

Community Viewer (CV) Release 1.5 System Design Document (SDD)



December 2016

Version 1.5

Department of Veterans Affairs

Revision History

Date			
12/22/2016	1.5	Addressed client comments and resubmitted	AbleVets
12/20/2016	1.4	Client comments addressed and resubmitted	AbleVets
12/09/2016	1.3	Updated for security banner information and resubmitted	AbleVets
11/14/2016	1.2	Edited per client comments and resubmitted	AbleVets
11/10/2016	1.1	Edited per client comments and resubmitted	AbleVets
11/07/2016	1.0	Submitted for CLIN 0003AA	AbleVets
11/02/2016	0.1	Initial draft of document	AbleVets

Artifact Rationale

The System Design Document (SDD) is a dual-use document that provides the conceptual design, as well as the as-built design. This document will be updated as the product is built, to reflect the as-built product.

Table of Contents

1. Introduction	9
1.1. Scope.....	9
1.2. User Profiles	9
2. Background	10
2.1. Overview of the System	10
2.2. Overview of the Business Process	10
2.3. Overview of the Significant Requirements	10
2.3.1. Overview of Functional Workload and Performance Requirements ..	11
2.3.2. Overview of Special Device Requirements	11
3. Conceptual Design	12
3.1. Conceptual Application Design	12
3.1.1. Application Context.....	12
3.1.2. High-Level Application Design	12
3.1.2.1. Graphical User Interface (GUI) Framework	12
3.1.3. Application Locations	13
3.1.4. System Framework Model.....	13
3.1.5. Architecture Tiers	14
3.1.5.1. Presentation Tier	14
3.1.5.2. Abstraction (Application) Tier	15
3.1.5.3. Data/Storage Tier	15
3.2. Conceptual Data Design.....	15
3.2.1. Project Conceptual Data Model	15
3.2.2. Database Information	15
3.2.3. User Interface Data Mapping.....	15
3.2.3.1. Application Screen Interface	15
3.2.3.1.1. CCP Login Page.....	15
3.2.3.1.2. CCP Password Reset	16
3.2.3.1.3. CCP VA Privacy and Security Awareness Training Page.....	17
3.2.3.1.4. VAS CCPM: Create New Provider Group.....	18
3.2.3.1.5. VAS CCPM: Facilities Search.....	19
3.2.3.1.6. VAS CCPM: Create/Edit Provider	20
3.2.3.1.7. VAS CCPM: Assign Patient	22
3.2.3.2. Application Report Interface	23
3.2.3.3. Unmapped Data Elements	23
3.3. Conceptual Infrastructure Design	23
3.3.1. System Criticality and High Availability	23
3.3.2. Special Technology	23
3.3.3. Technology Locations.....	23
3.3.4. Conceptual Infrastructure Diagram	23
3.3.4.1. Location of Environments and External Interfaces	23

3.3.4.2.	Conceptual Production String Diagram.....	23
4.	System Architecture.....	23
4.1.	Hardware Architecture	23
4.1.1.	Hardware Specifications	24
4.2.	Software Architecture	25
4.2.1.	Client-Side Development Technologies.....	25
4.2.2.	Server-Side Development Technologies.....	26
4.2.3.	Additional Design Considerations.....	26
4.3.	Network Architecture	26
4.4.	Service Oriented Architecture/ESS	26
4.5.	Enterprise Architecture	27
5.	Data Design	27
5.1.	Database Management System (DBMS) Files.....	27
5.1.1.	Database Tables	27
5.2.	Non-DBMS Files.....	30
5.3.	Data View	30
6.	Detailed Design	32
6.1.	Hardware Detailed Design.....	32
6.2.	Software Detailed Design.....	32
6.2.1.	Conceptual Design	34
6.2.1.1.	Product Perspective	34
6.2.1.1.1.	User Interfaces	34
6.2.1.1.2.	Hardware Interfaces	35
6.2.1.1.3.	Software Interfaces	35
6.2.1.1.4.	Communications Interfaces.....	35
6.2.1.1.4.1.	Data Request/Response Sequence.....	36
6.2.1.1.5.	Memory Constraints	37
6.2.1.1.6.	Special Operations	37
6.2.1.2.	Product Features	37
6.2.1.3.	User Characteristics	37
6.2.1.4.	Dependencies and Constraints	37
6.2.1.5.	External Data Sources.....	37
6.2.2.	Specific Requirements	37
6.2.2.1.	Database Repository	37
6.2.2.2.	System Features	38
6.2.2.3.	Design Element Tables	38
6.2.2.3.1.	Routines (Entry Points)	38
6.2.2.3.2.	Templates.....	38
6.2.2.3.3.	Bulletins	38
6.2.2.3.4.	Data Entries Affected by the Design.....	38
6.2.2.3.5.	Unique Record(s)	38
6.2.2.3.6.	File or Global Size Changes	38
6.2.2.3.7.	Mail Groups	38
6.2.2.3.8.	Security Keys.....	38

6.2.2.3.9.	Options	38
6.2.2.3.10.	Protocols.....	38
6.2.2.3.11.	Remote Procedure Call (RPC).....	38
6.2.2.3.12.	Constants Defined in Interface.....	38
6.2.2.3.13.	Variables Defined in Interface.....	38
6.2.2.3.14.	Types Defined in Interface	38
6.2.2.3.15.	GUI	39
6.2.2.3.16.	GUI Classes	39
6.2.2.3.17.	Current Form	39
6.2.2.3.18.	Modified Form	39
6.2.2.3.19.	Components on Form	39
6.2.2.3.20.	Events.....	39
6.2.2.3.21.	Methods.....	39
6.2.2.3.22.	Special References	39
6.2.2.3.23.	Class Events	39
6.2.2.3.24.	Class Methods.....	39
6.2.2.3.25.	Class Properties	39
6.2.2.3.26.	Uses Clause	39
6.2.2.3.27.	Forms	39
6.2.2.3.28.	Functions.....	39
6.2.2.3.29.	Dialog	39
6.2.2.3.30.	Help Frame.....	40
6.2.2.3.31.	HL7 Application Parameter	40
6.2.2.3.32.	HL7 Logical Link.....	40
6.2.2.3.33.	COTS Interface	40
6.2.2.4.	System Requirements	40
6.2.2.5.	Access Requirements.....	40
6.3.	Network Detailed Design.....	40
6.4.	Security and Privacy	40
6.4.1.	Security	40
6.4.2.	Privacy.....	41
6.4.3.	System Audit and Log Capabilities	42
6.5.	Service Oriented Architecture/ESS Detailed Design	43
6.5.1.	Service Description	43
6.5.2.	Service Design	43
6.5.2.1.	Introduction	43
6.5.2.1.1.	Purpose and Scope of Service	43
6.5.2.1.2.	Links to Other Documents.....	43
6.5.2.2.	Service Details.....	43
6.5.2.2.1.	Service Identification	43
6.5.2.2.2.	Service Versions	43
6.5.2.2.3.	Summary of Design and Platform Details.....	43
6.5.2.2.3.1.	SOA Pattern(s) Implemented	43
6.5.2.2.3.2.	COTS Platform vendor names and versions for hosting platform	43
6.5.2.3.	Dependencies.....	43
6.5.2.4.	Service Design Details	43
6.5.2.4.1.	Interface Technical Specs.....	43
6.5.2.4.1.1.	Service Invocation Type	44

6.5.2.4.1.2.	Service Interface Type.....	44
6.5.2.4.1.3.	Service Name	44
6.5.2.4.1.4.	Interface	44
6.5.2.4.1.5.	End Points	44
6.5.2.4.1.6.	Operations or Methods	44
6.5.2.4.1.7.	Message Schemas	44
6.5.2.4.2.	Information Model.....	44
6.5.2.4.2.1.	Class Diagram and Description of Entities Involved.....	44
6.5.2.4.2.2.	Mappings from ELDM to Standards Based Schemas	44
6.5.2.4.3.	Behavior Model (AKA Use Case Realization)	44
6.5.2.4.3.1.	Use Cases (Use Case Model).....	44
6.5.2.4.3.2.	Interaction Diagrams	44
6.5.2.5.	Gap Analysis.....	44
6.5.2.5.1.	Variances from Enterprise Target Architecture	44
6.5.2.5.2.	Variances from SLDs	44
6.5.2.5.3.	Variances from Standards and Policies.....	45
6.5.2.5.4.	Justification for Exceptions and Mitigation.....	45
7.	External System Interface Design	45
7.1.	Interface Architecture.....	45
7.2.	Interface Detailed Design	45
8.	Human-Machine Interface.....	45
8.1.	Interface Design Rules	45
8.2.	Inputs.....	45
8.3.	Outputs.....	45
8.4.	Navigation Hierarchy.....	45
9.	Quality of Service (QoS) (Health Monitor) Design.....	45
9.1.	System Status Checks	46
9.2.	Status Messages	47
9.3.	E-mail Notification	47
9.3.1.	Sample E-mail Notification.....	48
9.4.	Database Integration	48
9.5.	Required Permissions and Roles	49
9.6.	Modifications to External Systems and Services	49
9.6.1.	jMeadows Data Service	49
9.6.2.	Middleware Services	49
9.7.	GUI Status Message Display.....	49
9.7.1.	Sample System Status Messages	49
9.7.1.1.	Services Available System Status Messages.....	50
9.7.1.2.	Services Unavailable System Status Messages.....	51
9.8.	Security Impact.....	52
10.	Attachment A – Approval Signatures	53
A.	Appendix - Additional Information	54

A.1. Identification of Technology and Standards.....	54
A.2. Constraining Policies, Directives and Procedures.....	54
A.3. Requirements Traceability Matrix.....	54
A.4. Packaging and Installation.....	54
A.5. Design Metrics	54
B. Appendix – Acronyms and Abbreviations	55

Table of Figures

Figure 1: CV Context Diagram	12
Figure 2: Client/Server Technologies in the Stack	13
Figure 3: N-Tier Architecture Sample Structure	14
Figure 4: CCP Login Page	16
Figure 5: CCP Password Reset	17
Figure 6: CCP VA Privacy and Security Awareness Training Page	17
Figure 7: CCPM: Create Provider Groups	19
Figure 8: CCPM Facilities Search.....	20
Figure 9: CCPM Create/Edit Provider	21
Figure 10: CCPM: Assign Patient	22
Figure 11: CV Production Hardware Architecture Diagram	24
Figure 12: VAS User Authentication Sequence	33
Figure 13: CCP User Authentication Sequence	34
Figure 14: Communication Interface Diagram.....	36
Figure 15: CV VA Data Retrieval.....	37
Figure 16: System Status Check Sequence	47
Figure 17: Services Available Status Message – Login Page.....	50
Figure 18: Services Available Status Message – Portal Page.....	50
Figure 19: Patient Lookup Service Unavailable – Login Page.....	51
Figure 20: Patient Lookup Service Unavailable – Portal Page.....	52

Table of Tables

Table 1: CV User Profiles	9
Table 2: Operational Environment Requirements	11
Table 3: CCP Login Page Fields	16
Table 4: CCP Privacy and Security Awareness Training Page Fields.....	18
Table 5: CCPM: Create Provider Groups Page Fields	19
Table 6: CCPM Facilities Search Field	20
Table 7: CCPM Create/Edit Provider Page Fields	21
Table 8: CCPM Assign Patient Page Fields	22
Table 9: CV Server Specifications	24
Table 10: C_Organization Table	27
Table 11: C_OrganizationAudit Table	28
Table 12: C_OrganizationFacility Table	28
Table 13: C_Patient Table	28
Table 14: C_Patient Audit Table.....	29
Table 15: C_PatientUsage Table.....	29
Table 16: C_Provider Table	29
Table 17: C_Provider Audit Table	30
Table 18: C_SecurityAgreement Table	30
Table 19: CV System Stored Procedures	31
Table 20: Framework Elements and Implementation.....	35
Table 21: Audit Table Entries	42
Table 22: Heath Monitor Status Messages	47
Table 23: Sample Heath Monitor E-mail Notification	48
Table 24: cvuser Service Account Permissions.....	48
Table 25: Acronyms and Abbreviations.....	55

1. Introduction

The Community Viewer (CV) is a browser-based software application built on the Joint Legacy Viewer (JLV) system. CV allows Community Care Providers (CCPs) to securely access and view a Veteran's health record held by the Department of Veteran's Affairs (VA). The ability for CCPs to access this data improves care coordination and continuity of care for VA patients receiving treatment outside of the VA network.

CV consolidates information from the Veterans Information Systems and Technology Architecture (VistA) Electronic Health Record (EHR) in real time for viewing within a web browser. Through CV, VA Administrative Staff (VAS) can assign consultations to CCPs and provision CCP use within the CV system, allowing non-VA providers access to view patient records from multiple VistA systems.

1.1. Scope

The System Design Document (SDD) is a dual-use document that provides the conceptual design of the CV system, as well as the as-built design.

1.2. User Profiles

[Table 1](#) below details the intended user base for the CV system. Access levels are defined as follows:

- **Limited, read-only access to patient EHR** relates to users outside the VA network who have been granted access to patient records only after an active consult has been assigned.
- **Full access** relates to the assigning of elevated roles and permissions that enable the user direct rights to access information and computer security in general, and control over rules to process requests from (authenticated) consumers.
- **Full control** relates to the permissions established for a user that enables them to read and write to databases, system code, and interface configuration. Full control is generally provided to system developers.

Table 1: CV User Profiles

User Level				
Primary User	CCP	At the direction and authorization of VAS, uses the CV system to view patient records.	Limited, read-only access to patient EHR	Access & Authorization (A&A) Access Guidelines System Security Plan (SSP)
Primary User	VAS	Provision system access, assign patients, assign consults, specify duration of access to a patient's EHR.	Full Access	A&A Access Guidelines SSP

User Level				
Secondary User	VA Information Technology (IT) Support/ System Administrator	Access to system database (DB), servers, etc. to execute defect repair, patches, and system updates related to the current build.	Full Control	

2. Background

2.1. Overview of the System

CV has been developed to meet the needs of CCPs to treat Veterans, allowing providers outside the VA network the ability to access Veterans' EHR, as authorized by the patient, and on a need to know basis, to review existing consults/referrals, orders and/or progress reports, or other relevant health record data.

The benefits of the CV system include:

- Increased access to care for Veterans and VA beneficiaries
- Access to a patient's EHR, enabling a clinical decision to provide continuation of treatment and care when a Veteran is seen, via an approved referral, by a CCP
- Utilization of the Community Care Provider Management (CCPM) module's capabilities to limit the exposure of patient data outside of the VA

2.2. Overview of the Business Process

There is an immediate need for a complete, longitudinal health record, available to all Veterans and their providers, at points of care within and outside the VA. CV allows physicians from external partners to view consolidated health records to better inform their care decisions, and enhance the coordination of care for the Veteran.

The CCPM is a provider portal widget available to VAS users that enables the provisioning of CCPs, a process that includes associating the CCP with provider groups and facilities, assigning the CCP patient consults, and limiting access to historical patient information.

Additional elements of the business process include:

- Provide CCPs the ability to access Veterans' EHR, as authorized by the patient, and on a need to know basis, to review specific consults/referrals, orders and/or progress reports, or other relevant health record data.
- Enhance clinical decision-making by providing CCPs with the information necessary to effectively administer a patient's care.

2.3. Overview of the Significant Requirements

Refer to the *CV 1.5 Requirements Specification Document (RSD)*, submitted with this release.

2.3.1. Overview of Functional Workload and Performance Requirements

[Table 2](#) below outlines the functional workload and performance requirements. The requirements listed were originally developed for JLV, and are being utilized for CV.

Table 2: Operational Environment Requirements

Non-Functional Rqmt #	
OER 1.0	System response times and page load times shall be less than 10 seconds. Where response cannot be achieved in 10 seconds, user will be presented a busy working indicator.
OER 2.0	Maintenance, including maintenance of externally developed software incorporated into the Joint Legacy Viewer (JLV) application(s), shall be scheduled during off peak hours or in conjunction with relevant maintenance schedules. The business owner should provide specific requirements for establishing system maintenance windows when planned service disruptions can occur in support of periodic maintenance.
OER 3.0	Information about response time degradation resulting from unscheduled system outages and other events that degrade system functionality and/or performance shall be disseminated to the user community within 30 minutes of the occurrence. The notification shall include the information described in the current Automated Notification Reporting (ANR) template maintained by the VA Service Desk. The specific business impact must be noted in order for the Office of Information and Technology (OIT) to provide accurate data in the service impact notice of the ANR.
OER 4.0	Provide a real-time monitoring solution to report agreed/identified critical system performance parameters.
OER 5.0	Critical business performance parameters shall be identified (e.g. transaction speed, response time for screen display/refresh, data retrieval, etc.) in a manner that data capture can occur to support metric reporting and support the OIT performance dashboard display.
OER 6.0	Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance shall be disseminated to the business user community a minimum of 48 hours prior to the scheduled event.

2.3.2. Overview of Special Device Requirements

The CV interface is a front-end web application designed to run in a browser. It is recommended that users access the CV web application through Internet Explorer (IE) 11. The oldest version of IE that can be used to access CV is IE 10.

VAS users must present their Personal Identification Verification (PIV) credential before gaining access to CV. Based on PIV information, the jMeadows Data Service (jMeadows) retrieves the user's profile information from the CV database. The user's default host location, custom widget layout, and other unique user data are returned.

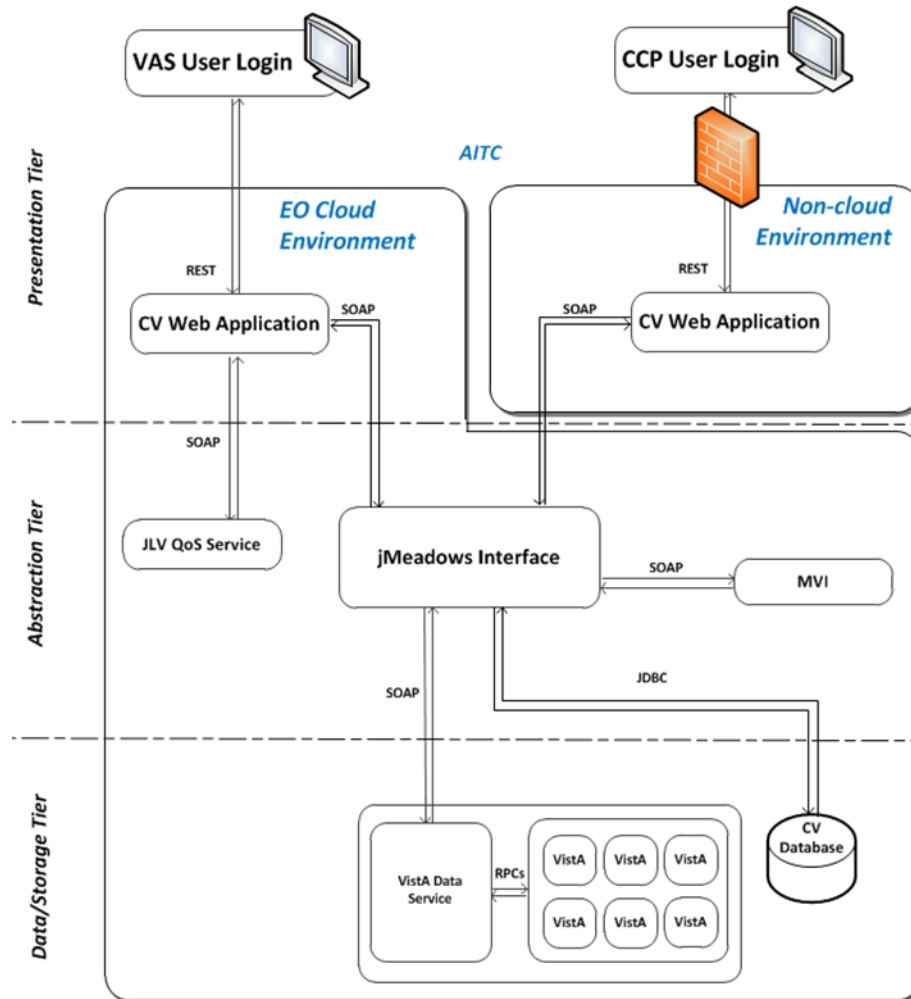
3. Conceptual Design

3.1. Conceptual Application Design

3.1.1. Application Context

[Figure 1](#) is a diagram of the CV application context.

Figure 1: CV Context Diagram

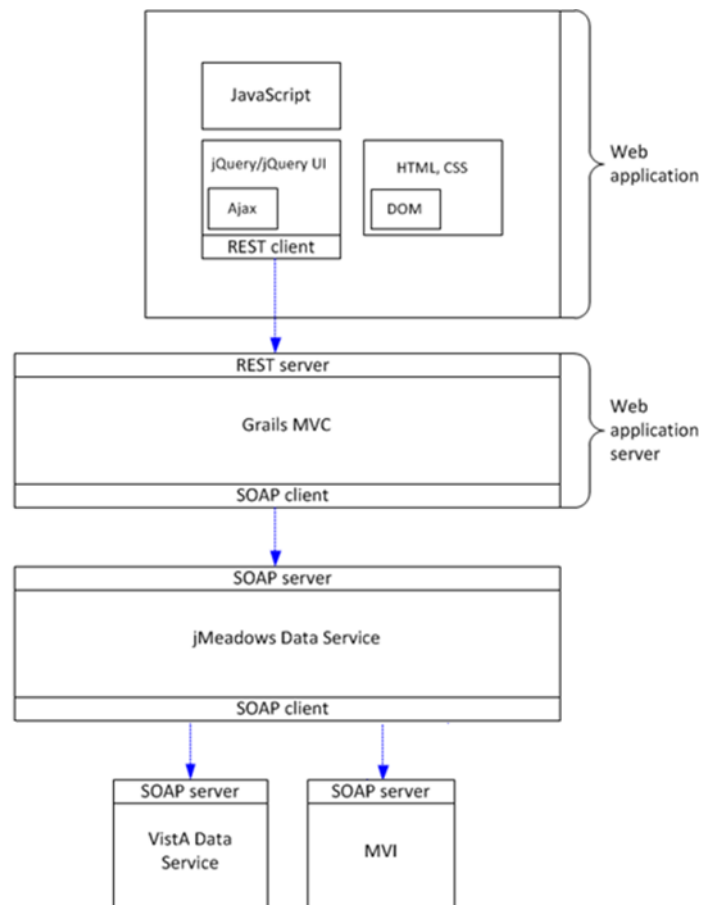


3.1.2. High-Level Application Design

3.1.2.1. Graphical User Interface (GUI) Framework

[Figure 2](#) illustrates the main components of CV, and the messaging protocols that communicate within and between tiers in the system. CV is a read-only GUI that differentiates between client-side and server-side technologies in its framework.

Figure 2: Client/Server Technologies in the Stack



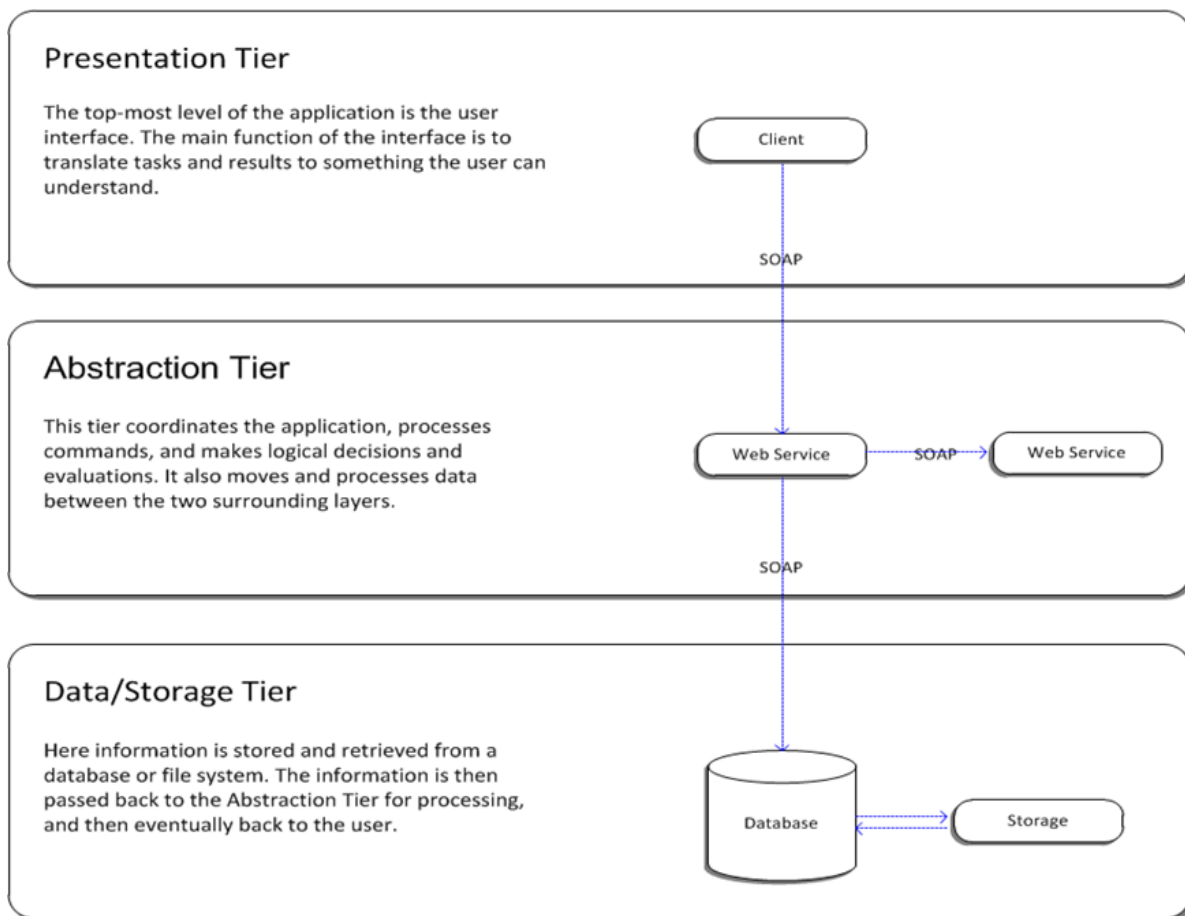
3.1.3. Application Locations

The CV web application executes from the Austin Information Technology Center (AITC). Location and server information can be found in the *CV 1.5 Deployment, Installation, Backout and Rollback Guide*, submitted with this release.

3.1.4. System Framework Model

The CV framework is an n-tier hierarchical model, comprising the presentation, abstraction, and data/storage tiers, as shown in [Figure 3](#).

Figure 3: N-Tier Architecture Sample Structure



3.1.5. Architecture Tiers

Each element in the hierarchy shown in [Figure 3](#) has a specific set of functions and services that it offers, and a specific role to play in each tier of the design.

3.1.5.1. Presentation Tier

The presentation tier, or client tier, is the top-most level of the n-tier architecture, and is considered the user interface. The main function of the interface is to translate tasks and results for the client to understand. CV provides the ability to view specific clinical data stored in any electronic medical record systems available to the abstraction tier.

VAS users must present their PIV credential before gaining access to CV. Based on the PIV information, jMeadows retrieves the user's profile information from the CV database. The user's default host location, custom widget layout, and other unique user data are returned. CCP users are provided username and password credentials, which are stored in the CV database.

Once VAS users launch the presentation layer, they are prompted to enter their credentials. CV sends these credentials to jMeadows, which then authenticates the users to their host EHR system, granting access to CV. User authentication takes place before CV interfaces with jMeadows. CCP users are authenticated against the CV database.

3.1.5.2. Abstraction (Application) Tier

The abstraction tier, or application tier, is the tier that the presentation tier and the data/storage tier use to communicate with each other. The abstraction tier moves and processes data between the presentation tier and the data/storage tier. It coordinates the application, processes commands, and makes logical decisions and evaluations. The process of abstracting the data sources from the application also takes place within this tier.

3.1.5.3. Data/Storage Tier

The data/storage tier is where the source application's data is stored, and from where data is retrieved.

3.2. Conceptual Data Design

3.2.1. Project Conceptual Data Model

A detailed overview of the database design is provided in [Section 5, Data Design](#).

3.2.2. Database Information

A detailed overview of the database design is provided in [Section 5, Data Design](#).

3.2.3. User Interface Data Mapping

3.2.3.1. Application Screen Interface

3.2.3.1.1. CCP Login Page

The CCP Login page, seen in [Figure 4](#), displays the fields a CCP user must complete in order to log into the CV web application. The page's fields are detailed in [Table 3](#).

Figure 4: CCP Login Page

Table 3: CCP Login Page Fields

GUI Field			
Username	C_Provider Table	Name Field	CCP E-mail Address
Password	C_Provider Table	Password Field	CCP Password

3.2.3.1.2. CCP Password Reset

[Figure 5](#) depicts the CCP password reset page. The CCP user completes all fields on this page to request a password reset. The information entered into the fields is inserted into a Simple Mail Transfer Protocol (SMTP) command, and is not saved to the database.

CCP passwords follow the characteristic guidelines for strong passwords:

- At least eight (8) characters; the more characters, the stronger the password
- A combination of uppercase and lowercase letters
- A combination of letters and numbers
- Inclusion of at least one special character: ! @ # ?]

Figure 5: CCP Password Reset

The screenshot shows the 'Community Viewer' logo at the top, with 'powered by JLV' underneath. Below the logo is the text 'Community Care Provider Login'. The main form is titled 'Password Reset' and contains the following text: 'Please fill in the fields below and click Send to request a password reset for your Community Viewer account. This request will be forwarded to a VA Administrator who contact you with a new password.' The form has four input fields: 'First Name:' (labeled 'Required'), 'Last Name:' (labeled 'Required'), 'Email Address:' (labeled 'Required'), and 'Phone:'. At the bottom right of the form are 'Cancel' and 'Send' buttons. Below the form, there is a green checkmark icon and the text 'CV data sources available.' and a blue link 'CV Help'. At the very bottom, it says 'Build 1.5.0.0.0.20161017'.

3.2.3.1.3. CCP VA Privacy and Security Awareness Training Page

[Figure 6](#) is a screen shot of the CCP VA Privacy and Security Awareness Training page. This page presents training documents for the CPP to download, and certification checkboxes the CCP checks to acknowledge training. These requirements must be met in order to access the CV web application for the first time, and again every 365 days. The fields are described in [Table 4](#).

Figure 6: CCP VA Privacy and Security Awareness Training Page

The screenshot shows the 'VA Privacy and Security Awareness Training' page. It begins with the heading 'VA Privacy and Security Awareness Training' and the text 'You are seeing this page for one of the following reasons:'. Below this is a numbered list: '1. You are attempting to access Community Viewer for the first time.' and '2. Your security and privacy training certification has expired.' The text continues: 'For Community Viewer access, please download and review the following training documents to satisfy VA security and privacy requirements. You will need to complete this training every 12 months.' This is followed by two bullet points with links: '• [Information Security Awareness \(pdf\)](#)' and '• [Electronic Health Records Rules of Behavior \(pdf\)](#)'. The text then states: 'After reviewing the training documents above, you must check all of the following boxes to acknowledge the training below in order to enable the "I Confirm" button and continue to Community Viewer.' Below this are three checkboxes: 'I certify that I have completed and understand the Information Security Awareness training.', 'I certify that I have renewed and understand the Electronic Health Records Rules of Behavior.', and 'I certify that I have completed and understand the HIPAA privacy training provided by my organization.' The section is titled 'Acknowledgement of Accuracy' and contains the text: 'Under penalty of perjury, I attest that the above information is accurate and true to the best of my knowledge, and I have completed the training shown above.' At the bottom are 'Cancel' and 'I Confirm' buttons.

Table 4: CCP Privacy and Security Awareness Training Page Fields

GUI Element			
Information Security Awareness link	C_SecurityAgreement	ISADownloadDate	User must download and read each file to complete the required training.
Electronic Health Record Rules of Behavior link	C_SecurityAgreement	EHRROBDownloadDate	
Information Security Awareness checkbox	C_SecurityAgreement	CertISADate	User must check the box beside each item to complete the required acknowledgement of training.
Electronic Rules of Behavior checkbox	C_SecurityAgreement	CertEHRROBDate	
HIPAA checkbox	C_SecurityAgreement	CertHIPAADate	User must check the box beside this item to confirm completion of HIPAA training within their organization
I Confirm button	C_SecurityAgreement	AgreementExpirationDate	Clicking the I Confirm button records the current date as the training completion date, and sets an expiration for 365 days in future.

3.2.3.1.4. VAS CCPM: Create New Provider Group

The CCPM enables VAS users to create provider groups using the Create New Provider Group dialog, as seen in [Figure 7](#). The fields within the dialog are described in [Table 5](#).

Figure 7: CCPM: Create Provider Groups

Table 5: CCPM: Create Provider Groups Page Fields

GUI Field			
Provider Group Name	C_OrganizationFacility	FacilityID	
Address	C_Organization	Address	
City	C_Organization	City	
State	C_Organization	State	
National Provider Identifier (NPI)	C_Organization	NPI	
Point of Contact (POC)	C_Organization	ContactName	
POC E-mail Address	C_Organization	ContactEmail	
POC Phone	C_Organization	ContactPhone	
Secondary Phone	C_Organization	ContactPhone	
RecordStatus	C_Organization	Not applicable	Clicking the Save button creates the organization and records its status as ACTIVE

3.2.3.1.5. VAS CCPM: Facilities Search

VAS users can search CCPM for previously configured facilities, as seen in the screen shot below ([Figure 8](#)). The field associated with this functionality is described in [Table 6](#).

Figure 8: CCPM Facilities Search

The screenshot shows the 'Community Viewer' interface. At the top, there is a navigation bar with 'Patient Search' and 'Provider Portal' tabs. The 'Provider Portal' tab is selected. Below the navigation bar, there is a 'Create / Edit Provider' window. On the left side of this window, there is a 'Search Providers' section. It contains a 'Facilities' input field with the text 'VA TEST SITE', a 'Browse' button, a 'Search' button, and a table with columns 'Provider Name' and 'Provider Group'. Below the table is a 'Create New Provider' button. The main area of the 'Create / Edit Provider' window displays 'No Provider Selected'.

Table 6: CCPM Facilities Search Field

GUI Field			
Facilities	C_OrganizationFacility	FacilityID	The search is performed against entries in database.

3.2.3.1.6. VAS CCPM: Create/Edit Provider

VAS users can create and edit CCP users in the CCPM, as depicted in [Figure 9](#). The fields associated with this functionality are described in [Table 7](#).

Figure 9: CCPM Create/Edit Provider

The screenshot shows the 'Create / Edit Provider' form in the 'Community Viewer' application. The sidebar on the left contains a 'Search Providers' section with a 'Facilities' dropdown set to 'VA TEST SITE', a 'Search' button, and a table with columns 'Provider Name' and 'Provider Group'. The main form area includes fields for 'Provider Group', 'Specialty', 'First Name', 'Last Name', 'NPI', 'Email', 'Account Type' (set to 'Outside Provider'), 'Phone', 'Allow Access to Data Types' (with checkboxes for VA, DoD, VA VLER, DoD VLER), 'User Name', and 'Password' (with a 'Generate' button). A 'Create New Provider' button is at the bottom left, and 'Cancel' and 'Save' buttons are at the bottom right.

Table 7: CCPM Create/Edit Provider Page Fields

GUI Field	Connected to DB (Table)	Connected to DB (Table) Field	Comments
Facilities	C_OrganizationFacility	FacilityID	Searches are performed against the entries in the database.
Provider Group	C_Provider	OrganizationRecordID	
Specialty	C_Provider	Specialty	
First Name	C_Provider	Name	
Last Name	C_Provider	Name	
NPI	C_Provider	NPI	
E-mail	C_Provider	E-mail	
Allow Access to Data Types	C_Provider	DataTypeAccess	
Account Type	Not applicable	Not applicable.	All Provider accounts are for CCPs in this release.
Phone	C_Provider	Phone	
User Name	C_Provider	Username	Auto-filled in form; equal to user's e-mail address.
Password	C_Provider	Password	Generated in CV and saved to the database.

3.2.3.1.7. VAS CCPM: Assign Patient

VAS users can assign patients to CCP users thorough the CCPM ([Figure 10](#)). The associated fields are described in [Table 8](#).

Figure 10: CCPM: Assign Patient

Table 8: CCPM Assign Patient Page Fields

GUI Field	Connected to DB (Table)	Connected to DB (Table) Field	Comments
Patient Search field	Not applicable.	Not applicable.	Patient search is not performed against the database.
Patient Select (from search results)	C_Patient	Name	Clicking the Assign button completes the process and writes the patient assignment to the database.
Consult (select from Consults list)	C_Patient	ProviderRecordID Name SiteID IEN ConsultNumber ConsultName ConsultProvider ConsultStatus	Clicking the Assign button completes the process and writes the consult to the database.
Default Date Range Start	C_Patient	StartDateFilter	Clicking the Assign button completes the process and writes the date to the database.

3.2.3.2. Application Report Interface

Not applicable to CV.

3.2.3.3. Unmapped Data Elements

All users are presented with an Information Systems Access Warning Disclaimer before the CV login page and login fields are displayed. The action users take to acknowledge the disclaimer is not mapped to the CV database (VAS users click the I Agree button, and CCP users click the OK button).

3.3. Conceptual Infrastructure Design

3.3.1. System Criticality and High Availability

System criticality and high availability criteria are provided in the *Business Impact Assessment*, associated with this release.

3.3.2. Special Technology

There is no special technology utilized for this project.

3.3.3. Technology Locations

This technology will be deployed at AITC.

3.3.4. Conceptual Infrastructure Diagram

Please see [Figure 11](#), below.

3.3.4.1. Location of Environments and External Interfaces

CV is hosted at the AITC. [Figure 11](#) provides an overview of the CV production infrastructure. CV Server specifications can be found in [Table 9](#).

3.3.4.2. Conceptual Production String Diagram

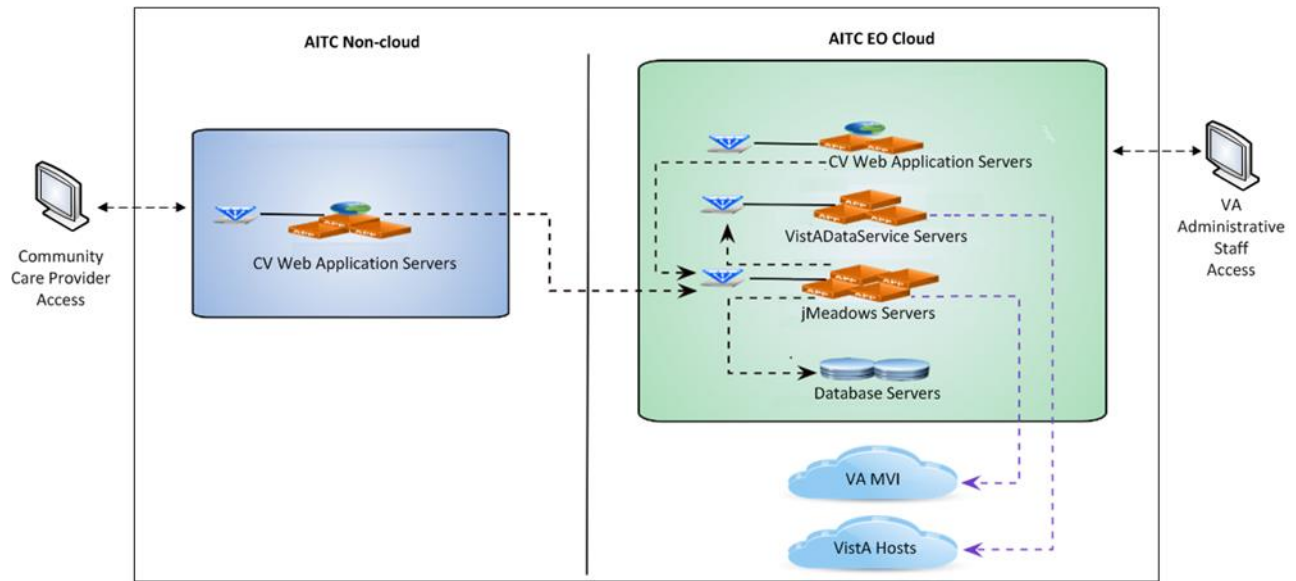
Please see [Figure 11](#).

4. System Architecture

4.1. Hardware Architecture

All servers, firewalls, and connections to the system are at the AITC, as shown in [Figure 11](#).

Figure 11: CV Production Hardware Architecture Diagram



4.1.1. Hardware Specifications

[Table 9](#) describes the server specifications for CV Production infrastructure, hosted at the AITC.

Table 9: CV Server Specifications

Application or Service	Server Specifications
CV Web Application (for VAS users)	Two (2) servers: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago) - Oracle WebLogic 12c
CV Web Application (for CCP users)	Three (3) servers: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago) - Oracle WebLogic 12c
VistA Data Service	Three (3) servers: - Intel Xeon CPU X7560 @ 2.27GHz, 2261 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago) - Oracle WebLogic 12c One (1) server: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago) - Oracle WebLogic 12c
jMeadows Data Service	Four (4) servers: - Intel Xeon CPU X7560 @ 2.27GHz, 2261 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago) - Oracle WebLogic 12c

Application or Service	Server Specifications
CV Database	Two (2) servers: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Microsoft Windows Server 2012 R2 Standard

4.2. Software Architecture

Refer to [Figure 2](#) for more information.

4.2.1. Client-Side Development Technologies

The following technologies are utilized for the development of client-side components within the CV system:

- **Backbone.js** (v1.1.2) provides structure to web applications by providing models with key-value binding and custom events, collections with a rich Application Program Interface (API) of enumerable functions, views with declarative event handling, and connects to existing API over a RESTful JavaScript Object Notation (JSON) interface.
- **Cascading Style Sheets (CSS)** is the language for describing the presentation, i.e., the formatting and layout of a HyperText Markup Language (HTML) document. CSS is designed to enable the separation of document control from the details of how it should be presented, including the typography, positioning, colors, and margins. This separation improves content accessibility, and provides more flexibility in controlling presentation characteristics. The application is CSS Level 3-compliant.
- **eXtensible Markup Language (XML)** is a set of rules for marking up documents. It is widely used to transmit arbitrarily structured data in mixed client/server environments. XML and HTML are compatible members of a family of markup languages called Standard Generalized Markup Language (SGML). HTML is an SGML language with a specific Document Object Model (DOM), focused on describing hypertext documents. The application is compliant with XML version 1.0, 5th Edition.
- **Extensible Stylesheet Language (XSL) Transformations (XSLT)** is a language used with XML documents to transform them into other formats or objects. The application is compliant with XSLT version 3.
- **HTML** is a markup language for web pages that provides a means to create structured documents using semantic tags. Images and other media objects can be embedded and can be used to create interactive forms. The application is HTML 5-compliant.
- **JavaScript** is an object-oriented scripting language. Although JavaScript has other uses, it is client-side JavaScript, the version that runs inside a user's browser and manipulates HTML page elements, in use. Client-side JavaScript is used to turn static HTML documents into interactive web applications. The application is JavaScript 5.1-compliant.
- **JSON** is a language-independent system for representing data objects, although it is based on JavaScript. It is simpler than XML, and is often used as an alternative to XML in Asynchronous JavaScript and XML (AJAX) applications to transfer data objects between a server and a script running in a user's browser. The application is JSON 1.0-compliant.

- **jQuery** (v1.11.1) is a feature-rich JavaScript library and easy-to-use API that works across a multitude of browsers, and simplifies development with HTML document traversal and manipulation, event handling, animation, and Ajax.
- **jQuery User Interfaces (UI)** (v1.12) is a set of UI interactions, effects, widgets, and themes built on top of the jQuery JavaScript Library.

4.2.2. Server-Side Development Technologies

The following technologies are used to build the server-side of the CV system:

- **Grails (v2.4.4)** is an open source, java web application framework that has been designed according to the Model-View-Controller (MVC) paradigm. MVC is a software architectural pattern (not software) that isolates domain logic (the application logic for the user) from the UI (input and presentation).
- **SOAP (Simple Objects Access Protocol)** (v2.0) is utilized as the messaging protocol that communicates between the systems. When SOAP requests are initiated from the Grails MVC framework running on the CV Server, the system waits for a response, as the request is synchronous. If the response is not given with a finite period of time (the default is 100 seconds), the connection terminates, the user receives a connection error message, and the system will not initiate any new requests until action is taken by the user. All SOAP messages are digitally signed.
- **Java** is the language used for development. Java v7u99 is required for Oracle WebLogic 12c on all application servers.

4.2.3. Additional Design Considerations

The CV system is designed to run within both IPv4- and IPv6-based environments. WebLogic Server is IPv4 and IPv6 compliant. CV does not use Internet Protocol (IP) addresses in its configurations.

CV implements session management and keeps track of a user's activity across sessions of the CV system. Session management allows the state of application(s) that are running to be saved and remembered.

CV implements session state on the server side for managing state. The process of knowing the values of controls and variables is known as state management. Session state is server side. In session state, a special session Identification (ID) is stored on the server. This session ID identifies a specific application. The session ID is assigned to the calling browser.

4.3. Network Architecture

CV utilizes the network infrastructure provided by the AITC. Refer to [Figure 11](#) for more information.

4.4. Service Oriented Architecture/ESS

The CV system does not participate in a VA Enterprise Service Bus at this time.

4.5. Enterprise Architecture

Enterprise software is summarized in the *CV 1.5 Deployment, Installation, Backout and Rollback Guide Document*, submitted with this release.

5. Data Design

This section summarizes the design of the CV database, a component within the data/storage tier, depicted in [Figure 3](#).

5.1. Database Management System (DBMS) Files

The database system is configured using utility programs that ship with Structured Query Language (SQL) Server 2012. These database management tools are available for the Microsoft Management Console (MMC). These tools manage services associated with the CV database, including actions such as the starting, pausing, resuming, and stopping of services. The tools are also used to configure client network protocols, manage network connectivity, and start the database engine, as necessary.

5.1.1. Database Tables

C_Organization Table

[Table 10](#) describes the C_Organization table, a list of organizations to which a provider may belong. A provider is associated with only one organization.

Table 10: C_Organization Table

Column Name	Type	Description
RecordID	int	Unique ID of each entry (auto-generated)
RecordStatus	varchar(16)	Record Status - ACTIVE or DELETED
Name	varchar(256)	Name of organization
Address	varchar(256)	Organization's address
City	varchar(256)	Organization's city
State	varchar(8)	Organization's state
ZIP	varchar(16)	Organization's zip code
Phone	varchar(32)	Organization's phone number
ContactName	varchar(256)	Organization's contact name
ContactPhone	varchar(32)	Organization's contact phone number
ContactEmail	varchar(256)	Organization's contact e-mail
NPI	varchar(32)	Organization's NPI

C_OrganizationAudit Table

[Table 11](#) describes the C_OrganizationAudit table, a list of audit actions when an organization is created, updated, and/or deleted, and the user who completed the action.

Table 11: C_OrganizationAudit Table

Column Name	Type	Description
RecordID	Int	Unique ID of each entry (Autogenerated)
Date	datetime	Entry date/time stamp
Action	varchar(16)	Action (create, update, delete) performed on record
OrganizationRecordID	Int	Organization ID whose action was implemented
OrganizationRecord	varchar(3072)	Concatenated string of record values from action
UserRecordID	Int	User ID who performed the action

C_OrganizationFacility Table

[Table 12](#) details the C_OrganizationFacility table, a list of facilities and VA sites tied to an organization. One organization can contain multiple sites.

Table 12: C_OrganizationFacility Table

Column Name	Type	Description
RecordID	int	Unique ID of each entry (Autogenerated)
OrganizationRecordID	int	Organization ID
FacilityID	varchar(10)	Facility ID/SiteCode

C_Patient Table

[Table 13](#) describes the C_Patient table, a list of VA patients, their consult information, and assigned provider.

Table 13: C_Patient Table

Column Name	Type	Description
RecordID	int	Unique ID of each entry (Auto-generated)
RecordStatus	varchar(16)	Record Status - ACTIVE or DELETED
ProviderRecordID	int	Assigned provider's record ID
Name	varchar(256)	Patient name
SiteID	varchar(16)	Patient site ID
IEN	varchar(16)	Patient site IEN
ConsultNumber	varchar(16)	Consult number
ConsultName	varchar(256)	Consult name
ConsultProvider	varchar(256)	Consult provider
ConsultStatus	varchar(16)	Consult status
StartDateFilter	datetime	Start date filter restriction

C_Patient Audit Table

[Table 14](#) describes the C_PatientAudit table, a list of audit actions when a patient is created, updated, and/or deleted, and the user who completed the action.

Table 14: C_Patient Audit Table

Column Name	Type	Description
RecordID	int	The unique ID of each entry (auto-generated)
Date	datetime	Entry date and time stamp
Action	varchar(16)	The action (create, update, delete) performed on a record
PatientRecordID	int	ID of patient whose action was implemented
UserRecordID	Int	ID of the user who performed the action

Patient Usage Table

[Table 15](#) describes the C_PatientUsage table, a list of patient records that were accessed, and the provider who accessed them.

Table 15: C_PatientUsage Table

Column Name	Type	Description
RecordID	int	The unique ID of each entry (auto-generated)
Date	datetime	Entry date and time stamp
ProviderRecordID	int	The ID of the provider accessing the record
PatientRecordID	int	The ID of patient whose record being accessed

C_Provider Table

[Table 16](#) depicts the C_Provider table, a list of outside providers recently added to CV.

Table 16: C_Provider Table

Column Name	Type	Description
RecordID	int	Unique ID of each entry (Autogenerated)
RecordStatus	varchar(16)	Record Status - ACTIVE or DELETED
OrganizationRecordID	int	Assigned organization
Name	varchar(256)	Provider's name
Specialty	varchar(64)	Provider's specialty
NPI	varchar(32)	Provider's NPI
Phone	varchar(32)	Provider's phone number
E-mail	varchar(256)	Provider's e-mail address
DataTypeAccess	varchar(64)	Type of data access
Username	varchar(256)	Provider login username (auto-filled; equal to e-mail)
Password	varchar(256)	Provider login hashed password (autogenerated at GUI)

C_ProviderAudit Table

[Table 17](#) describes the C_ProviderAudit table, a list of audit actions when a provider is created, updated or deleted, and the user who completed the action.

Table 17: C_Provider Audit Table

Column Name	Type	Description
RecordID	int	The unique ID of each entry (auto-generated)
Date	datetime	Entry date and time stamp
Action	varchar(16)	The action (create, update, delete) performed on a record
ProviderRecordID	int	The affected provider record
ProviderRecord	varchar(3072)	The change in record details
UserRecordID	int	The ID of the user who performed the action

C_SecurityAgreement Table

[Table 18](#) describes the C_SecurityAgreement table, a list of the security agreements (training) completed by the CCP user, and certification expiration dates.

Table 18: C_SecurityAgreement Table

Column Name	Type	Description
RecordID	int	The unique ID of each entry (auto-generated)
Provusername	varchar(256)	Provider username/e-mail
ISADownloadDate	datetime	Information Security Awareness PDF download date
EHRROBDownloadDate	datetime	Electronic Health Record Rules of Behavior PDF download date
CertISADate	datetime	Certificate of Information Security Awareness checkbox checked date
CertEHRROBDate	datetime	Certificate of Electronic Health Record Rules of Behavior checkbox checked date
CertHIPAADate	datetime	Certificate of Organization HIPAA Training checkbox checked date
SecurityAgreementConfirmed	datetime	Date provider confirmed that all security agreement requirements were fulfilled
AgreementExpirationDate	datetime	Increment of 365 days from the date of Security Agreement confirmation date

5.2. Non-DBMS Files

Not applicable to CV.

5.3. Data View

The design of the CV system includes the development and use of stored procedures, sets of operations, or queries sent to a database. Stored procedures for the CV database are executed through jMeadows. [Table 19](#) lists the stored procedures utilized within the CV system.

Table 19: CV System Stored Procedures

Column Name	Description
C_createOrganization	<ol style="list-style-type: none"> 1. Creates organization record into C_Organization. 2. Updates organization facility mapping in C_OrganizationFacility. 3. Creates organization audit record into C_OrganizationAudit.
C_createPatient	<ol style="list-style-type: none"> 1. Checks if patient is already assigned to provider. 2. If patient not assigned to provider, inserts new patient record into C_Patient. Sets recordStatus to ACTIVE. 3. Inserts new patient audit record into C_addPatientAudit to record patient action.
C_createPatientUsage	Inserts new patient usage record into C_PatientUsage
C_createProvider	<ol style="list-style-type: none"> 1. Checks if provider exists by <unique> e-mail. 2. If provider does not exist, adds new provider to C_Provider. 3. Inserts new provider audit into C_addProviderAudit to record provider action.
C_createSecurityAgreement	Creates a record of dates of security agreement requirements fulfilled after user has confirmed completion of the listed requirements.
C_deleteOrganization	<ol style="list-style-type: none"> 1. Updates C_Organization's RecordStatus to 'Deleted' when organization is deleted. 2. Remove organization's records from C_OrganizationFacility. 3. Inserts record into C_OrganizationAudit to record audit of delete action.
C_deletePatient	<ol style="list-style-type: none"> 1. Update C_Patient's RecordStatus = 'DELETED' when patient is deleted. 2. Insert audit record into C_addPatientAudit to record patient delete action.
C_deleteProvider	<ol style="list-style-type: none"> 1. Update C_Provider's RecordStatus = 'DELETED' when provider is deleted. 2. Update C_Patient's RecordStatus = 'DELETED' for 'deleted' provider. 3. Insert audit record into C_addProviderAudit when provider is set to deleted.
C_isOrganizationExists	Check if organization exists based on name search with 'ACTIVE' RecordStatus.
C_loginProvider	Authenticates Provider during login.
C_retrieveOrganization	Returns 'ACTIVE' organization by organization's name.
C_retrieveOrganizationList	Returns an 'ACTIVE' organization list and the facilities they are tied to, based on similar name search and facilities.
C_retrieveOrganizationPatientList	Returns a list of 'ACTIVE' patients tied to an organization that a given provider belongs to.
C_retrieveOrganizationProviderList	Returns a list of 'ACTIVE' providers tied to an organization.
C_retrievePatient	Returns a patient record based on SiteID and IEN and 'ACTIVE'.
C_retrievePatientUsage	Returns patient usage records based on provider ID.
C_retrieveProvider	Returns an 'ACTIVE' provider record based on provider's username.

Column Name	Description
C_retrieveProviderList	Returns a list of 'ACTIVE' providers tied to an organization based on a similar name search.
C_retrieveProviderPatientList	Returns a list of patients belonging to a provider.
C_retrieveSecurityAgreement	Returns the most recent security agreement record for the provider.
C_retrieveSiteList	Returns a list of sites and their names based on the facilities list of IDs.
C_updateOrganization	1. Updates organization record in C_Organization and C_OrganizationFacility. 2. Adds audit info into C_organizationAudit.
C_updatePatientConsultStatus	Update C_Patient's consultStatus using VistA Consult Status based on patient ID.
C_updateProvider	Update C_Provider record based on Provider ID. Insert audit record into C_ProviderAudit.

6. Detailed Design

6.1. Hardware Detailed Design

See [Table 9](#) in [Section 4.1.1, Hardware Specifications](#) for a description of the server configuration for CV production infrastructure.

6.2. Software Detailed Design

This section provides detailed information regarding the design of the CV 1.5 software.

Access and Authorization Design

For VAS Users:

- The CV system restricts access to the CV GUI to authorized users within the VA enterprise
- VAS user access will be provided by System Administrators through a Uniform Resource Locator (URL)
- VAS users are required to use their VA PIV card and Personal Identification Number (PIN) to log in, along with their local existing VistA/Computerized Patient Record System (CPRS) access and verify codes (for VHA/clinical users)

For CCP Users

CCP users are configured and authorized by VAS users in the CV GUI, as described in the *CV 1.5 User Guide*, provided with the CV release package.

VAS User Authorization Sequence

For VAS users, user access control and authentication takes place before CV interfaces with jMeadows. The user is authenticated to their host EHR system, granting them access to the presentation layer. Based on their credentials, jMeadows retrieves the user's profile information

from the JLV database. The user's default host location, custom widget layout, and other user-specific data are returned.

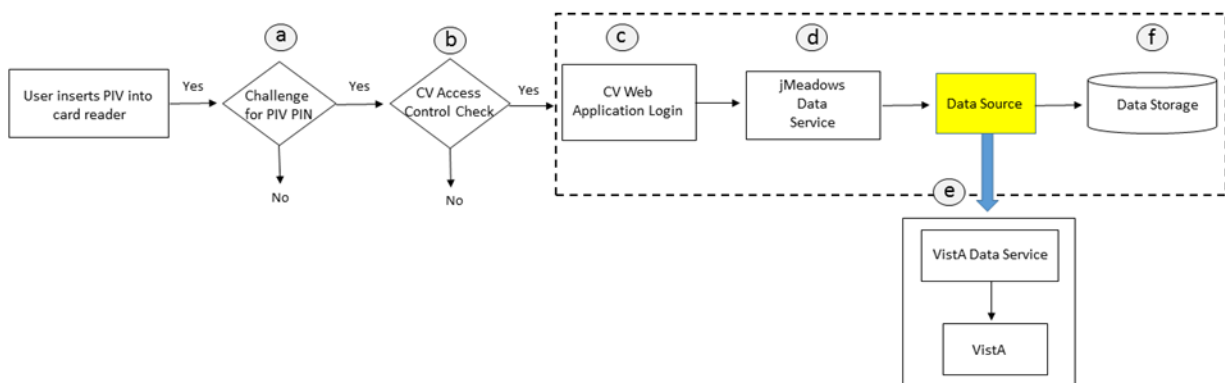
NOTE: The CV system does not directly manage VAS user roles. There is no administrative user access into the JLV web application, either.

A user must insert their PIV card into the computer before entering the URL of the CV application into a browser. The CV login pages guide the user through the login process, including, where necessary, fields to enter user credentials, such as PIV PIN, agency, and site. A detailed overview of this process, from the user's perspective, is included in the *CV 1.5 User Guide*, provided with the CV release package.

In the sequence shown in [Figure 12](#), the following occurs:

1. CV checks for the user's PIV card and retrieves the PIV ID from the smart card
2. The PIV ID is validated against the list of authorized users in the CV database
3. The user enters host system's Access/Verify codes
4. The jMeadows Data Service retrieves user profile information, based on the PIV ID
5. jMeadows uses the Access/Verify codes, and the user's site location, to authenticate the VAS user, via the VistA Data Service
6. Successful login is captured in the database for auditing

Figure 12: VAS User Authentication Sequence



CCP User Authorization Sequence

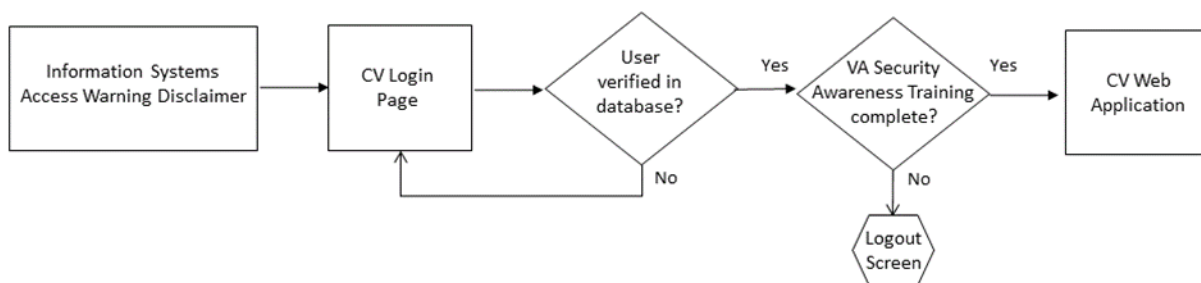
CCP users receive access to CV via their VAS liaison. CV authenticates all CCPs against a list of registered users, provisioned by VAS in the GUI. Credentials entered on the Login page are checked against the database. After logging in, CV verifies that the CCP user has completed VA security training, against the C_SecurityAgreement table in the database. If VA training is not complete, the user is prompted to complete the training before they can access CV.

The CCP login sequence for CV, depicted in [Figure 13](#), is as follows:

1. User navigates to the URL for the CV web application, as provided by VAS
2. CV prompts the user to accept the Information Access Warning Disclaimer, and the user clicks OK to continue
3. The user enters their username and password on the CV Login page, and clicks Login

4. CV validates the user's username and password against the C_Provider table in the CV database
5. Once the CCP user is validated, CV ensures that the CCP user's training is current:
 - a. CV validates the username against the C_SecurityAgreement table in the CV database
 - b. If the username is in the C_SecurityAgreement table, and the expiration date is within the 365-day window of the current date, the user is directed to the CV web application
 - c. If the username is not in the C_SecurityAgreement table, the user is redirected to the VA Privacy and Security Awareness Training page, where they must perform the required actions, before access to CV is granted
6. Successful logins are captured in the CV audit log

Figure 13: CCP User Authentication Sequence



6.2.1. Conceptual Design

Please refer to [Section 3, Conceptual Design](#), for detailed software design and context information.

6.2.1.1. Product Perspective

Refer to [Section 2, Background](#), of this document. For more detailed information, please see the *CV 1.5 Requirements Specification Document (RSD)*, submitted with this release.

6.2.1.1.1. User Interfaces

User interfaces are within the Presentation Tier ([Figure 3](#)), and are built on a simple architecture consisting of portals, tokens, widgets, and sessions. These elements, the definition of each, and their implementation in the GUI, are summarized in [Table 20](#).

Table 20: Framework Elements and Implementation

Element	Implementation
PORTAL A gateway for a website or web application that is the major starting point for users, once connected to the web. A gateway for a website or web application that users visit as an anchor.	The CV interface has two portals: a <i>provider</i> portal and a <i>patient</i> portal. Each portal: <ul style="list-style-type: none"> • Pertains to a particular subject or topic. • Includes a library of widgets. • Provides a column-based widget layout and layout customization. • Provides a tabular layout design and the ability to view any number of widget layouts.
TOKEN One object that represents another object, either physical or virtual, or an abstract concept.	The GUI uses these types of tokens: a <i>patient</i> token and a <i>record</i> token. A <i>patient</i> token: <ul style="list-style-type: none"> • Consists of patient ID, patient site code, and date/timestamp. • Is tied to an active session that is initiated by the provider upon log in to the system. • Is generated in Grails and encrypted. Data encryption is provided by the Advanced Encryption Standard (AES). A <i>record</i> token is used to retrieve specific details.
WIDGET An element of a GUI that displays information, or provides a specific way for a user to interact with the operating system and application. Widgets include icons, pull-down menus, buttons, selection boxes, progress indicators, on/off checkmarks, scroll bars, windows, window edges (that allow the resizing of a window), toggle buttons, forms, and many other devices for displaying information, and for inviting, accepting, and responding to user actions.	Each widget: <ul style="list-style-type: none"> • Is a mini-application, running within a larger application. • Is a generic container to which provider data, or clinical data, can be ported. • Contains data coming from one source; in this case, from the Representational State Transfer (REST) layer. • Requires a patient token to retrieve data.
SESSION A session is initiated when an authorized user logs in to the CV web application.	During an active session, a user has access to the following CV capabilities: <ul style="list-style-type: none"> • View/Edit user profiles. • Change on-screen user interface themes. • Search for patient records. By default, a CV session will terminate automatically after a period of inactivity.

6.2.1.1.2. Hardware Interfaces

Not applicable. There are no hardware interfaces within the CV system.

6.2.1.1.3. Software Interfaces

Software interfaces are illustrated in [Figure 1](#).

6.2.1.1.4. Communications Interfaces

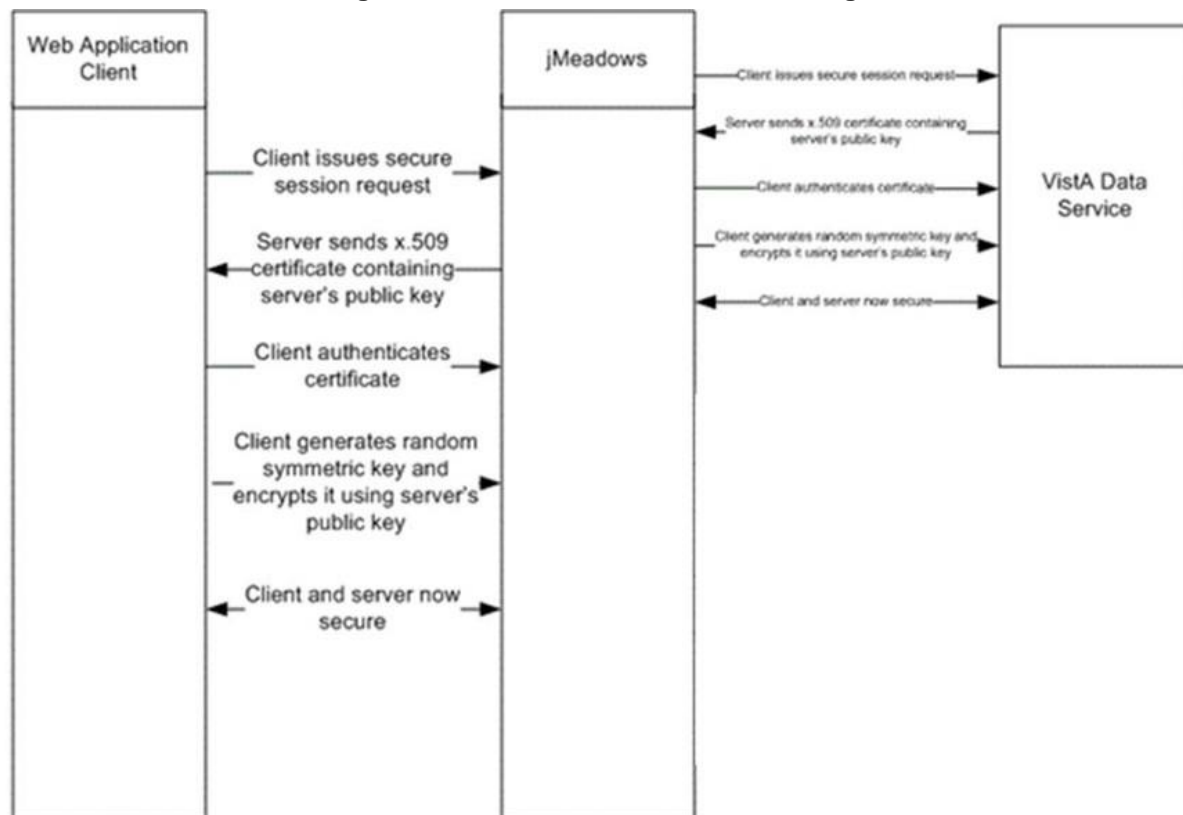
Within the portal pages, the CV system provides an on-screen status indicator:

- **System Status:** The CV system includes a health monitoring service that communicates the status of external systems and services on the Login, Provider, and Patient Portal pages. Please see the *CV 1.5 User Guide*, submitted with this release, for a detailed overview of the CV system status implementation, and GUI status messages.

CV is comprised of the following data services that retrieve clinical data ([Figure 14](#)):

- jMeadows retrieves and aggregates clinical data from multiple source systems
- VistA Data Service retrieves clinical data from all VA VistA systems

Figure 14: Communication Interface Diagram



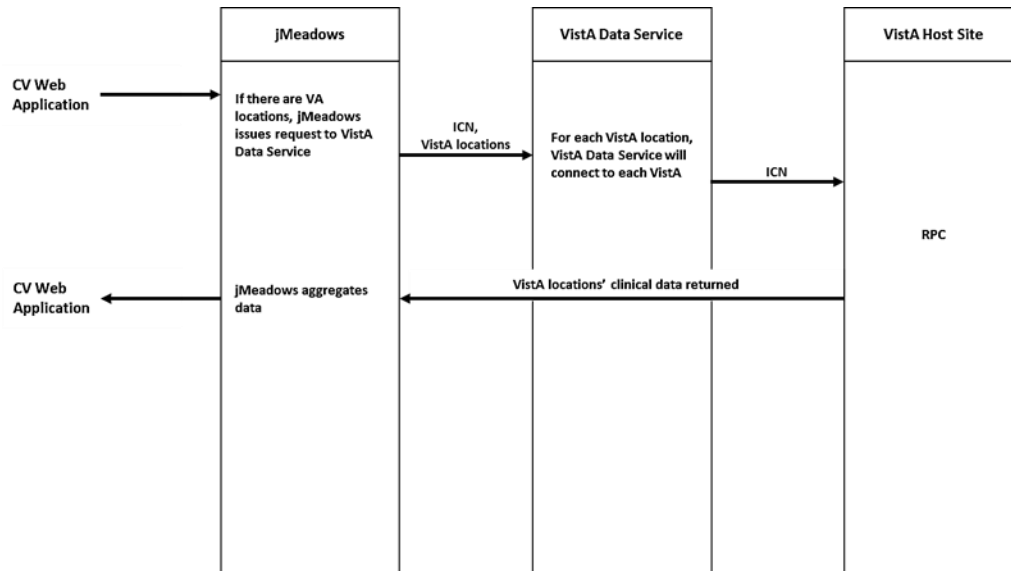
6.2.1.1.4.1. Data Request/Response Sequence

The process of CV requesting patient data from sources, and the resulting response to CV, is as follows:

1. A widget requests data for a clinical domain from the REST service. This request can also be initiated by the CCP user, accessing patient data through the Assigned Patients list
2. The REST service calls a corresponding SOAP service
3. The jMeadows SOAP service layer makes the corresponding clinical domain request from jMeadows
4. jMeadows returns a SOAP response that contains a VistA bean.
5. The VistA bean is mapped to a GUI bean

6. The REST service returns the GUI bean to the widget
7. The GUI bean is communicated back to the GUI, and returns the response to the widget

Figure 15: CV VA Data Retrieval



6.2.1.1.5. Memory Constraints

Not applicable. There are no memory constraints known at this time.

6.2.1.1.6. Special Operations

Special operations, such as disaster recovery, are provided by the AITC data center.

6.2.1.2. Product Features

Please see [Section 2, Background](#), for more information.

6.2.1.3. User Characteristics

Details are provided in [Section 1.2, User Profiles](#).

6.2.1.4. Dependencies and Constraints

CV is dependent on data provided from external data sources, VA MVI, and VistA.

6.2.1.5. External Data Sources

CV is dependent on data provided from VA Master Veteran Index (MVI) and VistA systems.

6.2.2. Specific Requirements

6.2.2.1. Database Repository

Not applicable. There are no special requirements for the database repository at the time of this writing.

6.2.2.2. System Features

Details regarding system features can be found in [Section 2, Background](#).

6.2.2.3. Design Element Tables

Not applicable to Community Viewer.

6.2.2.3.1. Routines (Entry Points)

Not applicable to Community Viewer.

6.2.2.3.2. Templates

Not applicable to Community Viewer.

6.2.2.3.3. Bulletins

Not applicable to Community Viewer.

6.2.2.3.4. Data Entries Affected by the Design

Not applicable to Community Viewer.

6.2.2.3.5. Unique Record(s)

Not applicable to Community Viewer.

6.2.2.3.6. File or Global Size Changes

Not applicable to Community Viewer.

6.2.2.3.7. Mail Groups

Not applicable to Community Viewer.

6.2.2.3.8. Security Keys

Not applicable to Community Viewer.

6.2.2.3.9. Options

Not applicable to Community Viewer.

6.2.2.3.10. Protocols

Not applicable to Community Viewer.

6.2.2.3.11. Remote Procedure Call (RPC)

CV utilizes VistADataService to call VistA RPCs on the local VistA hosts. See the *VistaDataService Interface Control Document (ICD)* for the RPCs that are utilized.

6.2.2.3.12. Constants Defined in Interface

Not applicable to Community Viewer.

6.2.2.3.13. Variables Defined in Interface

Not applicable to Community Viewer.

6.2.2.3.14. Types Defined in Interface

Not applicable to Community Viewer.

6.2.2.3.15. GUI

The GUI for CV is presented as a web page. The pages presented are HTML version 5, and are CSS level 3 compliant. Access to the system has only been verified using IE versions 10 and 11. IE versions below 10 are known to have issues. Other modern browsers, such as Safari and Chrome, may work, but testing for compatibility has not yet been completed.

6.2.2.3.16. GUI Classes

Not applicable to Community Viewer.

6.2.2.3.17. Current Form

Not applicable to Community Viewer.

6.2.2.3.18. Modified Form

Not applicable to Community Viewer.

6.2.2.3.19. Components on Form

Not applicable to Community Viewer.

6.2.2.3.20. Events

Not applicable to Community Viewer.

6.2.2.3.21. Methods

Not applicable to Community Viewer.

6.2.2.3.22. Special References

Not applicable to Community Viewer.

6.2.2.3.23. Class Events

Not applicable to Community Viewer.

6.2.2.3.24. Class Methods

Not applicable to Community Viewer.

6.2.2.3.25. Class Properties

Not applicable to Community Viewer.

6.2.2.3.26. Uses Clause

Not applicable to Community Viewer.

6.2.2.3.27. Forms

Not applicable to Community Viewer.

6.2.2.3.28. Functions

Not applicable to Community Viewer.

6.2.2.3.29. Dialog

Not applicable to Community Viewer.

6.2.2.3.30. Help Frame

Not applicable to Community Viewer.

6.2.2.3.31. HL7 Application Parameter

Not applicable to Community Viewer.

6.2.2.3.32. HL7 Logical Link

Not applicable to Community Viewer.

6.2.2.3.33. COTS Interface

Not applicable to Community Viewer.

6.2.2.4. System Requirements

System requirements for the server environment can be found in the *CV 1.5 Deployment, Installation, Backout and Rollback Guide*, submitted with this release.

System requirements for end users are IE version 10 or 11. A valid PIV card and Access/Verify credentials are also required for VAS users.

6.2.2.5. Access Requirements

Please see [Section 2.3.2, Overview of Special Device Requirements](#), for details regarding access requirements for end users of the CV web application.

6.3. Network Detailed Design

CV utilizes the network infrastructure provided by the AITC.

- Firewall rules exist to allow granular control of the traffic between servers within the system. Explicit rules allow communication only over specific ports
- For the web-facing servers within the AITC, only 443 (HyperText Transfer Protocol Secure (HTTPS)) traffic, directed at the URL communityviewer.va.gov, is allowed to access the web interface. Login and query traffic from the web-facing servers to the internal jMeadows server cluster over 443 (HTTPS), with VA certificates, is allowed

Refer to [Section 4.3, Network Architecture](#) for more information.

6.4. Security and Privacy

6.4.1. Security

The following security design principles are applied to the CV system to ensure that it follows security protocol standards for secured systems, as required by VA Information Security Program, Handbooks 6500 and 6500.5, as well as VA Directive 6500:

- Session security: By the use of secured unique session tokens generated using a 128-bit hash from a secure random number generator for each authenticated user, the system ensures prevention of communication session hijacking. Once the user logs out of the system, the session is immediately destroyed and the session hash can no longer be used.

If in some instance the SessionID were to be obtained, the user cannot paste it as part of a URL string to gain system access.

- Data encryption: The use of Secure Socket Layer (SSL) with Transport Layer Security (TLS) 1.0 ensures that all server communication is encrypted, which limits the ability to perform Man in the Middle (MitM) attacks.
- Database Encryption at Rest: Microsoft SQL Server Transparent Data Encryption (TDE) Encryption level AES 256-bit is used to encrypt Personal Identification Information (PII)/ Protected Health Information (PHI) data at rest.
- Firewall rules exist to allow granular control of the traffic between servers within the system. Explicit rules allow communication only over specific ports.
- For the web-facing servers within the AITC, only 443 (HyperText Transfer Protocol Secure (HTTPS)) traffic, directed at the URL communityviewer.va.gov, is allowed to access the web interface. Login and query traffic from the web-facing servers to the internal jMeadows server cluster over 443 (HTTPS), with VA certificates, is allowed.
- Schema validation: Web Services used in CV employ schema validation. This helps prevent Denial of Service (DoS) attacks by blocking the invocation of eXtensible Markup Language (XML) bombs.

6.4.2. Privacy

The following security and privacy requirements are included in the design of the CV system:

- Consent: Prior to accessing the Login page, users are prompted to agree to a security and legal disclaimer, confirming they are aware that they are accessing a government information system, provided for authorized users only.
- Download and review training documents: After logging in for the first time, and 365 days after the user has completed training, CCPs are prompted to download and review the documents listed below. The user must click each link and download each document in order to access the web application.
 - VA Information Security Awareness
 - VA Electronic Health Records Rules of Behavior
- Training certification: The CCP is required to check the boxes for each of the following statements in order to access the web application:
 - I certify that I have completed and understand the Information Security Awareness training
 - I certify that I have renewed and understand the Electronic Health Records Rules of Behavior
 - I certify that I have completed and understand the HIPAA privacy training provided by my organization
- Print: Printing is disabled in the web application. Print icons are removed from the user interface.
- Copy/Paste: The Copy/Paste feature is disabled. Data must be requested from the VA through standard practices, utilizing existing agreements.

6.4.3. System Audit and Log Capabilities

The CV system has the ability to trace and audit the actions a user executes within the application. CV audits are provided through the use of audit trails and audit logs that offer a backend view of system use, in addition to storing user views of patient data. Audit trails and logs record key activities, including the date and time of an event, patient identifiers, user identifiers, type of action(s) performed, and the access location to show system threads of access to, and the viewing of, patient records.

jMeadows retains user actions within the CV application, as seen in [Table 21](#). Specific events regarding user transactions are also audited or captured in log files, including, but not limited to, user identification, date and time of the event, type of event, success or failure of the event, successful log ons, and the identity of the information system component where the event occurred.

Each time an attempt is made to interface with jMeadows, whether it is a service communicating or a user searching for a patient, the activity is logged and stored in the CV database. The purpose of retention is for traceability; specifically, to see which calls/actions are being made, where, by whom, and when they terminated. Each CV query for data is audited, and has the user ID linked to it.

Table 21: Audit Table Entries

Column Item	Description
auditID	The unique ID of each entry
entryDate	The date at which the audit was entered
startDate	Works with “endDate” to set the date range for the data request
endDate	Works with “startDate” to set the date range for the data request.
systemID	The user’s login site identifier. On the VA side, systemID specifies the VistA host system to which the userID is associated. CCP user entry will be “OP”
userNPI	The user’s National Provider Identifier (NPI)
userID	The user’s identifier. On the VA side, userID is the VistA IEN of the VistA host system that is associated with the user’s Access/Verify codes
userName	The name of the user
patID	The patient’s Electronic Data Interchange Personal Identifier (EDIPI)
category	The query action: such as login or clinical domain data
queryType	The application name
cardID	The VA user’s PIV card
ipAddress	The IP address of the system from which data is accessed
info	Additional information for the user
email	The e-mail address of the user

6.5. Service Oriented Architecture/ESS Detailed Design

The CV system is does not participate in a VA Enterprise Service Bus at this time.

6.5.1. Service Description

Not applicable to Community Viewer.

6.5.2. Service Design

Not applicable to Community Viewer.

6.5.2.1. Introduction

Not applicable to Community Viewer.

6.5.2.1.1. Purpose and Scope of Service

Not applicable to Community Viewer.

6.5.2.1.2. Links to Other Documents

Not applicable to Community Viewer.

6.5.2.2. Service Details

Not applicable to Community Viewer.

6.5.2.2.1. Service Identification

Not applicable to Community Viewer.

6.5.2.2.2. Service Versions

Not applicable to Community Viewer.

6.5.2.2.3. Summary of Design and Platform Details

Not applicable to Community Viewer.

6.5.2.2.3.1. SOA Pattern(s) Implemented

Not applicable to Community Viewer.

6.5.2.2.3.2. COTS Platform vendor names and versions for hosting platform

There are no COTS products in use at the time of this writing.

6.5.2.3. Dependencies

Not applicable to Community Viewer.

6.5.2.4. Service Design Details

Not applicable to Community Viewer.

6.5.2.4.1. Interface Technical Specs

Not applicable to Community Viewer.

6.5.2.4.1.1. Service Invocation Type

Not applicable to Community Viewer.

6.5.2.4.1.2. Service Interface Type

Not applicable to Community Viewer.

6.5.2.4.1.3. Service Name

Not applicable to Community Viewer.

6.5.2.4.1.4. Interface

Not applicable to Community Viewer.

6.5.2.4.1.5. End Points

Not applicable to Community Viewer.

6.5.2.4.1.6. Operations or Methods

Not applicable to Community Viewer.

6.5.2.4.1.7. Message Schemas

Not applicable to Community Viewer.

6.5.2.4.2. Information Model

Not applicable to Community Viewer.

6.5.2.4.2.1. Class Diagram and Description of Entities Involved

Not applicable to Community Viewer.

6.5.2.4.2.2. Mappings from ELDM to Standards Based Schemas

Not applicable to Community Viewer.

6.5.2.4.3. Behavior Model (AKA Use Case Realization)

Not applicable to Community Viewer.

6.5.2.4.3.1. Use Cases (Use Case Model)

Not applicable to Community Viewer.

6.5.2.4.3.2. Interaction Diagrams

Not applicable to Community Viewer.

6.5.2.5. Gap Analysis

Not applicable to Community Viewer.

6.5.2.5.1. Variances from Enterprise Target Architecture

Not applicable to Community Viewer.

6.5.2.5.2. Variances from SLDs

Not applicable to Community Viewer.

6.5.2.5.3. Variances from Standards and Policies

Not applicable to Community Viewer.

6.5.2.5.4. Justification for Exceptions and Mitigation

Not applicable to Community Viewer.

7. External System Interface Design

Not applicable to Community Viewer.

7.1. Interface Architecture

Not applicable to Community Viewer.

7.2. Interface Detailed Design

Not applicable to Community Viewer.

8. Human-Machine Interface

Refer to the *CV 1.5 User Guide*, submitted with this release.

8.1. Interface Design Rules

Not applicable to Community Viewer.

8.2. Inputs

Refer to the *CV 1.5 User Guide*, submitted with this release.

8.3. Outputs

Not applicable. There are no known outputs in the CV web application at the time of this writing.

8.4. Navigation Hierarchy

Refer to the *CV 1.5 User Guide*, submitted with this release.

9. Quality of Service (QoS) (Health Monitor) Design

The Health Monitor examines the availability of services that connect CV to data sources and other outside systems. Status changes within the CV environment are written to the CV database, and are displayed within the CV web application. System health and status notifications are available in near real-time to CV users through the Login screen and Home page.

The Health Monitor examines the availability of the following services:

- MVI
- VistA Data Service

- jMeadows Data Service

System status is displayed within the CV web application for the systems noted above, with the exception of the jMeadows Data Service. System status events for the jMeadows Data Service are logged to the CV database and included in an automated e-mail notification, but are not provided through the user interface.

The QoS service is a standalone application (service) within the CV system that monitors connected systems and data sources, and record system status changes. Additional properties of the application include:

- The application runs as a service within the web application container alongside the jMeadows Data Service. The service does not require administrative privileges at the operating system level.
- The service is a closed service, and is not exposed to users of the CV system.

9.1. System Status Checks

System status checks are performed as follows:

1. The Health Monitor pings the monitored services every five minutes.
2. The Health Monitor receives a system status from each monitored service.
3. System status events are written to the QOS_LOGS table, within the CV database.
4. The Health Monitor sends an automated e-mail notification every 12 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the twelve-hour timer is reset. The next e-mail is generated after twelve hours, if no further system status changes are detected.
5. The jMeadows Data Service pings the CV database every two minutes for status checks.
6. The jMeadows Data Service stores the data returned from the CV database in an internal cache, the jMeadows Data Service cache.
7. When a user accesses the CV Login page, the CV application requests and receives system status data from the jMeadows Data Service cache.
8. During active user sessions, the CV application requests system status data from the jMeadows Data Service cache every five minutes. Current system status is retrieved from the cache, and sent to the CV GUI.

[Figure 16](#) provides an overview of the system monitoring process.

[illegible]

When all monitored systems are connected and available, the System Status will read *CV data sources available* on the Login and portal pages.

[Table 22](#) summarizes the status messages displayed in the CV GUI when the monitored service or system is detected as *unavailable*.

Notification	Meaning
MVI	The VA Patient Identity Service is unavailable. VA data may not display.
VistA Data Service	The VistA data service is unavailable. VA data may not display.
CV Health Monitor Service	System status is unavailable. NOTE: This indicates that CV's Health Monitor service is unable to retrieve system status information. This is not an indicator that data sources are unavailable to CV.

When enabled, CV can send automatic system status e-mail notifications, if the SMTP service is available in the environment where CV is deployed. The e-mail recipient is configured in the

appconfig-production.properties file, where production represents the environment. The file is contained within the application's .war file.

E-mail notification is enabled by default. Messages are generated and sent every twelve hours, if changes in system status are not detected during the twelve-hour period. If a status change is detected, a notification is generated, an e-mail is sent immediately, and the twelve-hour timer is reset. The next e-mail is generated after twelve hours if no further system status changes are detected.

9.3.1. Sample E-mail Notification

The CV installations are configured to provide automatic QoS status messages via e-mail. Sample notifications are listed in [Table 23](#).

Table 23: Sample Heath Monitor E-mail Notification

Notification	Meaning
No errors detected.	All monitored systems and services are available.
Service: MVIService Status: ERROR Message: Failed to complete service test.	MVI Service may be offline or unavailable.
Service: VistaDataService Status: ERROR Message: javax.xml.ws.soap.SOAPFaultException: java.io.IOException: Async IO operation failed (1), reason: RC: 55 The specified network resource or device is no longer available.	VistA Data Service may be offline or unavailable.
Service: JMeadowsDataService Status: ERROR Message: Failed to complete service test.	jMeadows may be unavailable. Users may not be unable to log in and data may not display.

9.4. Database Integration

The following elements related to the health monitor are integrated within the CV (SQL Server) database:

- System status table: The QOS_LOGS table has been added to the CV database to record health status events. All monitoring results are retained in the QOS_LOGS table.
- SQL service account: The cvuser account has been created to be utilized only by the CV application.

[Table 24](#) summarizes the permissions for the cvuser service account.

Table 24: cvuser Service Account Permissions

Database Element	Permissions		
	r (read)	w (write)	x (execute)
QOS_LOGS (Table)	X	X	
<i>Encrypted Stored Procedures</i>			

Database Element			
addQoSReport			X
getQoSShareEndPoints			X
getRecentQOSServiceErrors			X

9.5. Required Permissions and Roles

No additional permissions or roles are required at the database level for the implementation of the Health Monitor. Only approved/authorized System Administrators have access to the CV database, and the database tables that record system status events.

No additional user roles are required to implement the Health Monitor in the CV GUI.

9.6. Modifications to External Systems and Services

This section provides an overview of the modifications made to external systems and services in order to implement the Health Monitor.

9.6.1. jMeadows Data Service

Within the Health Monitor, an interface within the jMeadows Data Service enables the return of status updates to the CV application. System status data is returned from queries to the QOS_LOGS table from the CV database.

9.6.2. Middleware Services

In order to implement the Health Monitor, the Health Monitor application (service) is deployed to the services cluster on the same server where the jMeadows Data Service resides.

9.7. GUI Status Message Display

Health Monitor status messages are provided on the Login screen and the Home page, on both the Provider and Patient Portals:

- When all monitored systems and services are online and connected, a green icon appears next to the message *CV data sources available*.
- When one or more monitored systems or services are offline or unavailable, a yellow icon appears next to the message *CV is having problems*. The message also indicates which service is offline, and provides an e-mail address for the Help Desk.
- When CV's Health Monitor service is unable to retrieve system status information, a red icon appears next to the message *System status is unavailable*. This is not an indicator that data sources are unavailable to CV.

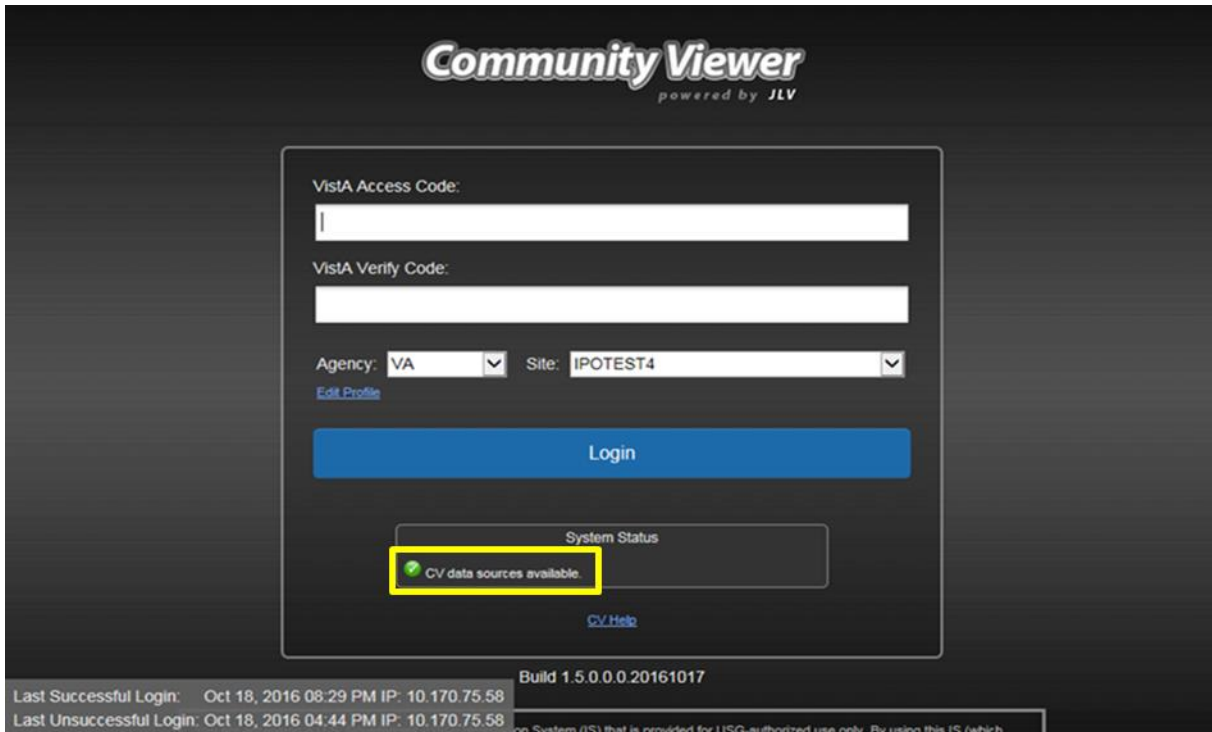
9.7.1. Sample System Status Messages

The figures in the following subsections depict various system status messages that may appear in the CV web application GUI.

9.7.1.1. Services Available System Status Messages

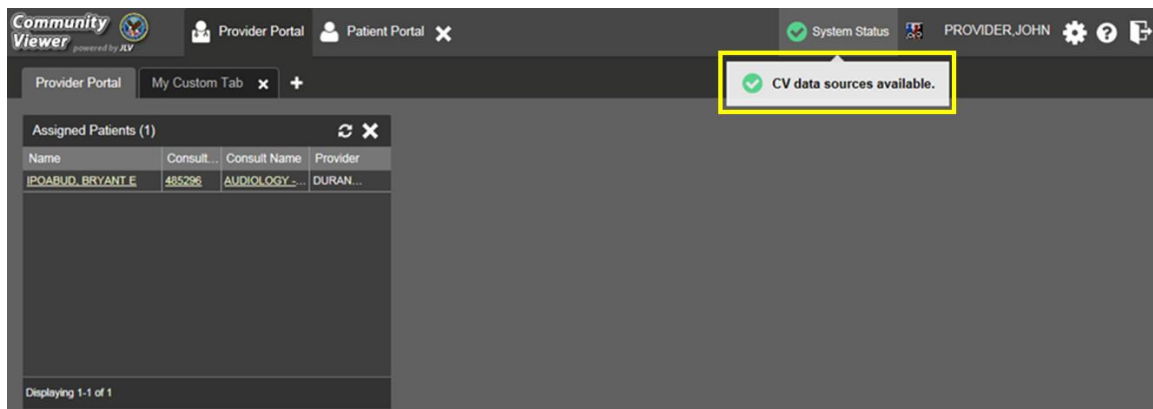
The detail highlighted within the yellow border in [Figure 17](#) depicts the *CV data sources available* message, as seen on the Login page. This message indicates that all monitored services are available.

Figure 17: Services Available Status Message – Login Page



The detail highlighted within the yellow border in [Figure 18](#) displays the sample status message seen on the Provider Portal page when all monitored services are available.

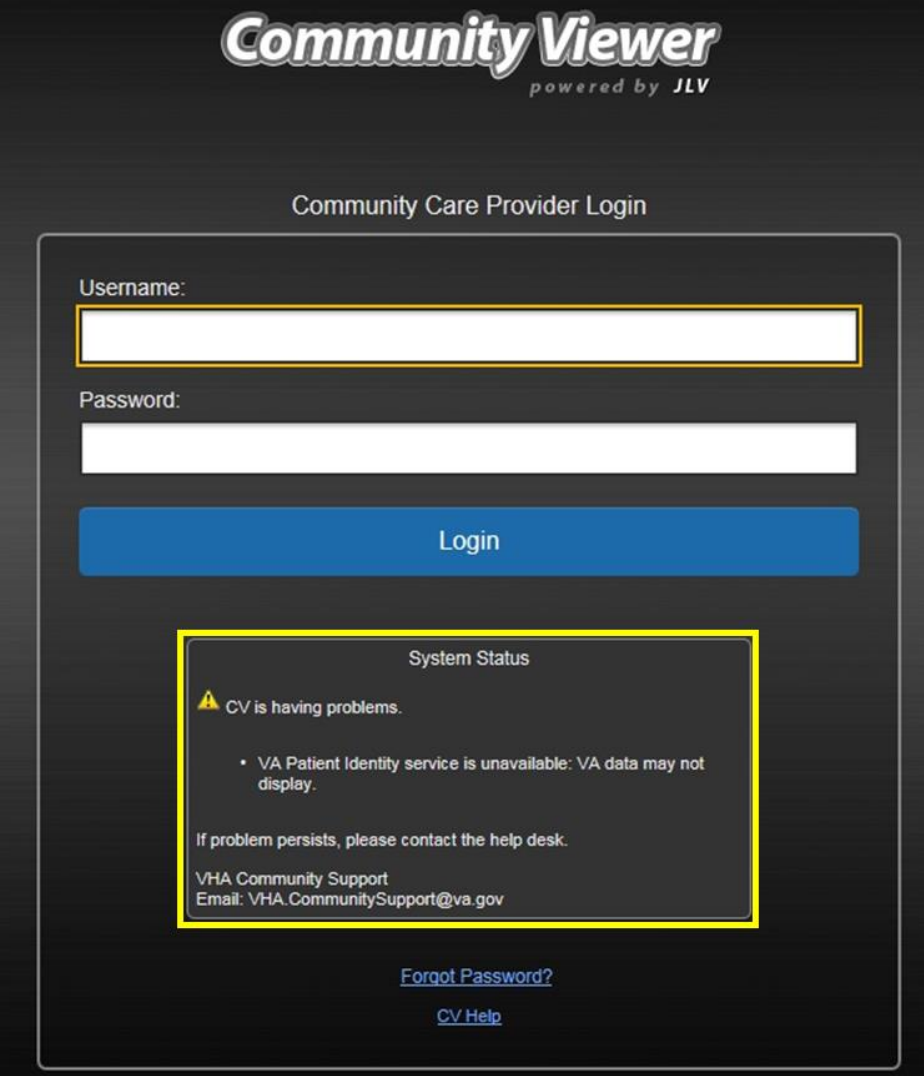
Figure 18: Services Available Status Message – Portal Page



9.7.1.2. Services Unavailable System Status Messages

The detail highlighted within the yellow border in [Figure 19](#) shows the *Patient Lookup service is unavailable: Unable to search for a patient* message, as seen on the Login page. This message indicates that CV is unable to connect to MVI.

Figure 19: Patient Lookup Service Unavailable – Login Page



The screenshot displays the 'Community Viewer' login interface, powered by JLV. The title 'Community Care Provider Login' is centered above the login fields. There are two input fields: 'Username:' and 'Password:'. Below these is a blue 'Login' button. A yellow-bordered box highlights a 'System Status' message. The message states: 'CV is having problems.' followed by a bullet point: 'VA Patient Identity service is unavailable: VA data may not display.' It also includes the instruction 'If problem persists, please contact the help desk.' and contact information for 'VHA Community Support' with the email 'VHA.CommunitySupport@va.gov'. At the bottom of the login area, there are links for 'Forgot Password?' and 'CV Help'.

Community Viewer
powered by JLV

Community Care Provider Login

Username:

Password:

Login

System Status

⚠ CV is having problems.

- VA Patient Identity service is unavailable: VA data may not display.

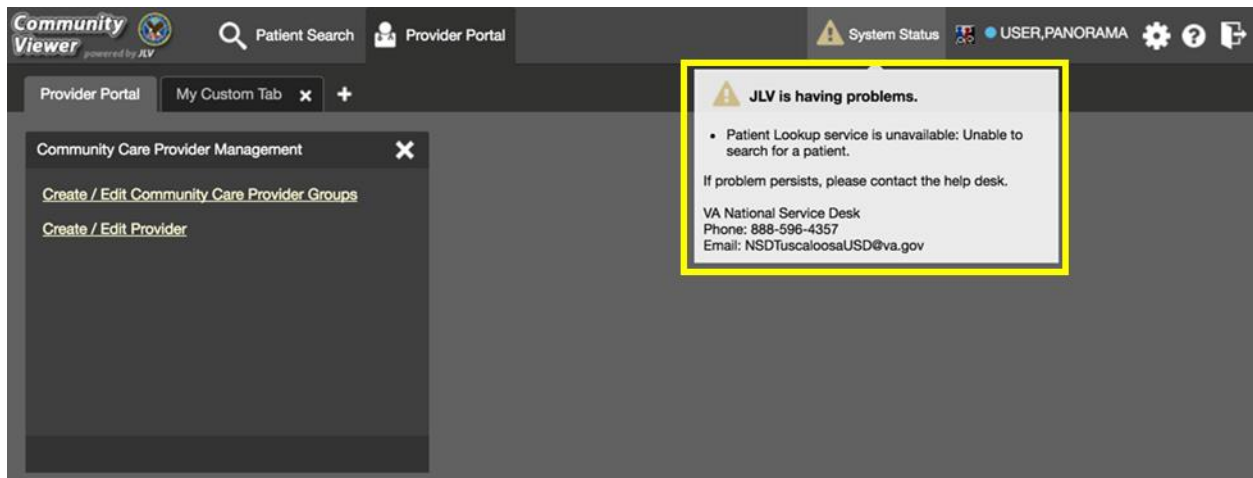
If problem persists, please contact the help desk.

VHA Community Support
Email: VHA.CommunitySupport@va.gov

[Forgot Password?](#)
[CV Help](#)

The detail highlighted within the yellow border in [Figure 20](#) displays the *Patient Lookup service is unavailable: Unable to search for a patient* message, as seen on the Provider Portal page. This message indicates that CV is unable to connect to MVI.

Figure 20: Patient Lookup Service Unavailable – Portal Page



9.8. Security Impact

There is no associated security impact with the implementation of the Health Monitor. The service does not allow for user input, or contain write-back capability to any database or external system. System status messages, both seen in the GUI and within the generated e-mail message, are provided to the user as read-only status notifications, with no required query validation.

Only approved/authorized System Administrators have access to the CV database and the database tables that record health monitor status updates. No additional permissions or roles are required at the application level, the operating system level, or the database level for the design of the Health Monitor, as described in this document.

10. Attachment A – Approval Signatures

NOTE: The Business Sponsor and Project Manager are required to sign.

Michelle Rowe, Business Sponsor

Date

Betsy Green, Project Manager

Date

A. Appendix - Additional Information

A.1. Identification of Technology and Standards

Please reference Sections [4.2.1, Client-Side Development Technologies](#), and [4.2.2, Server-Side Development Technologies](#), for the technology leveraged as part of the CV application.

A.2. Constraining Policies, Directives and Procedures

The CV web application is constrained by the Health Insurance Portability and Accountability Act (HIPAA).

A.3. Requirements Traceability Matrix

Please see the *CLIN 0003AF CV 1.5 Requirements Traceability (RTM)* document, submitted with this release.

A.4. Packaging and Installation

Please reference the *CV 1.5 Deployment, Installation, Backout and Rollback Guide* for application installation instructions for the CV software into the server environment.

A.5. Design Metrics

Design details are referenced throughout this System Design Document.

B. Appendix – Acronyms and Abbreviations

[Table 25](#) lists the acronyms and abbreviations used throughout this document, and their descriptions.

Table 25: Acronyms and Abbreviations

Acronym	Definition
A&A	Access and Authorization
AES	Advanced Encryption Standard
AITC	Austin Information Technology Center
AJAX	Asynchronous JavaScript and XML
ANR	Automated Notification Reporting
API	Application Program Interface
CCP	Community Care Provider
CCPM	Community Care Provider Management
COTS	Commercial-Off-the-Shelf
CSS	Cascading Style Sheets
CV	Community Viewer
DB	Database
DOM	Document Object Model
DoS	Denial of Service
EHR	Electronic Health Records
EMR	Electronic Medical Record
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Secure
ID	Identification
IE	Internet Explorer
IP	Internet Protocol
IT	Information Technology
JDBC	Java Database Connectivity
JLV	Joint Legacy Viewer
JSON	JavaScript Object Notation
MitM	Man in the Middle
MMC	Microsoft Management Console
MVC	Model-View-Controller

Acronym	Definition
MVI	Master Veteran Index
OIT	Office of Information and Technology
PHI	Protected Health Information
PII	Personal Identification Information
PIV	Personal Identification Verification
QoS	Quality of Service
REST	Representational State Transfer
RTM	Requirements Traceability Matrix
SDD	System Design Document
SGML	Standard Generalized Markup Language
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Objects Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSMS	SQL Server Management Studio
SSP	System Security Plan
TDE	Transport Data Encryption
TLS	Transport Layer Security
UCP	Utility Control Point
UI	User Interface
VA	Veterans Administration
VAS	VA Administrative Staff
VistA	Veterans Information Systems and Technology Architecture
XML	eXtensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformations