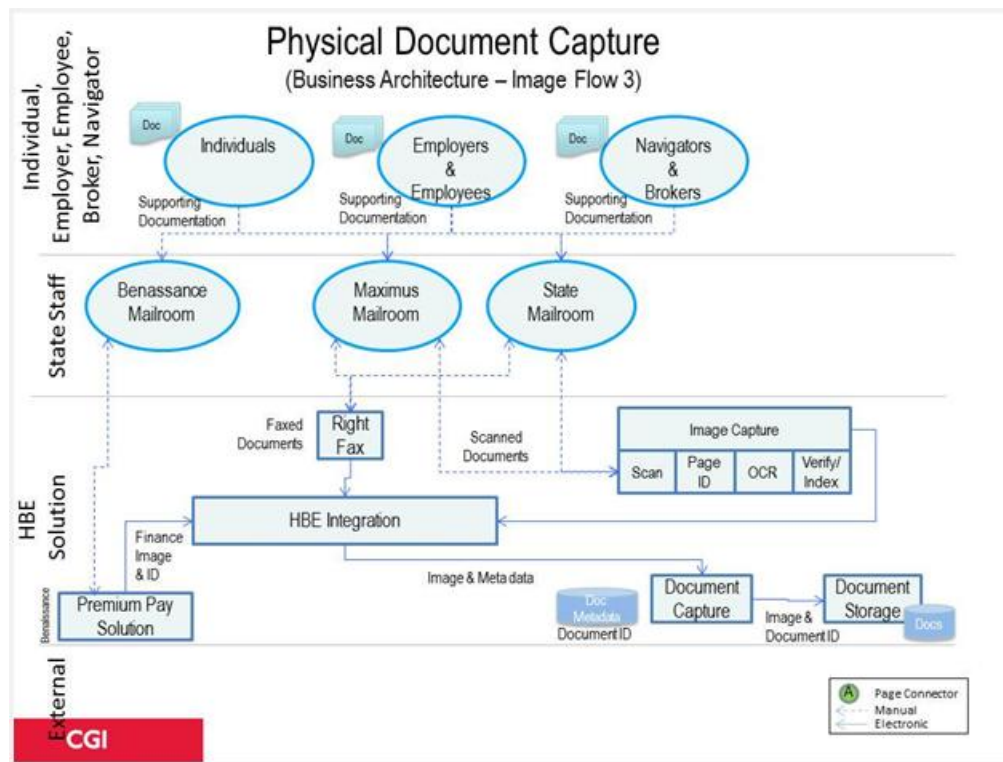


Exhibit 64: Physical Document Capture – (Business Architecture Flow 3)

14 Detailed Design

The following sections provide the detailed designs for the VT HBE solution.

14.1 Hardware Detailed Design

The VT HBE will be hosted the in CGI Federal Cloud. The following section will provide the detailed design for the VT HBE environments. As the system is currently being designed/configured, the following will focus on the detailed Hardware Design for the Development, Test, and Training environments and the Staging, Production, and DR environments will be addressed in the next version of this deliverable.

14.1.1 Development Environment

Exhibit 65: Development Environment

Virtual Machine	vCP U	Memory (GB)	Local Disk (GB)	SAN	Virtual Machine	vCPU	Memory (GB)
vtix1devweb01	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1devweb02	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1devweb03	4	8	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1devweb04	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1devweb05	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	Windows 2008 R2
vtix1devapp01	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp02	8	16	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp03	8	16	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp04	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp05	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp06	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp07	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp08	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp09	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp10	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp11	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp12	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp13	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp14	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devapp15	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	Windows 2008 R2
vtix1devapp16	2	4	40GB	(/u01 - 50GB)	(/u02 - 100GB)	1	
vtix1devapp17	4	12	40GB	(/u01 - 50GB)	(/u02 - 950GB)	1	
vtix1devdb01	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	

Virtual Machine	vCP U	Memory (GB)	Local Disk (GB)	SAN	Virtual Machine	vCPU	Memory (GB)
vtix1devdb02	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1devdb03	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	

14.1.2 Testing Environment

Exhibit 66: Testing Environment

Virtual Machine	vCP U	Memory (GB)	Local Disk (GB)	SAN	Virtual Machine	vCPU	Memory (GB)
vtix1tstweb01	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1tstweb02	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1tstweb03	4	8	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1tstweb04	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtix1tstweb05	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	Windows 2008 R2
vtix1tstapp01	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp02	8	16	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp03	8	16	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp04	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp05	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp06	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp07	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp08	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp09	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp10	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp11	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp12	4	8	80GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp13	4	8	80GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp14	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstapp 15	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	Windows 2008 R2
vtix1tstdb01	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstdb02	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtix1tstdb03	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	

14.1.3 Training Environment

Exhibit 67: Training Environment

Virtual Machine	vCP U	Memory (GB)	Local Disk (GB)	SAN	Virtual Machine	vCPU	Memory (GB)
vtfix1trnweb01	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtfix1trnweb02	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtfix1trnweb03	4	8	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtfix1trnweb04	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	
vtfix1trnweb05	2	4	40GB	(/u01 - 50GB)	(/u02 - 30GB)	1	Windows 2008 R2
vtfix1trnapp01	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp02	8	16	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp03	8	16	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp04	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp05	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp04	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp05	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp06	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp07	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp08	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp09	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp10	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp11	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp12	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp13	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp14	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trnapp15	2	4	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trndb01	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trndb02	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trndb03	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trndb02	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	
vtfix1trndb03	12	32	40GB	(/u01 - 50GB)	(/u02 - 50GB)	1	

14.1.4 Client Backup /Recovery Requirements (by host):

Exhibit 68: Client Backup / Recovery Requirements (by host)

Host	Type	Schedule	Comments
All Hosts (excluding VMware Host)	Incremental Backup	Daily	Daily incremental all Hosts DB Host daily to include exports from DB as a file on local storage of Host.
	Full Backup	Weekly	Weekly Full all Host DB Host weekly to include a full export from DB as a file on local storage of DB Host. 30-day retention for these backups

14.1.5 All Network Devices to be Configured

Exhibit 69: All Network Devices to be Configured

Site	Function	Make/Model/OS if to be added	Name (if exists)	Comments
PDC	Firewall	Fortinet (cloud)		VDOM config
SDC	Firewall	Fortinet (cloud)		VDOM config
VT #1 - Montpelier	Firewall	Fortinet 80C		NEW Setup
VT #2 - Burlingame	Firewall	Fortinet 80C		NEW Setup
Midlands	Firewall	Fortinet 80C		NEW Setup
Lenexa	Firewall	Fortinet 80C		NEW Setup

14.1.6 Site Information

Exhibit 70: Site Information

Site Name	Area Code/Prefix (NPA/NXX)	Address of Demarcation Point	Site Contact Name	Site Contact Telephone Number	Site Contact E-mail Address
PDC	480-496	10007 South 51st Street Phoenix, AZ 85044	TBD	TBD	TBD
SunGard	215-351	1500 Spring Garden Philadelphia, PA 19130	TBD	TBD	TBD
VT #1	802-223	1 National Life Drive, Montpelier, VT 05604	TBD	TBD	TBD
VT #2	802-862	21 Gregory Drive, Suite 165, South Burlington, VT 05403	TBD	TBD	TBD
Midlands	402-339	11425 South 84th Street Papillion, NE 68046	TBD	TBD	TBD
Lenexa	913-410	14500 West 105th Street Lenexa, KS 66215	TBD	TBD	TBD

14.1.7 MPLS Circuit End Points (include both circuits if redundant)

Exhibit 71: MPLS Circuit End Points

Site Name	Bandwidth	Circuit	With or Without WAN Encryption of Traffic?	Site Name
PDC	10 Mbps	DS3		
SunGard	10 Mbps	DS3		
VT #1	10 Mbps	DS3		
VT #2	10 Mbps	DS3		
Midlands	3 Mbps			
Lenexa	3 Mbps			

14.1.8 Physical Server and Virtual Machine VLAN Assignment

Exhibit 72: Physical Server and Virtual Machine VLAN Assignment

Site	Server Name (if using a hypervisor, list VMs underneath)	Physical Switch Port Count	Virtual Switch Port Count	Access or Trunk Port	VLAN Name (if exists) or VLAN Function
PDC	PHX-CUS-ESX01	2		Trunk	Prod Web Prod App
		1		Trunk	TSM/NAS PVLAN
	PHX-CUS-WEBVM		2	Access	Prod Web
			1	Access	TSM/NAS PVLAN
	PHX-CUS-APPVM		2	Access	Prod App
			1	Access	TSM/NAS PVLAN
PDC	PHX-CUS-DB01	2		Access	Prod DB
		1		Access	TSM/NAS PVLAN

14.1.9 VMware Host Management Firewall requirements VMware Management

The VMware host management and firewall requirements will be provided in the *VT HBE Solution Install Guide* at the time of completion.

14.2 Software, Security, Performance, Internal Communication, and System Integrity Controls Detailed Design

As the system is currently being designed/configured, these sections will be addressed in a future version of this deliverable.

15 External Interfaces

The following are the anticipated types of users accessing the Vermont Health Benefit Exchange Portal, requiring different types of access:

- General Public
- Consumer
- Employer
- Broker
- Navigator
- Customer Service
- State Staff
- Operational Support

The VT HBE must integrate effectively with various external solution partners. The VT HBE is based on an SOA foundation that provides the ability to integrate with its partners through open standards-based implementation. Access to the VT HBE Portals will be provided by front-end Web servers.

The framework for this integration sits on top of the Oracle ESB and provides a set of configurable components, including adapters and integration services that manage protocol, transport, security, logging, audit, monitoring, and other integration services.

The framework provides transactions as Web services that can be used to share business functions with partner systems to perform activities such as eligibility determinations from the following systems: DHS Eligibility, Federal Exchange Eligibility Service, Federal Data Hub, Exchange Accounting System, and other state agencies and issuer systems.

In addition, the VT HBE must integrate with a number of insurance companies to exchange plan and enrollment details. The VT HBE processing framework includes multi-level validations, integrated reconciliation, alerts and notifications, and administrative components directly within the solution that support staff with direct access to interface data to support monitoring, analysis, and error resolution functions.

16 Glossary

The following is a list of terms and their definitions introduced in this document.

Exhibit 73: Glossary

Term	Definition
access management	The management of end user access to the environments.
Actuate Report Server	The software that is installed on a Windows Server in accordance with the Certified Configuration for Siebel CRM Programs for reporting and printing purposes.
Administrative Services Only (ASO)	An arrangement in which an employer hires a third party to deliver employee benefit administrative services to the employer. These services typically include health claims processing and billing. The employer bears the risk for health care expenses under an ASO plan.
administrative user	An end user assigned by a client to, identify the end users permitted to use certain components of the hosted environment and, to assign one or more responsibilities to each end user.
administration service	Application Management Services delivered by hosting provider under a defined deployment model.
after-action review	A meeting held between the hosting provider and the customer after Production Go-Live of a migration or Transition to Hosting Services for the purpose of assessing the success of the project and any outstanding issues.
anticipated peak workload	The target or goal workload for the hosting environment during testing.
application administrator	The role assigned to an end user who assumes the responsibility for performing as a technical lead administrator.
Application Management Services	Services performed by the hosting provider to manage, monitor, and administer the programs within the client's environments.

Term	Definition
application tier	The server that resides in a middle-tier, between the desktop clients and the database tier. Desktop clients send their requests to a server in the application tier, which processes the request or sends it to another server, such as the database server. (Web Server, Forms Server, Concurrent Processing Server, Reports Server, Admin Server, etc.).
approved third-party software	Software separately acquired by the hosting provider or the customer that adheres to hosting provider's integrations and operational standards.
architecture design document	A document prepared by the hosting provider that specifies the customer's hosted architecture (Physical and Logical) at the commencement of hosting services.
Authorized Network Provider (ANP)	A network provider approved by the client that the hosting provider has retained for the purpose of providing connectivity for the hosting services in accordance with service level standards.
back out plan	A list of steps, and the roles or individuals responsible for performing such steps that are required to reverse changes that had been applied to a client's production and non-production environments.
balance billing	When a provider bills you for the difference between the provider's charge and the allowed amount. For example, if the provider's charge is \$100 and the allowed amount is \$70, the provider may bill you for the remaining \$30. A preferred provider may not balance bill you for covered services.
base configuration	The standard amount of server, storage, networking, firewall, and load balancing provided for the client's environment.
base products	Unaltered software components, such as executable programs and compiled libraries.
Batch Management software	Software to enable the hosting provider to schedule, monitor, and manage batch workloads in the client's environment. An example of batch management software is Concurrent Manager.
break-fix	A code change designed to restore, to its pre-change state, the logic or functionality of a CEMLI that had been affected by a change to an environment.
Business Intelligence Technology and Application Program	A program identified by a Business Intelligence application or a Business Intelligence technology program.
capacity management	The process of planning, analyzing, and sizing storage and transaction processing capability to enable the Production Environment to handle data processing demand.
Centers for Medicare and Medicaid Services (CMS)	CMS is a Federal agency, which is a federal agency within the United States Department of Health and Human Services (DHHS) that administers the Medicare program and works in partnership with state governments to administer Medicaid, the State Children's Health Insurance Program (SCHIP), and health insurance portability standards.
certified configuration	The combination of the configuration, instances, programs, and the operating system, as provided by hosting provider, that is compliant with hosting provider standards and policies.
certification	A decision to declare an issuer as an authorized health insurance provider in Vermont.

Term	Definition
change	A hosting provider - or client-initiated deployment of a specific addition, modification or removal, of a component, item, feature or function, to an environment. Examples of changes are the deployment of a release into the environment and a modification to the environment configuration.
change action plan	A plan that identifies the steps, and the roles or individuals responsible for performing such steps that are required to complete a specific change to an environment.
change management	The management and deployment of changes to an environment.
change request	A request by customer via Hosting Provider Change Management process for a change to an environment.
code refresh	The process of copying the full application code from a Source Environment to a target environment and making the required configuration changes within the application tier of the target environment.
computer and administration services	Application Management Services delivered by hosting provider deployment model.
Concurrent Manager	An example of Batch Management software.
Concurrent PeopleSoft Enterprise Users	The number of PeopleSoft Enterprise - Professional Application users, PeopleSoft Enterprise CRM Self Service Application users, PeopleSoft Enterprise Financials Self Service Application users, PeopleSoft Enterprise Human Resources Self Service Application users, PeopleSoft Enterprise Portal Self Service Application users, and PeopleSoft Enterprise Learning Solutions Self Service Application Users simultaneously logged into the Environment.
concurrent review	Concurrent review involves monitoring the medical treatment and progress toward recovery, once a patient is admitted to a hospital, to assure timely delivery of services and to confirm the necessity of continued inpatient care. This monitoring is under the direction of medical professionals. Concurrent review is a component of "Utilization Review."
configuration migration	The process of copying application metadata and artifacts from a Source Environment to a Target Environment and making the required configuration Changes within the Target Environment.
contract document	The contract signed by both Hosting Provider and Customer that is governed by the Agreement that outlines the Hosting Provider Programs and Services.
critical patch updates	Updates that are provided to Customer by Hosting Provider's Support Services organization as part of provider's technical support services and that are applied to the Environment as part of the Emergency Release Management process. Critical Patch Updates are designed to address significant security vulnerabilities and other issues that may relate to, or serve as prerequisites to, security issues, and may also include non-security fixes that are designed to address interdependency issues related to security patches.
custom services	Services performed by hosting provider.
data center	The physical location where the Environments for which Hosting Provider performs Hosting Provider Services reside.

Term	Definition
data center security policy	A document prepared and maintained by Hosting Provider that outlines access control requirements applicable to Hosting Provider's Data Center, including access requests, physical screening, on-site behavior and prohibited items.
database refresh	The process of copying a database from a Source Environment to a Target Environment and making the required configuration Changes within the database of the Target Environment.
decommission	The process defined by hosting provider under which Customer's use of Hosting Provider Environments is ended and the Hosting Provider Services are terminated.
decommission tape	The magnetic tapes provided by Hosting Provider as part of the Decommission of Computer and Administration Services that contain a copy of the production data from Customer's Production Environment.
dedicated	Isolated physical and virtual infrastructure for purpose of completely segregating Customer environments from other Hosting Provider tenants. Including firewall, load balancer, switch, router, server, storage.
default-deny	A network-oriented approach to access control that implicitly denies the transmission of all network traffic but then specifically allows only required network traffic based on protocol, port, source, and destination.
demilitarized zone	The "neutral zone" between the Internet and Hosting Provider's, or as applicable, a Customer's, private network.
demo and demo environment	Demo, and Demo Environment, means a Demonstration Environment.
demonstration environment	A type of Production Support Environment that is used for demonstration purposes.
Dev and Dev environment	A Development Environment.
development environment	A type of Non-Production Environment in which Customer or Customer Alternate performs development activities in support of Hosting Provider Services, such as the creation of customizations.
diagnostic server	A server enabled by Hosting Provider as part of Administration Services to remotely monitor the status and operation of Customer's Environment.
disaster	An Unplanned Outage that causes a complete loss of access to and use of the Hosting Provider Programs in the Production Environment at the Primary Site for a period greater than 24 hours.
disaster recovery	Services provided by Hosting Provider in accordance with the applicable Schedule to recover Production Environment data and to re-establish the Production Environment.
disaster recovery environment	The instance within the Secondary Site that mirrors Production in capacity, configuration in every way for the sole purpose of maintaining and operating Customers Production applications in the event of a disruption to the Hosting Providers services in Primary Site.
disaster recovery plan	A plan prepared and maintained by Hosting Provider that identifies tasks related to recovery and business continuity in the event of a Disaster.

Term	Definition
discharge planning	Medical personnel of a health plan working with the attending physician and hospital staff to assess alternatives to hospitalization, evaluate appropriate settings for care, and arrange for the discharge of a patient, including planning for subsequent care at home or in a skilled nursing facility. The goal is to determine when patients are ready to go home, and to provide a more comfortable, cost-efficient setting for continued treatment.
Data Loss Prevention (DLP)	A system that is designed to detect potential data breach incidents in timely manner and prevent them by monitoring data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
DMZ server	A public-facing application server or web server located in the Demilitarized Zone.
duty manager	The Hosting Provider personnel identified by Hosting Provider as Customer's point of contact for escalating Service Requests within Hosting Provider.
Electronic Medical Record	An EMR is a computerized medical record created in an organization that delivers care, such as a hospital or physician's office. Electronic medical records tend to be a part of a local stand-alone health information system that allows storage, retrieval and modification of records.
embedded software	Third-party software that is incorporated by hosting provider into certain hosting provider programs.
emergency release management	The process by which critical patch updates are applied to a client's environment.
end user	An individual who is authorized by the client to use the hosting provider programs within the environment.
enhanced recovery services	The Service under which hosting provider provides Disaster Recovery services – to meet Production RPO and RTO.
enterprise data warehouse/business intelligence	Refers to the entire set of enterprise data warehouse, business intelligence, and analytic capabilities.
enterprise governance	A hosting provider program identified by hosting provider as an enterprise governance, risk, and compliance program.
entitlement	The base level of services that are included as part of hosting provider's standard hosting provider services.
environment	The combination of Infrastructure and supporting software that is (i) configured for the hosting provider programs operating on it and for specific uses as part of the hosting provider services, and (ii) used by Hosting Provider to perform hosting provider services. For computer and administration services and administration services, the environment consists of the production environment, any production support environment(s) and any non-production environment(s).
environment plan	A document prepared and maintained by hosting provider that identifies the environments used during implementation of the hosting provider services and their respective purposes, such as development, CEMLI design and test, UAT, or staging purposes.
federal environment	A dedicated, caged hosting provider environment at the hosting provider's data center for United States Federal Government entity customers that purchase computer and administration services and hosting provider's federal security services.

Term	Definition
Federal Security Services	A service option applicable to Computer and Administration Services for United States Federal Government Customers, as described in the Federal Security Services Schedule.
full refresh	The process of copying of the database and full application code from a source environment to a target environment and making the required configuration changes within the database and application tier of the target environment.
functional service desk	Services under which hosting provider creates, receives, monitors, routes, and closes functional service desk service requests.
functional service desk service request	A request for assistance with the client's environment or any component thereof submitted to the functional service desk.
Go-Live	Refers to when a production system actually goes online "live."
Health Benefits Exchange (HBE)	Health Benefits Exchange (HBE) is the name given by the State of Vermont to the Vermont Health Insurance Exchange. Also known as the Health Insurance Exchange (HIX).
Health Insurance Exchange (HIX)	Health Insurance Exchange (HIX) is a set of state-regulated and standardized health care plans in the United States, from which individuals may purchase health insurance eligible for federal subsidies.
Health Insurance Portability and Accountability Act	Title I of the Health Insurance Portability and Accountability Act (HIPAA) protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
hosting provider	The line of business that delivers the Hosting Provider Services.
hosting provider application list	A document that lists all application programs covered by Hosting Provider services.
hosting provider continuous connection network	A dedicated network designed to support Network Connectivity between Hosting Provider and Customer's Environment, and that uses the following elements: a firewall, VPN, intrusion detection, authentication, reporting, and DNS.
hosting provider controlled environments	Those environments in which Hosting Provider has sole control to make Changes.
hosting provider controlled infrastructure	Infrastructure used for Administration Services that is managed and maintained solely by Hosting Provider.
hosting provider customer portal	The Customer-specific Internet based portal provided by Hosting Provider to Customer as part of the Hosting Provider Services by which Customer may view performance reports generated by Hosting Provider and the status of Service Requests.
hosting provider data center	The Data Center(s) retained and managed by Hosting Provider, or by a third party retained by Hosting Provider, at which Hosting Provider delivers Hosting Provider Services.
hosting provider data center badge access	An Hosting Provider form that must be completed by a person seeking to visit Hosting Provider's Data Center. Once completed by the visitor, the form is forwarded within Hosting Provider for review and approval purposes, and is retained by Hosting Provider in accordance with Hosting Provider policy.

Term	Definition
hosting provider internal support network	Hosting Provider Internal Support Network is comprised of a firewall, VPN, intrusion detection, authentication, reporting, and DNS. This isolated network is the standard Network Connectivity option for Hosting Provider personnel to connect to the Environment.
hosting provider product issue	An Incident associated with the functioning of Hosting Provider Program(s) (including program errors) but is not caused by Hosting Provider's performance of Hosting Provider Services.
hosting provider program	The Hosting Provider software product licensed to Customer separately and for which Hosting Provider Hosting Provider performs Hosting Provider Services. Hosting Provider Programs shall be deemed to mean all the Hosting Provider Programs identified for which Hosting Provider is providing Hosting Provider Services. Hosting Provider Programs may include Hosting E-Business Suite Programs, PeopleSoft Enterprise Programs, Siebel CRM Programs, Hosting Provider Technology Programs, Hosting Provider Hyperion Programs, Business Intelligence Technology and Applications Programs, Retail Programs, Agile Product Lifecycle Management Programs, Enterprise Governance, Risk, and Compliance Programs, User Productivity Kit Programs. The term Hosting Provider Program includes any Embedded Software within the applicable Hosting Provider Program.
hosting provider project plan	The document prepared by Hosting Provider that outlines the tasks to be performed by Hosting Provider, including anticipated start and end dates, for Transition Advisory Services.
hosting provider service desk	A team of resources provided by Hosting Provider Hosting Provider as part of Hosting Provider Services, under which Hosting Provider Hosting Provider creates, receives, monitors, routes, and closes Service Requests or Incidents, as described in the applicable Schedule.
hosting provider support	The Hosting Provider technical support organization (Hosting Provider Support Services) that provides product-related technical support services for Hosting Provider Programs.
hosting provider technology program	An Hosting Provider Program identified by Hosting Provider as a Technology Program. Hosting Provider performs Hosting Provider Services under an applicable agreement.
Intrusion Detection System (IDS)	A system that monitors the client's environment for security violations such as attack signatures, anomalous ports, and anomalous protocols being accessed.
implementer	A third-party vendor or software integrator retained by customer to provide implementation services to customer in support of hosting provider services. for the purpose of this definition, an implementer may be hosting provider's consulting line of business.
incident	Any event experienced by the client in its use of the hosting provider services for which a service request has been submitted, that is not consistent with the standard, documented operation of the hosting provider services, and which causes, or may cause, a service interruption.
individual patch	A software fix, created by hosting provider, to an hosting provider program and provided between patch set releases. Individual patches are designed to address specific software errors or vulnerabilities but not otherwise intended to change the functionality of programs.
information security incident response lead	The hosting provider employee assigned by hosting provider to lead hosting provider's response to severity 1 and severity 2 information security incidents.

Term	Definition
information security incident response plan	A document prepared by hosting provider that details activities that are to be performed in the event of an information security incident related to the applicable environment and hosting provider services. Hosting provider periodically updates the ISIRP document to reflect current information security Incident response planning.
information security incident response team	The Hosting Provider team that is designated by Hosting Provider to prepare for, and respond to, information security Incidents.
information security manager	An Hosting Provider employee designated by Hosting Provider to act as a liaison regarding security issues that affects the applicable Hosting Provider line of business. Each Hosting Provider line of business unit may have an Information Security Manager.
infrastructure	The combination of Hosting Provider's Data Center, hardware, servers, virtualization, operating system, storage, and networking equipment, used for the delivery of Hosting Provider Services.
infrastructure requirements	Information provided by the client in the Infrastructure Requirements Document regarding the Infrastructure for the Hosting Provider Services, such as capacity and usage information.
infrastructure requirements document	The document required by Hosting Provider in which Customer specifies its Infrastructure Requirements.
internet protocol security	A security framework based on open standards and designed to protect communications over Internet Protocol networks through the use of cryptography.
least privilege	A system-oriented approach to access control under which user permissions and system functionality are specifically evaluated and access is restricted to the resources required for users or systems to perform their respective duties.
maintenance code release	Any Release designed to address the manner in which hosting provider programs process data or operate, and neither contains new functionality nor changes the results of processing data. Examples of Maintenance Code Releases are Individual Patches, tool updates, tax updates, bug fixes, and maintenance packs. The term Maintenance Code Release specifically excludes any Service Pack or Upgrade.
maintenance window	Depending on the context, a Weekly Maintenance Window, a Semiannual Maintenance Window, or any other period of time scheduled by Hosting Provider for a Planned Outage within which Hosting Provider may perform maintenance activities on Infrastructure.
major maintenance window	The agreed to time when Hosting Provider can perform system maintenance/configuration changes on Production Environment that will reduce or make the Production Environment unavailable.
major release	An upgrade that is designated as follows: (i) for all Hosting Provider Programs by the identifying first number of the Upgrade (e.g., change from Application 9.x to Application 10.x), and (ii) for PeopleSoft Enterprise Programs, by the identifying first number of the Upgrade after the decimal place (e.g., change from version 9.1 to 9.2).
major upgrade	A major release.
management link	The type of Network Connectivity used for Administrations Services.

Term	Definition
Medicaid information technology architecture	A federal initiative of the United States Center for Medicaid & State Operations (CMSO) intended to foster integrated business and IT transformation across Medicaid, and to improve the administration of the Medicaid program in all states. MITA is a national framework intended to support improved systems development and health care management for the Medicaid enterprise.
Medicaid Statistical Information System	Prior to Federal fiscal year 1999, the Medical Statistical Information System (MSIS) were a voluntary program and those states participating in the MSIS project provided data tapes from their claims processing systems to the Centers for Medicare & Medicaid Services (CMS) in lieu of the hard-copy statistical 2082 tables. However, in accordance with the Balanced Budget Act (BBA) of 1997, all claims processed are submitted electronically through MSIS.
Medicare	Medicare is a national social insurance program, administered by the U.S. Federal Government, which guarantees access to health insurance for Americans ages 65 and older and younger people with disabilities as well as people with end stage renal disease.
Migration Readiness Assessment	A document that contains Hosting Provider's assessment of Customer's Infrastructure and that is used for creating a Production Environment that conforms to Hosting Provider's Certified Configuration.
Minor CEMLI Enhancement Request	A request by Customer, via Hosting Provider's Change Management process, for Hosting Provider Hosting Provider to enhance a CEMLI to an Hosting Provider Program within Customer's Environment, where such enhancement is designed to improve the functionality of the CEMLI and does not require Hosting Provider more than 40 person hours to perform. A "person hour" is one hour of work performed by one Hosting Provider resource.
minor maintenance window	The agreed to time when Hosting Provider can perform system maintenance/configuration changes on Production Environment that will have no effect on Production Environment availability.
minor release	An upgrade that contains new functionality and that is upwardly compatible to an earlier Release of the applicable Hosting Provider Program.
My Hosting Provider Support	Hosting Provider's web-based customer support system under which Hosting Provider provides technical support for Hosting Provider Programs and by which Customer may submit Service Requests. Customer obtains the use of My Hosting Provider Support by purchasing technical support services from Hosting Provider.
non-production environment	An instance that is specifically configured for Customer's use (or, as applicable, Customer's Implementer's use) of the Hosting Provider Programs for non-production activities that relate to the Hosting Provider Services, such as development, training, data conversion, and CEMLI maintenance.
North American Data Center	The U.S. data center.
OneGate	OneGate is a Commercial off the shelf (COTS) software that incorporates rulesets, SOA composites, functional portlets and customized Siebel objects, which in the implementation of the Vermont HBE will lead the consumer through the process of shopping for health insurance.
optional third-party software	Any third-party software not supplied by hosting provider.

Term	Definition
outage	A complete loss of access to and use of the Production Environment, the Production Support Environment, the Non-Production Environment, or the Pre-Production Environment. An Outage may be a Planned Outage or an Unplanned Outage.
overall program plan	A project plan prepared by Hosting Provider that outlines the necessary tasks, task performance schedules, and the roles or individuals required to perform such tasks, for a transition.
partial refresh	The process of copying a database and/or a portion of application code from a Source Environment to a Target Environment and making the required configuration Changes within the database and application tier of the Target Environment.
password manager utility	An hosting provider-proprietary tool used by Hosting Provider to manage passwords and provide controlled-access to database and application passwords to those end users who have named Linux/Windows operating system accounts.
PeopleSoft applications	PeopleSoft Enterprise CRM, Enterprise Financials, Human Resources, Portal, Performance Management, Learning Solutions.
performance management	A subset of Hosting Provider Services under which Hosting Provider manages the speed of transaction response of the Hosting Provider Programs, and batch job execution in the Production Environment.
periodic maintenance plan	A written plan prepared and maintained by Hosting Provider that generally describes the schedule for the application of Changes, new Releases, and Upgrades, to the Production Environment.
planned outage	An Outage scheduled by Hosting Provider during which Hosting Provider performs system maintenance and other activities for the Environment and the Hosting Provider Services.
point release	A minor release.
Post Production Go-Live	The period following the Production Go-Live of the Production Environment.
Pre-Production Environment	The instance within the Environment that mirrors Production in capacity, configuration in every way for the sole purpose of applying and testing all changes, hot fixes, patches, code release and/or upgrades before releasing changes to Production.
primary site	The Data Center at which Customer's Environment is located and at which Hosting Provider delivers Hosting Provider Services. The Environment and the delivery of Hosting Provider Services may be relocated to a Secondary Site in the event of a Disaster.
priority level	The classification used in conjunction with Severity Level to identify the priority of a Service Request with respect to the Hosting Provider Services.
problem	The collection of multiple recurring Incidents that exhibit common symptoms and that originate from a single, common cause, and for which the cause is unknown, or (ii) a single Incident that results from a single error and that has an on-going significant impact on the Hosting Provider Services (such as an Unplanned Outage), and for which the cause is unknown.
Problem Management	A subset of Hosting Provider Services under which Hosting Provider manages Problems within Customer's Environment.

Term	Definition
Production Assessment	A document that is prepared by Hosting Provider prior to Production Go-Live and that contains Hosting Provider's assessment of the compliance of Customers' Environment with Hosting Provider Hosting Provider standards.
Production Environment	The instance within the Environment that is specifically set up and configured to support Customer's use of the Hosting Provider Programs, and used by Customer, for production operations. The Production Environment consists of the collection of database servers, application ("mid-tier") servers, and other servers comprising Customer's transactional production system.
Production Go-Live	The date on which Customer first commences use of the Production Environment for production operations (i.e., to process live data).
Production Ready Status	A designation given by Hosting Provider to Customer indicating that Customer may commence use of a Production Environment for production operations.
Production Support Environments	The TEST and DEMO Environments that are specifically set up and configured in a manner that closely resembles the Production Environment, and that are used, as applicable, to troubleshoot and facilitate Incident resolution, to test changes prior to promotion of such changes to the Production Environment and for demonstration purposes.
Program Responsibilities	The functionality that a User may use within the Hosting Provider Programs.
Program-Specific Application Management	The Application Management Services specifically applicable to a certain set of Hosting Provider Programs.
Program-Specific Standards	The Standards Schedule specifically applicable to a certain set of Hosting Provider Programs.
Provisioning Release Plan	A document or set of documents prepared by Hosting Provider that describes the installation and configuration of hardware and software required for the Hosting Provider Environment.
Recovery Point Objective (RPO)	Hosting Provider's objective for the potential maximum time period of data loss, calculated from the onset of a Disaster.
Recovery Time Objective (RTO)	Hosting Provider's objective for the potential maximum period of time between the declaration of a Disaster and the point at which Customer can resume production operations in the Production Environment.
referral	An OK from the primary care physician for the patient to see a specialist or get certain services. In many HMO plans, the insured person needs to get a referral before they get care from anyone except the primary care physician. If the referral is not received, the HMO may cover resulting expenses.
refresh	The process of copying a Customer's database files, application files, and/or the application metadata and artifacts from a Source Environment to a Target Environment and updating related configurations within the Environment.
release	A software change or set of software changes, to Hosting Provider Programs, that is provided to Customer by Hosting Provider's Support Services organization as part of Hosting Provider's technical support services. The term Release includes Upgrades and Maintenance Code Releases.
release management	A subset of Hosting Provider Services under which Hosting Provider manages the deployment of Releases into Customer's Environment.

Term	Definition
release plan	A document that details the planning, testing, and executing of proposed Releases. The Release Plan includes a Back Out Plan.
required software	Third-party software for which hosting provider requires Customer to separately purchase a license and technical support in connection with Hosting Provider Services for certain Hosting Provider Programs, and for which Hosting Provider expressly performs Hosting Provider Services.
restore	The process of copying a database and/or full application code from a disk or tape backup to the Environment from which the copy was made.
sandbox or sandbox environment	A type of Production Support Environment that is used by Customer for the purposes of prototyping, alternative analysis, proof of concept. This environment is not in the development life cycle.
server	A computing platform with defined processing power, memory capacity, and operating system. The Server may be implemented as a virtual or shared allocation from one or more physical computing platform(s).
server for customer managed applications	A Service Option under which Hosting Provider initializes and installs operating system software on an Hosting Provider-provisioned server to enable Customer to access, manage, and monitor such server.
server for hosting provider managed applications	The Service Option for Computer and Administration Services under which a server is added by Hosting Provider to Customer's Environment to support additional environments.
service interruption	A material reduction of the functionality and responsiveness of a component of the Production Environment, a Production Support Environment, or a Non-Production Environment, such that Customer's ability to use the Hosting Provider Services to process one or more of Customer's key business transactions is significantly impacted.
service pack	A minor release.
service request	A request for assistance with the Environment or any component thereof submitted to My Hosting Provider Support or the Hosting Provider Service Desk.
service-specific application management	Program-Specific Application Management Services Schedule.
service-specific standards	Program-Specific Standards.
seven conditions and standards (CMS)	Issued by the Centers for Medicare & Medicaid Services (CMS) to foster better collaboration with states, reduce unnecessary paperwork, and focus attention on the key elements of success for modern systems development and deployment.
severity level	The level of criticality assigned to a Service Request based on defined criteria.
Siebel CRM Program	An Hosting Provider Program identified by Hosting Provider as an Hosting Provider Siebel CRM Program. Hosting Provider performs Hosting Provider Siebel Programs.
site	A website for which Hosting Provider Services for all Programs.
site go-live	The date on which a Site first becomes available to the general public and transactions can be processed on the Site.

Term	Definition
source environment	A Production Environment, Production Support Environment or Non-Production Environment from which data for a Refresh is obtained.
special benefit networks	Provider networks for particular services, such as mental health, substance abuse, or prescription drugs
staging or staging environment	Pre-Production Environment.
standard industrial classification (sic)	Coding of businesses by their product or service. This classification is used in group insurance in determining rates for various industries.
standard operating procedures	Hosting Provider's set of security-focused processes that set forth the standard procedures, activities and tasks performed by Hosting Provider resources while delivering Hosting Provider Services to Hosting Provider customers.
standby environment	An Environment located at the Secondary Site that closely resembles the capacity and performance capabilities of the Production Environment at the Primary Site, and that may be used for production operations in the event of a Disaster.
super user	An End User that the customer has assigned to assist other End Users in the use of Hosting Provider Services. Super Users serve as the liaison between End Users, Customer's Help Desk, and the Hosting Provider Service Desk.
supplemental services	Service Options.
supported CEMLI	CEMLIs that were reviewed and approved by Hosting Provider as part of the Production Assessment process and for which Hosting Provider provides Hosting Provider Services in the Production Environment.
systems administrator	An Hosting Provider resource assigned by Hosting Provider to perform tasks to maintain the Environment as part of the Hosting Provider Services.
target environment	The Production Environment, Production Support Environment or Non-Production Environment to which data for a Refresh will be applied.
technology stack	Any database, operating system and middleware used in an Environment.
test or test environment	A type of Production Support Environment that is used by Hosting Provider for testing and validating Changes prior to promotion to the Production Environment as well as for recreating events and duplicating issues occurring in the Production Environment for the purposes of troubleshooting and facilitating Incident resolution.
third-party software	Any software from a Third-Party Software Vendor, which is not provided by Hosting Provider as part of the Hosting Provider Services, and any software developed or provided by Customer.
third party vendor	A provider, other than Hosting Provider, of products or services.
tools	Software scripts provided and used by Hosting Provider in the Environment for the delivery of Hosting Provider Services (e.g., to perform environment clones, password changes, service monitoring, and file system maintenance).
training or training environment	A type of Production Support Environment that is used by Customer for the purposes of training.
transaction link	The type of Network Connectivity used for Computer and Administration Services.

Term	Definition
transition	The activities completed and modifications made to a Customer's system and/or to an Hosting Provider Environment as part of Transition Advisory Services.
transition advisory services	A service performed by Hosting Provider to convert a Customer's system to an Hosting Provider Environment or to make significant Changes (such as an Upgrade) to an existing Hosting Provider Environment.
U.S. Data Center	Hosting Provider's Data Center(s) located in the United States.
UAT Environment	A type of Production Support Environment that is used by Customer for testing User Acceptance and validating Changes prior to promotion to the Production Environment.
United States Data Center	U.S. Data Center
unplanned outage	An outage that was not scheduled by Hosting Provider or Customer and is caused by an Incident or Problem.
upgrade	A new Release of an Hosting Provider Program that contains new functionality and/or under which the results of how such program processes data differs as compared to an earlier Release of such program.
user	An end user.
user acceptance testing	A formal testing process that is part of the Change Management Process conducted by Customer of a specified Change to the Environment for the purpose of determining whether such Change meets identified acceptance criteria.
Weekly Maintenance Window	The period of time, to occur once per week, during which Hosting Provider may schedule Planned Outages to perform maintenance activities on Infrastructure. The maintenance activities typically performed by Hosting Provider during a Weekly Maintenance Window involve components of the Infrastructure that are used to deliver Hosting Provider Services to Hosting Provider's customers generally, including to Customer.
Windows Software Update Service	A Microsoft service provided to Hosting Provider under which Microsoft delivers current security updates to Hosting Provider-owned Windows-based computers.
X12 Standards	In 1979, the American National Standards Institute (ANSI) chartered the Accredited Standards Committee (ASC) X12 to develop uniform standards for inter industry electronic exchange of business transactions-electronic data interchange (EDI). ASC X12 provides a single standard with a single architecture, producing a common, uniform language for electronic communications. The X12 Standards will be followed for EDI's developed within the Vermont HBE project.

17 Acronyms

The following table lists acronyms and their definitions introduced in this document.

Exhibit 74: Acronyms

Acronym	Definition
ACA	Affordability Care Act
BRE	Business Rules Engine
CI	Configuration Item
CM	Configuration Management
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial Off the Shelf Software
CRUD	Create, Read, Update and Delete; commonly used in reference to database operations.
DBMS	Database Management System
DDD	Database Design Document
DNS	The translation of a URL text address (e.g., state.vt.us) into a numeric Internet address (e.g., 200.213.11.6).
DR	Disaster Recovery
DVHA	Department of Vermont Health Access
EA	Enterprise Architecture
EDBC	Eligibility Determination and Benefits Calculation
GUI	Graphical User Interface
ICD	Interface Control Document
IRS	Internal Revenue Service
JSP	Java Server Pages
LAN	Local Area Network
LDM	Logical Data Model
MAGI	Modified Adjusted Gross Income
MDM	Master Data Management
MEMC	Medicaid Eligibility and MITA Compliance
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
SDD	System Design Document
SDLC	Software Development Lifecycle
SLOC	Source Lines of Code
SNAP	Supplemental Nutrition Assistance Program

Acronym	Definition
SOA	Service-Oriented Architecture
SR	A Service Request.
SSL	A “secure sockets layer,” a commonly used protocol for managing the security of a data transmission on the Internet. SSL uses a public-and-private key encryption system, which also includes the use of a digital certificate.
UAT	User Acceptance Testing.
VPN	VPN means Virtual Private Network.
WAN	Wide Area Network
WSUS	WSUS means Windows Software Update Service.