

Joint Longitudinal Viewer (JLV) 2.10
Veterans Affairs Enterprise Cloud
Production Operations Manual (POM)



October 2021
Version 1.0

Department of Veterans Affairs

Revision History

Date	Version	Description	Author
08/13/2021	0.1	Initial draft of document from last approved	Liberty ITS
08/24/2021	0.2	Updated after VA review	Liberty ITS
08/31/2021	0.3	Updated for adjudication meeting	Liberty ITS
10/12/2021	1.0	Final document for signatures	Liberty ITS

Table of Contents

1. Introduction	1
2. Routine Operations	2
2.1. Administrative Procedures	2
2.1.1. System Startup.....	2
2.1.1.1. System Startup from Emergency Shutdown	4
2.1.2. System Shutdown.....	5
2.1.2.1. The Amazon Command Line Interface (CLI) Emergency System Shutdown	5
2.1.3. Backup and Restore	5
2.1.3.1. Backup Procedures	5
2.1.3.2. Restore Procedures.....	6
2.1.3.3. Storage and Rotation	6
2.2. Security/Identity Management.....	6
2.2.1. Identity Management	8
2.2.2. Access Control.....	8
2.3. User Notifications	9
2.3.1. User Notification Points of Contact	9
2.3.2. JLV QoS Mail Groups	11
2.3.3. Scheduled Downtime Notifications.....	12
2.3.3.1. Service Now (SNOW) Process.....	15
2.3.3.2. Patch Release Notification E-mail (Example)	16
2.3.4. Unscheduled Outage Notifications	16
2.3.4.1. Initial Response to Issues Within 30 Minutes of Alert	16
2.3.4.1.1. Initial Outage Response Notification E-Mail (Example).....	17
2.3.4.2. Outage Escalation to External Teams	17
2.3.4.2.1. Outage Escalation to External Teams E-Mail (Example)	17
2.3.4.2.2. Outage Update E-Mail (Example)	18
2.3.5. Announcement Banners	19
2.3.5.1. Placing Announcement Banners	21
2.3.5.2. Removing Announcement Banners.....	22
2.3.5.2.1. Manual Removal	22
2.3.5.2.2. Automatic Expiration	22
2.3.5.3. Announcement Banner Extensions.....	22
2.4. System Monitoring, Reporting, and Tools	23
2.4.1. Dataflow Diagram.....	23
2.4.2. Availability Monitoring	23
2.4.2.1. Domain-Level Availability Monitoring	25
2.4.3. Performance/Capacity Monitoring	26

2.4.4.	Critical Metrics	26
2.5.	Routine Updates, Extracts, and Purges	27
2.5.1.	Routine Updates.....	27
2.5.2.	Extracts	27
2.5.3.	Purges	27
2.6.	Scheduled Maintenance	27
2.7.	Unscheduled Outage Triage Process	28
2.7.1.	Outage Triage Timeline	29
2.7.2.	Escalation	29
2.7.3.	Issue Resolution and After Action	30
2.8.	Capacity Planning	30
2.8.1.	Initial Capacity Plan	30
3.	Exception Handling.....	30
3.1.	Routine Errors	31
3.1.1.	Security Errors	31
3.1.2.	Timeouts	31
3.1.2.1.	Application Timeout	31
3.1.2.2.	Connection Errors	32
3.1.3.	Concurrency	33
3.2.	Significant Errors	33
3.2.1.	Application Error Logs	33
3.2.2.	Application Error Codes and Descriptions	34
3.2.3.	Services Infrastructure Errors	35
3.2.3.1.	DB	35
3.2.3.2.	Web Server	36
3.2.3.3.	Application Server	36
3.2.3.4.	Network.....	36
3.2.3.5.	Authentication and Authorization (A&A).....	36
3.2.3.6.	Logical and Physical Descriptions	37
3.3.	Dependent System(s) and Services.....	37
3.4.	Troubleshooting.....	37
3.5.	System Recovery	38
3.5.1.	Restart After an Unscheduled System Interruption	38
3.5.2.	Restart after DB Restore	38
3.5.3.	Backout Procedures	38
3.5.4.	Rollback Procedures	38
4.	Operations and Maintenance Responsibilities.....	38
Appendix A.	Approval Signatures.....	41

Appendix B. Acronyms and Abbreviations	42
Statement on Auditing Standards-70	44

Table of Figures

Figure 1: The JLV Patient Portal	1
Figure 2: The Database Details Window	6
Figure 3: Mockup of Regularly Scheduled Downtimes.....	12
Figure 4: Scheduled Downtime Notification Process	15
Figure 5: Service Now (SNOW) Process.....	16
Figure 6: User-facing Banner on the JLV Login Page.....	21
Figure 7: System Status Check Sequence	24
Figure 8: System Status Message on the JLV Login Page.....	25
Figure 9: System Status Message on the Patient Portal Page	25
Figure 10: Connection Status Details.....	26
Figure 11: Patching Process for VA and DOD Components.....	27
Figure 12: Scheduled Downtime and Unscheduled Outage Overview.....	28
Figure 13: Outage Event Activities and Timeline.....	29
Figure 14: Session Timeout Notification	31
Figure 15: Session Timeout (SSOi)	32
Figure 16: Connection Error	32
Figure 17: jMeadows Log Output.....	34
Figure 18: JLV Architecture and Components	35
Figure 19: Audit Log	36

Table of Tables

Table 1: User Authentication and Login Overview	8
Table 2: Access Control Design.....	9
Table 3: JLV Scheduled Downtime Notification List (VA Stakeholders).....	9
Table 4: Announcement Banner Content for Maintenance Events Impacting End Users	20
Table 5: Database Table Entry Prior to Manual Removal	22
Table 6: Database Table Entry After Manual Removal.....	22
Table 7: Database Table Entry for a Planned Maintenance Announcement Banner	22
Table 8: Database Table Entry as Initially Posted	23
Table 9: Database Table Entry After a Date Extension Update.....	23
Table 10: Services Monitored by QoS.....	23
Table 11: Response Time Log Location	33
Table 12: JLV Dependent Systems and Services.....	37
Table 13: Operations and Maintenance Responsibility Matrix.....	38
Table 14: Acronyms and Abbreviations	42

1. Introduction

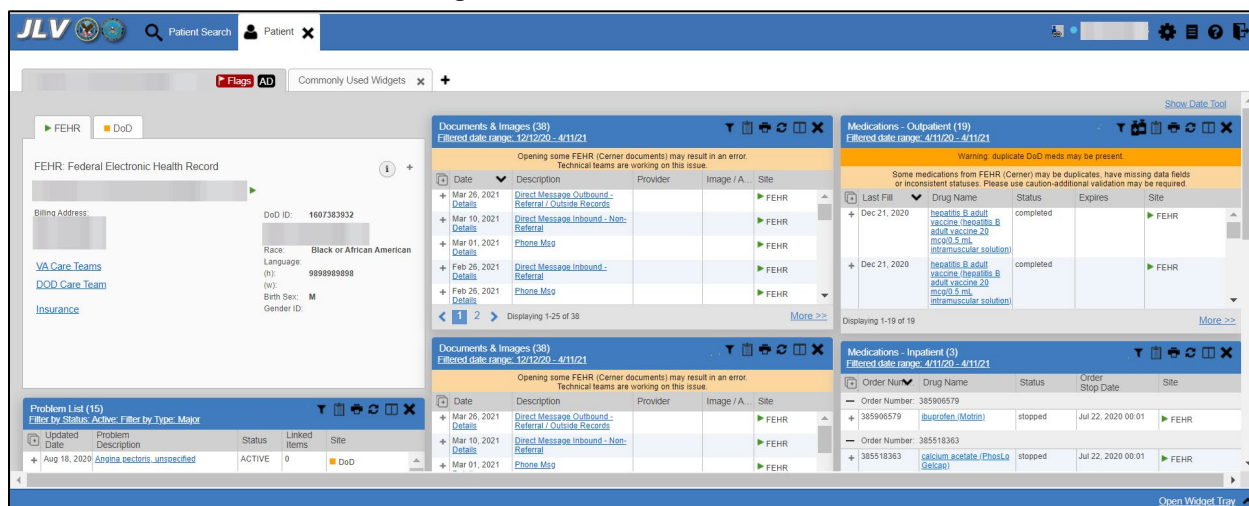
Born from a joint Department of Defense (DOD)–Department of Veterans Affairs (VA) venture called JANUS, Joint Longitudinal Viewer (JLV) was directed by the Secretary of the VA and the Secretary of Defense in early 2013 to further support interoperability between the two departments. JLV is a centrally hosted, Java-based web application managed as two similar but distinct products - one tailored for DoD use and another tailored for VA use. Each JLV product is deployed to its respective DoD and VA hosting environments. Although separately hosted, the respective applications use several shared data services. The browser-based Graphical User Interface (GUI) provides an integrated, read-only view of Electronic Health Record (EHR) data from the VA, DOD, and community partners within a single application.

JLV eliminates the need for VA and DOD clinicians to access disparate viewers. The GUI retrieves clinical data from several native data sources and systems, then presents it to the user via widgets, each corresponding to a clinical data domain.

Users can create and personalize tabs, drag, and drop widgets onto tabs, sort data within a widget's columns, set date filters, and expand a widget for a detailed view of patient information. Within each widget, a blue circle indicates VA data; an orange square indicates DOD data; a purple hexagon indicates community partner data; and a green triangle indicates Cerner Millennium Federal Electronic Health Record (FEHR) data.

[Figure 1](#) depicts the main application window, comprised of the Patient Portal (details displayed) and widgets. The widgets retrieve clinical data from sources in real time, displaying them in a unified, chronological view.

Figure 1: The JLV Patient Portal



JLV is being installed in the VAEC using Fargate Containers. The Elastic Container Registry stores and manages the container images.

Docker technology is used to create file images. Docker is a set of Platforms as a Service (PAAS) products that use OS-level virtualization to deliver software in packages called containers

When a docker file is built the configuration, instructions are executed, and the artifacts are installed into the image. This activity creates the container.

Docker files are packaged up and sent to Elastic Container Registry (ECR). When changes are made to individual containers a new docker file is created, and the new file is sent to ECR, where a new container is created to replace the outdated container.

- JLV Fargate Cluster is a regional grouping of containers which together form the JLV application.
 - there is a setting in the cluster which describes the number of containers that are needed at any one time.
 - Anytime one of the containers crashes this service will automatically create a new container to ensure the desired number of containers is maintained.
- Each container is described by the task definition associated with each specific container.
- The JLV Cluster definition is stored in the ECR.
 - The ECR stores and manage container images.

The JLV database has migrated to VAEC and is using Amazon Relational Database Service (RDS). RDS provides automated administration tasks such as hardware provisioning, database setup, patching and backups.

2. Routine Operations

System administrators perform routine operations to maintain the configuration, upkeep, and reliable operation of computer systems. System administrators also ensure that the performance, uptime, resources, and security of the systems meet the needs of the end users.

2.1. Administrative Procedures

JLV is being installed in the VAEC using Fargate Containers. The ECR stores and manages the container images.

Docker technology is used to create file images. Docker is a set of Platforms as a Service (PAAS) product that use OS-level virtualization to deliver software in packages called containers.

When a docker file is built, the configuration instructions are executed, and the artifacts are installed into the image. This activity creates the container image.

Docker images are packaged and sent to ECR. When changes are made to individual services, a new docker image is created, and the new image is sent to ECR, where a new container is created to replace the outdated container.

2.1.1. System Startup

1. Start the JLV RDS database (DB) instance.
 - a. The DB instances processes are configured to run as system services and are automatically started with the DB instances.
 - b. Validation:

- i. Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the DB instances are up and operational.
2. Start the Veterans Information Systems and Technology Architecture (VistA) Data Service (VDS) container.
 - a. The service processes are configured to run as system services and are automatically started with the VDS container.
 - b. Validation:
 - i. Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the VDS instances are up and operational.
 - ii. Review each of the Tomcat-managed VDS server application logs for connection and/or application errors.
3. Start the JLV jMeadows container.
 - a. The service processes are configured to run as system services and are automatically started with the task.
 - b. Validation:
 - i. Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging into the application confirms that the jMeadows containers are up and operational.
 - ii. Review each of the Tomcat-managed jMeadows container application logs for connection and/or application errors.
4. Start the Electronic Health Record Modernization (EHRM) Service containers.
 - a. The service processes are configured to run as system services and are automatically started with the EHRM Service instance.
 - b. Validation:
 - i. Startup is validated through the successful smoke test of the application; loading Cerner Millennium FEHR data confirms the EHRM Service instances are up and operational.
 - ii. Review each of the Tomcat-managed EHRM Service application logs for connection and/or application errors.
5. Start the Report Builder container
 - a. The service processes are configured to run as system services and are automatically started with the instances.
 - b. Validation:
 - i. Startup is validated through the successful smoke test of the application; loading a document into Report Builder and testing the print feature confirms that the Report Builder servers are up and operational
 - ii. Review each of the Tomcat-managed Report Builder instance application logs for connection and/or application errors
6. Start the JLV front-end web container and the Apache Single Sign-On Internal (SSOi) container

- a. The service processes are configured to run as system services and are automatically started with the instances
- b. Validation:
 - i. Startup is validated through the successful smoke test of the application; loading the JLV Login page and logging in to the application confirms that the dependent backend JLV systems are up and operational
 - ii. Review each Apache-managed web server for connection and/or application errors
- c. Access and launch the JLV Universal Resource Locator (URL), also referred to as the Global Traffic Manager (GTM) URL REDACTED in a web browser
- d. Log in as a Veterans Health Administration (VHA) user with a VHA test account:
 - i. Verify that the JLV Login page displays as expected and that the system status indicates services are online and connected
- e. Log in as a Veterans Benefits Administration (VBA) Compensation and Pension Record Interchange (CAPRI)-Claims user with a VBA test account:
 - i. Verify that the JLV Login page displays as expected and that the system status indicates services are online and connected

2.1.1.1. System Startup from Emergency Shutdown

The VAEC infrastructure is hosted by AWS GovCloud, a cloud service provider. The AWS GovCloud platform is used to provide a variety of hosting environments to suit a variety of needs. AWS GovCloud can support applications categorized up to High as rated in accordance with Federal Information Processing Standard (FIPS) 199. VA applications available to the public are hosted in AWS GovCloud.

A dedicated private data link (AWS Direct Connect) provides all connectivity for VA resources communicating to the environment. Virtual Private Clouds (VPCs) wrap the applications within AWS GovCloud to encapsulate network access. Access from the applications to VA internal resources such as Identity, Credential, and Access Management (ICAM) and Active Directory (AD) Services are conducted over the encrypted private data link to the VA Network.

VAEC is in two regions with three Availability Zones designed to allow U.S. government agencies, contractors, and customers to move sensitive workloads into the cloud for addressing specific regulatory and compliance requirements. AWS GovCloud does not manage logical access controls within the VAEC system boundary. VAEC offers the same level of security as other VA physical technology centers and supports existing VA security controls and certification requirements such as FISMA, Health Insurance Portability and Accountability Act of 1996 (HIPAA), HITECH, SAS-70, ISO 27001, FIPS 140-2 compliant end points, and PCI DS

- JLV Fargate Cluster is a regional grouping of containers which together form the JLV application.
 - there is a setting in the cluster which describes the number of containers that are needed at any one time.
 - Anytime one of the containers crashes this service will automatically create a new container to ensure the desired number of containers is maintained.

- Each container is described by the task definition associated with each specific container.
- The JLV Cluster definition is stored in the Elastic Container Registry (ECR)

The ECR stores and manage container image. If there is a power outage or other abrupt termination of the server operating systems, start up the servers as detailed in [System Startup](#) and allow the operating system to check the disks for corruption. Consult with IO to ensure that the DB successfully recovers.

Enable SSOi Bypass on Apache Server

Note: Bypass has not been completed yet, but the system will have the capability.

2.1.2. System Shutdown

The application is shut down by stopping the running instances of the JLV containers and stopping the RDS JLV instance.

2.1.2.1. The Amazon Command Line Interface (CLI) Emergency System Shutdown

In an emergency, services can be stopped by accessing the Amazon Command Line Interface (CLI) and running the following command:

```
aws ecs update-service --service <service name> --desired-count 0
```

2.1.3. Backup and Restore

JLV Operations manages the platform and installation of both the operating systems and the baseline installation of MS SQL Server in the VA Production environments.

The active transaction log (known as the tail of the log) must be backed up under the full or bulk-logged recovery model before a DB can be restored in SSMS. RDS backs up and manages the keys for the encrypted database.

2.1.3.1. Backup Procedures

The Production VAEC RDS Database is automatically backed up daily and stored in AWS-managed S3. These backups have a seven-day retention, meaning that they are kept for seven days until deleted.

A detailed list of the instances referenced throughout this POM can be found in the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

Using the AWS console or Command Line Interface (CLI), the VAEC RDS production database instance can be restored to any specific time during the backup retention period.

If the database instance does not have automated backups enabled, it can be enabled by setting the backup retention period to a positive nonzero value. Once the automated backup is enabled, the RDS instance and database is taken offline, and backup is immediately created.

To enable automated backups immediately:

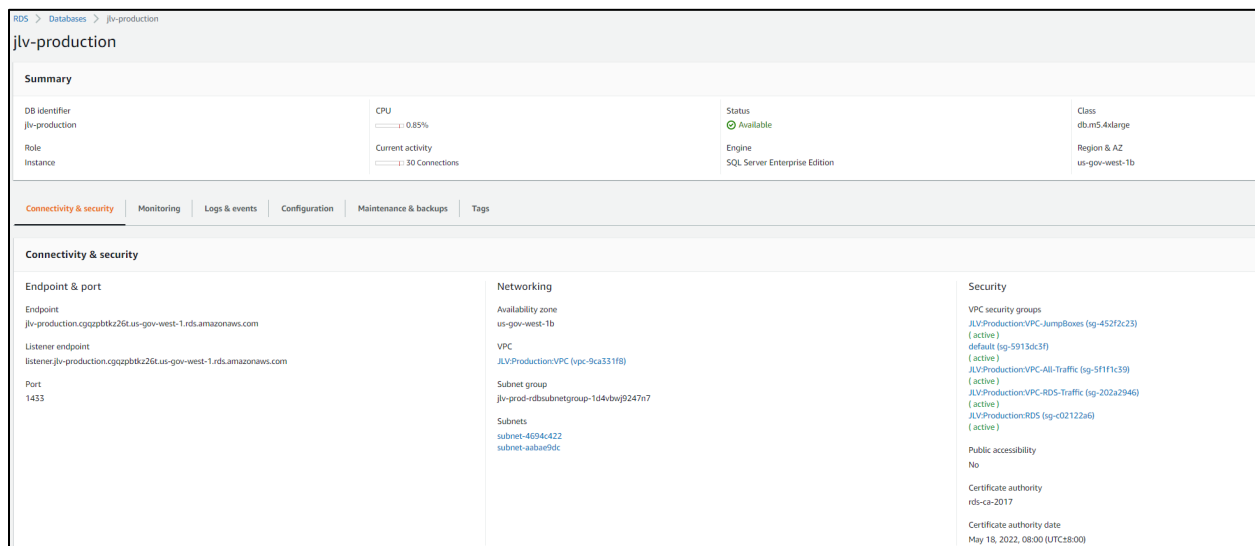
1. Sign into the AWS Management Console and open the Amazon RDS Console:
REDACTED
2. Choose Databases, then choose the JLV database instance to modify.
3. Choose Modify. The Modify DB instance page opens.
4. Choose a positive nonzero value for the backup retention period, for example 7 days.
5. Choose Continue, apply immediately and on the confirmation page, choose Modify DB instance to save changes made and enable the automated backups.

2.1.3.2. Restore Procedures

When restoring the VAEC RDS DB instance:

1. Choose the default VPC security group or apply a custom VPC security group to the VAEC RDS DB instance.
2. Choose Automated backups in the Amazon RDS console to see the latest restorable time for the VAEC RDS DB instance.
3. Choose Restore Snapshot and select the latest restorable time.

Figure 2: The Database Details Window



Backup Testing

Backups of the Production VAEC DBs are done on the AWS RDS console. Backups are automatically taken daily with a seven-day retention.

2.1.3.3. Storage and Rotation

JLV Operations ensures the system is operating properly, with daily inspections of JLV QoS logs, system notifications, and frequent systems checks.

2.2. Security/Identity Management

JLV restricts access to the GUI to authorized users within the VA. Users access JLV via a URL.

Users are authenticated through the SSOi system, which allows them to link their Personal Identity Verification (PIV) card to their VistA account using their Access and Verify codes. Once linked, users may log in directly to the Patient Portal, with just their PIV and PIN and without their Access and Verify codes. When authenticating users with SSOi, JLV attempts to retrieve agency and site profile information from the SSOi system. When enabled, users are authenticated through SSOi (default).

SSOi Bypass is used as a failover authentication mechanism if Identity and Access Management's (IAM) SSOi services are unavailable. If SSOi Bypass (failover) is enabled, users must present their PIV card and Personal Identification Number (PIN) or their Windows authentication credentials before gaining access to the JLV Login page, where they will need to enter their Access and Verify codes.

PIV exempt users are prompted for their Windows username and password before continuing to the JLV Login page. If a user selects Windows authentication and is not PIV exempt, the authentication fails and the SSOi Bypass message, *"Access denied. You are not an authorized user."* appears.

JLV requires that VA users provide the following credentials at the Login page:

- **VHA/Clinical Users:** The user's local existing VistA Access and Verify codes
- **VBA/Benefits Users:** The user's existing National Claims VistA Access and Verify codes

Access control and authentication takes place before JLV displays any data. The user is authenticated to their host EHR system, granting them access to the presentation layer. jMeadows retrieves the user's profile information from the JLV DB based on their credentials. The user's default host location, custom widget layout, and other user data are returned. See [Access Control](#) for more information. [Table 1](#) provides a user authentication and login overview.

Table 1: User Authentication and Login Overview

User	Context Root	Authentication Overview
VBA/ CAPRI- Claims	/JLV	<p>The VA SSOi system is enabled for CAPRI users:</p> <ul style="list-style-type: none"> • The user is prompted to enter their PIV and PIN • CAPRI-Claims users are authenticated through SSOi • If the user's PIV is not linked to Claims (e.g., first time login), the user is prompted to identify their home site and will be asked to provide their Access/Verify login credentials on the Login page • If the user has linked their PIV to their home site (e.g., subsequent logins), JLV validates their credentials against their local VA Claims system <p>If SSOi Bypass is enabled (failover):</p> <ul style="list-style-type: none"> • VBA/CAPRI-Claims users are authenticated through JLV using their PIV and PIN • If a user is PIV exempt, the user is prompted for their Windows username and password • JLV receives the VBA/CAPRI-Claims user's e-mail address • The user enters their VistA/CAPRI Access and Verify codes in the Login page fields • JLV validates these credentials against the user's local VA system and users proceed to the JLV Provider Portal
VHA	/JLV	<p>When SSOi is enabled (default):</p> <ul style="list-style-type: none"> • VHA users are authenticated through SSOi using their PIV and PIN • IAM authenticates VHA users and users proceed to the JLV Provider Portal <p>If SSOi Bypass is enabled (failover):</p> <ul style="list-style-type: none"> • VHA users are authenticated through JLV using their PIV and PIN • If a user is PIV exempt, the user is prompted for their Windows username and password • JLV receives the VHA user's e-mail address • The user enters their VistA/CPRS Access and Verify codes in the Login page fields • JLV validates these credentials against the user's local VistA and users proceed to the JLV Provider Portal

2.2.1. Identity Management

Users with a valid VA PIV card and PIN can access JLV.

2.2.2. Access Control

JLV access control for VA users consists of IAM validating the user's PIV card and PIN (SSOi) or JLV validating the user's email address from the user's PIV card, PIV PIN, and CPRS or CAPRI access and verify codes (SSOi Bypass). If the user provides an invalid PIN or access and verify codes an error message is presented above the Access/Verify code fields on the Login page. [Table 2](#) summarizes the JLV system components and the settings utilized for access control.

Table 2: Access Control Design

Component	Description
Configuration settings	<p>A configuration setting within the <i>appconfig-production.properties</i> file that enables access control:</p> <ul style="list-style-type: none"> • <i>Enable VA Access Control, On/Off</i>, This setting enables access control for VA users

2.3. User Notifications

JLV is comprised of hardware and software, interfaces to the dependent partner systems, such as Patient Discovery Web Service (PDWS) and Master Person Index (MPI), as well as other infrastructure necessary to deliver the JLV application. Each of the individual components may undergo scheduled downtime for maintenance on a periodic basis. JLV Support follows a notification process to alert VA stakeholders of pending downtime in advance of each known event.



NOTE: The VHA JLV team is responsible for notifying end users.

2.3.1. User Notification Points of Contact

[Table 3](#) details the current notification list for alerting for VA stakeholders of JLV scheduled downtime. The list is maintained by JLV Support.

Table 3: JLV Scheduled Downtime Notification List (VA Stakeholders)

Name	Organization	Email Address
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED.gov
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	VA-Government	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED

Name	Organization	Email Address
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	Liberty ITS	REDACTED
REDACTED	SMS	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED
REDACTED	Government CIO	REDACTED

2.3.2. JLV QoS Mail Groups

VA:

- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED

DOD:

- REDACTED (Navy)
- REDACTED (Navy)
- REDACTED (Navy)
- REDACTED (Defense Medical Information Exchange [DMIX])
- REDACTED (DMIX)
- REDACTED (contractor)
- REDACTED (contractor)
- REDACTED (DMIX)
- REDACTED (DMIX)
- REDACTED (DMIX)
- REDACTED (contractor)
- REDACTED (DMIX)
- REDACTED (contractor)
- REDACTED (contractor)

Liberty Team:

- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED

2.3.3. Scheduled Downtime Notifications

JLV Support monitors the maintenance schedules of systems that provide notification of planned outages, then communicates the upcoming downtime to VA stakeholders.

i **NOTE:** JLV Support depends on the receipt of timely information from dependent systems and infrastructure. Not all systems and/or infrastructure teams provide downtime notices to JLV Support. Detailed information, such as organization, frequency of planned downtime, and points of contact (POCs), is available in Appendices A, B, and C for each of the dependent systems and other infrastructure.


[Figure 3](#) shows a typical calendar of regularly scheduled downtimes for JLV and external systems. Refer to the detailed list following the calendar mockup for a complete list of planned downtimes.

Figure 3: Mockup of Regularly Scheduled Downtimes

Outages Calendar						
May 2021						
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
25 No impact_DNR_Scheduled: DHA NSOC Netw 12:00 am - 4:00 am No impact_DNR_Sched	26 5:30 pm Unscheduled: JLV 8:00 pm Scheduled: JLV ▼ 1 more item	27 9:00 am Unscheduled: 1:10 pm Unscheduled:	28 1:30 pm Unscheduled: 8:00 pm No impact_DNR	29 No Impact_DNR_DHA NSOC NETWORK MAIN 12:00 am No impact_DNR 8:00 pm No impact_DNR	30 12:00 am No impact_DNR 12:00 am Scheduled: VA	1 8:00 am No impact_DNR 9:00 pm Planned: Weekly DV 10:00 pm AppD_DNR
2 12:00 am AppD_DNR_Scheduled 12:00 am No impact_DNR	3	4 4:55 pm - 6:15 pm Unscheduled: JLV Servi	5 8:50 am - 10:15 am Unscheduled: JLV Servi	6 8:00 am - 9:00 am NI_DNR_Scheduled: D	7 12:00 am - 4:00 am AppD_DNR_Scheduled	8 9:00 pm - 12:00 am Planned: Weekly DV
9	10	11	12 2:00 pm Scheduled: CH 8:00 pm Scheduled: CH	13	14	15 9:00 pm - 12:00 am Planned: Weekly DV
16	17	18 9:00 am - 5:00 pm NI-DNR_Scheduled: NI	19 9:00 am NI_DNR_Sched 1:00 pm NI_DNR_Sched	20	21 12:00 am - 4:00 am NI_DNR_Scheduled: VA	22 9:00 pm Planned: Weekly DV 10:00 pm NI_DNR_Scheduled

The following list details the maintenance notices currently known to JLV Support.

- **JLV**
 - Organization: VA
 - Frequency: Monthly, the 3rd weekend of the month
 - Time Frame: 8:00 pm – 12:00 am ET Sunday
 - (The actual downtime necessary varies depending on update packages but does not exceed four hours.)
- POC: REDACTED and REDACTED

- **VA Authentication Federation Infrastructure (VAAFI)**
 - Organization: VA
 - Frequency: As needed; since move to Azure, no longer direct impact to JLV during maintenance window(s)
 - Time Frame: Varies
 - Email Subject: VAAFI Datacenter flip Miami to Culpeper
 - POC: REDACTED
- **MPI (VA and DOD)**
 - Organization: VA
 - Frequency: As needed
 - Time Frame: Varies, typically the 3rd weekend and from 3:00 pm to 9:00 pm
 - Email Subject: VAAFI Data center flip Miami to Culpeper
 - VA POC: REDACTED "
 - DOD POC: REDACTED
- **VA/DOD Gateway**
 - Organization: Joint DOD/VA
 - Frequency: As needed
 - Time Frame: Varies
 - POC: REDACTED
 - Data Exchange Service (DES) (includes data from the Clinical Data Repository [CDR], Composite Health Care System [CHCS], Federal Electronic Health Record [FEHR], and Community Partners):
 -  **NOTE:** JLV Support does not receive a distribution notice for all DOD downstream data sources (Theater Medical Data Store [TMDS], Essentris, SHARE, Bidirectional Health Information Exchange (BHIE) Framework, Joint Health Information Exchange (HIE)¹, Community Partners)
- **Military Health System (MHS) Enterprise Services Operations Center (MESOC) / Defense Information Systems Administration (DISA)**
 - Organization: DOD
 - Frequency: TBD
 - Time Frame: TBD
 - Email Subject: DMIX Integration Alert
 - POC: REDACTED
- **Military Health System (MHS) Enterprise Services Operations Center (MESOC) / Defense Information Systems Administration (DISA)**
 - Organization: DOD
 - Frequency: Monthly, 3rd weekend of every month

¹ DES to Joint HIE switch is a configuration change and requires a redeployment

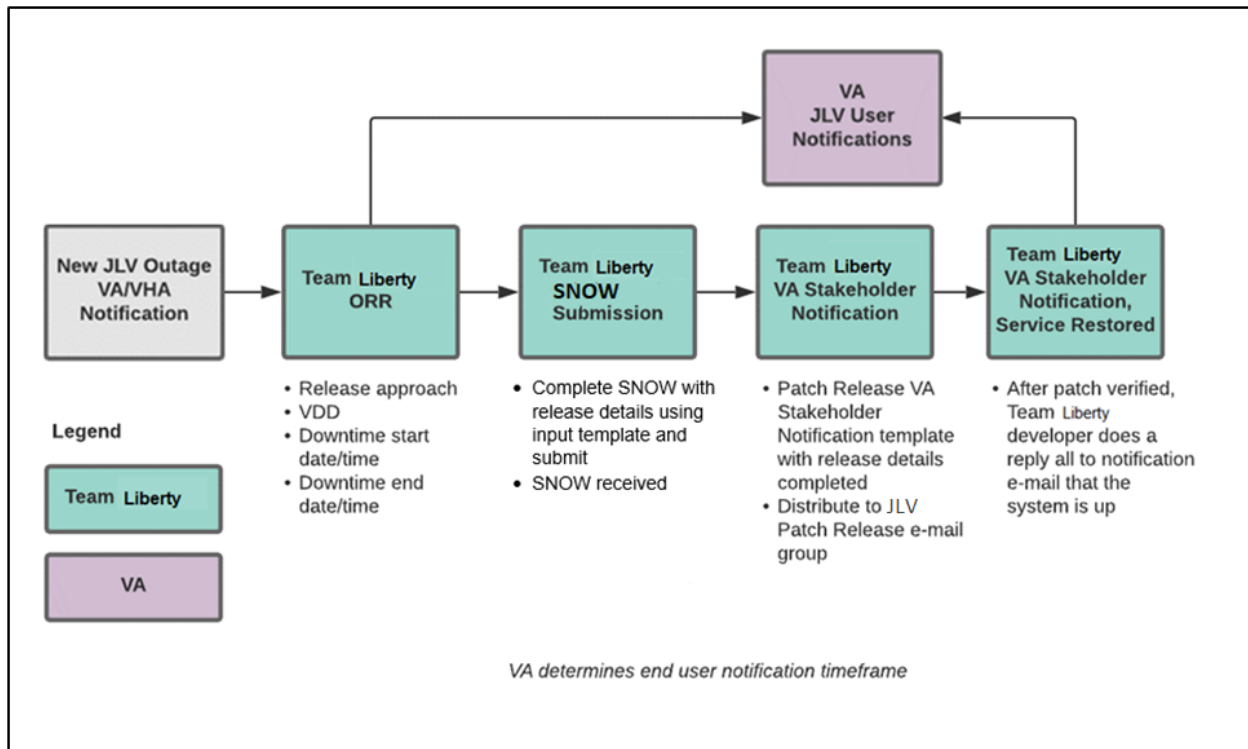
- Time Frame: Varies
- Email Subject: DMIX Integration Alert
- POC: REDACTED
- **PDWS / Defense Manpower Data Center (DMDC)**
 - Organization: DOD
 - Frequency: Weekly (actual downtime plan verified with the PDWS team)
 - Email Subject: DMIX Integration Alert
 - Time Frame: 9:00 pm ET Saturday to 6:00 am ET Sunday
- **CAPRI:** JLV Support does not currently receive a distribution notice
 - Organization: VA
- **VistA:** JLV Support does not currently receive a distribution notice
 - Organization: VA

The JLV Support team actively monitors all relevant systems maintenance schedules, and the team follows the scheduled downtime notification process for JLV code-driven patch releases:

- VA notifies JLV users of pending system downtime, when JLV is unavailable, and when the system is restored
- The JLV Support team notifies the VA stakeholders (see [Table 3](#)) when the JLV system is restored to service

The process flow shown in [Figure 4](#) was designed primarily for *JLV code-driven patch releases* and is used as a guide for scheduled downtime notifications. However, not all steps may apply for JLV downtimes triggered by scheduled maintenance or outages on external components that are outside the control of the JLV application.

Figure 4: Scheduled Downtime Notification Process



While all JLV scheduled downtime, communications follow a similar format, each is tailored to the specific activity and system/service affected.

2.3.3.1. Service Now (SNOW) Process

2.3.3.1.1. Creating a new Release

Once the team has decided to develop and make available a group of changes as a Release, a person from the team will enter a new Release into Service Now.

For detailed instructions on how to add a new Release to SNOW, please consult the following work instruction: REDACTED

A11.

- The CHG number is **CHGxxxxx**
- The ServiceNow Ticket number is **INCxxxxxxx**
- JLV Enterprise Patch version x.x.x.x.x will be released to DOD and VA Production environments on <Day>, <Month> <Day>, <Year> starting at <Time 24-hour clock> (Time am/pm) ET. Patching is expected to be completed by <Time 24-hour clock> (Time am/pm) ET, <Day>, <Month> <Day>, <Year>. JLV-Enterprise will be unavailable during this time.

2.3.4.1. Initial Response to Issues Within 30 Minutes of Alert

1. If a QoS e-mail is received and errors have **not** been cleared within 30 minutes of receipt of the initial error alert, proceed to Step 2
2. Within 30 minutes of the initial error e-mail, JLV Support ([Table 13](#)) sends an e-mail to the JLV stakeholders ([Table 3](#)), stating that the Support team is investigating the issue
 - a. Using the e-mail example below, tailored to the specific activity and the system(s)/service(s) that are affected

2.3.4.1.1. Initial Outage Response Notification E-Mail (Example)

Subject: JLV Outage Notification

All,

JLV is currently experiencing an error in the <Environment Name> environment.

The error detail is: <Error from QoS>

This error impacts <service impacted> (choose one from list below)

- PDWS: the users' ability to perform a patient search
- MPI: the users' ability to retrieve VA records
- VDS: the users' ability for VA users to log in and retrieve VA records
- VistA Host: the ability for JLV to retrieve records for the specified host
- BHIE Relay Service (BRS): the users' ability to retrieve DOD records
- Database: the ability for the application to check the authorized users list, retrieve a user's profile, generate a site list for the log in, and the ability for JLV to log auditing records
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to JLV until service is restored
- CAPRI: the ability for JLV to authenticate VBA users
- BRS/DES: the users' ability to retrieve DOD, FEHR, and Community Partner records

Please stand by as we further investigate the error. You will be notified by e-mail as soon as the issue is rectified. If the issue persists longer than 90 minutes from now, you will be notified of the error status and resolution progress in another e-mail.

Thank you.

2.3.4.2. Outage Escalation to External Teams

The following information details the escalation process to external teams in the case of an issue caused by a service outside JLV Support's purview. A status update is requested within 2 hours of the initial alert.

1. Send an e-mail to the applicable external service group as specified in [Table 13](#)
2. Request the status of the issue within 2 hours of the initial alert
 - a. Copy JLV Support ([Table 13](#))
 - b. Use the e-mail example(s) below, tailored to the specific activity and system(s)/service(s) that are affected

2.3.4.2.1. Outage Escalation to External Teams E-Mail (Example)

Subject: JLV Service Verification Request

All,

JLV is currently experiencing an error in the <Environment Name> environment.

The error detail is: <Error from QoS>

This error impacts <service impacted> (choose one from list below)

- PDWS: the users' ability to perform a patient search
- MPI: the users' ability to retrieve VA records
- VDS: the VA users' ability to authenticate and to retrieve VA records
- VistA Host: the ability for JLV to retrieve records for the specified VistA host
- CAPRI: the ability for JLV to authenticate VBA users
- BRS/DES: the users' ability to retrieve DOD, FEHR, and Community Partner records
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to JLV until service is restored

JLV Support would like to verify that <application/service> is up, running, and not experiencing any errors.

Optional: JLV Support has verified that network connectivity is not the issue. Please verify and respond to JLV Support with your findings.

Thank you for your assistance in troubleshooting this issue.

1. Generate a trouble ticket (VA or DOD) and assign it to the appropriate application team
2. Send a notification to the JLV stakeholders ([Table 3](#)) with all pertinent information
 - a. Use the e-mail example(s) below, tailored to the specific activity and system(s)/service(s) that are affected

2.3.4.2.2. Outage Update E-Mail (Example)

Subject ALERT: JLV Service Degradation - (Affected Service) errors - (insert error start time YYYYMMDD 24:00 ET)

All,

JLV is currently experiencing an error in the <Environment Name> environment.

The error detail is: <Error from QoS>

- PDWS: the users' ability to perform a patient search
- MPI: the users' ability to retrieve VA records
- VDS: the VA users' ability to authenticate and to retrieve VA records
- VistA Host: the ability for JLV to retrieve records for the specified VistA host
- CAPRI: the ability for JLV to authenticate VBA users
- BRS/DES: the users' ability to retrieve DOD, FEHR, and Community Partner records
- jMeadows: the application's ability to connect to external sources; users will not be able to log in to JLV until service is restored

The JLV Engineering team has determined the following:

- Severity: Severity Level ONE
- Impact: <List impacted users (VA, DOD, or VA and DOD), and state which services are impacted, and the functionality lost>

- Fault is isolated to: <Where the error resides (local JLV containers, local JLV DB, network (provide details if possible) or external application>
- Estimated Time of Service Restoration: <Estimated time frame of restoration>
- CHG Number: <CHG number, only if applicable and approved by VA JLV PM or VHA JLV Team>
- Ticket Number: <Ticket number submitted to the VA or DOD service desks, only if issue is with the network or external application>

The JLV Engineering team will continue to monitor and troubleshoot the issue. Updates will be provided every 2 hours until the issue is resolved.

Thank you.

1. Continue monitoring the issue
2. Provide updates every **2 hours** to the JLV stakeholders ([Table 3](#)) until issue is resolved:
 - a. Liberty ITS Emergency Contact: Stan Khabiev (442- 333-8459)
 - b. Liberty ITS Alternate Contact: Corey Kramek (808-219-3548)
 - c. Liberty ITS Alternate Contact: Christopher Lutz (571-265-4874)
 - d. Liberty ITS Alternate Contact: Lawrence Wilson (808-478-6742)

JLV Support Hours: 24x7x365

2.3.5. Announcement Banners

Announcement banners are provided for the end users' benefit and information. They appear in the Announcements section of the JLV Login page, and within the JLV application in the form of banners.

The primary goal of announcement banners is to inform end users of important information about their use of JLV. The use of acronyms and IT jargon within announcement banners is minimized to clearly communicate any temporary limitations of JLV.

It is important to note that the system maintenance notices shared among technical groups are different from the application-level announcement banners as they are not appropriate for end users.

Announcement banners are posted no more than 24 hours prior to a planned event and removed immediately upon completion of the planned event.

Announcement banners for an unplanned outage are posted immediately after the confirmation of the outage and are removed immediately upon resolution of the outage.

The following announcement banners are prioritized:

1. Patient Safety
2. Newly discovered defects/issues with broad impact
3. Unplanned outages or unexpected loss of data lasting more than 2 hours that are not already communicated by System Status notifications
4. Planned maintenance/outages with expected impact or disruption

- a. Maintenance events of no or inconsequential impact should not be posted

End users can become desensitized to the important information in announcement banners when too many alerts are posted too often. The plan to minimize alert fatigue is as follows:

1. Display announcement banners by severity
 - a. Add a prefix category (Patient Safety, Issue, Outage, Maintenance, etc.) to the announcement banner titles and content to further differentiate context and priority
2. Post only those alerts that impact end users
 - a. Informational announcement banners for maintenance events where there is no expected or an inconsequential impact should not be posted
3. Set an expiration date for announcement banners, and remove them as soon as possible after the event has completed or the issue has been corrected

The following groups have the responsibility and authority to enable certain types of announcement banners:

- JLV Project Support Team: Maintenance-related notifications that impact end users
- VHA JLV Team: Notifications regarding patient safety and other critical issues that impact end users

[Table 4](#) lists the announcement banner content for maintenance events with expected user impact and for special events and issues.

Table 4: Announcement Banner Content for Maintenance Events Impacting End Users

Maintenance Event Titles (50-character limit)	“More” Hyperlink Expanded Content (255-character limit)
MAINTENANCE DOD Patient Identity System-5/17-5/18 <u>More</u>	Maintenance window: 05/17/18 9pm ET–05/18/18 12pm ET Impact: JLV will be available for use, but users may experience problems with patient lookups/patient search using DOD EDIPI or issues viewing DOD patient demographics.
MAINTENANCE VA Patient Identity System -5/17 <u>More</u>	Maintenance window: 05/17/18 9pm ET–05/18/18 12pm ET Impact: Users may experience problems with patient search: CPRS via CCOW may display VA data only; DOD EDIPI or recently viewed list may display DOD data only; SSN ² searches may display no data.
MAINTENANCE DOD Theater Records System– 5/21-5/22 <u>More</u>	Maintenance window: 05/21/18 9pm ET–05/22/18 12pm ET Impact: Records from DOD theater systems may be unavailable. These include records from an area where military events were occurring at the time of care delivery (e.g., wartime).
MAINTENANCE Community Partner System—6/29 <u>More</u>	Maintenance window: 06/29/18 8pm ET–06/29/18 11 pm ET Impact: JLV will be available for use, but the Community Health Summaries & Documents widget may not retrieve records. If you experience this problem, please try again later.
ISSUE Please Check Federal EHR/MHS GENESIS Widget Date Filter	An error caused Federal EHR/MHS GENESIS widgets added to workspaces before 6/28/18 to display only the past 4 months instead of 1/1/17-present. To correct this, click the funnel-shaped filter icon and manually adjust the dates or close/re-add the widget.

² Social Security Number (SSN)

Maintenance Event Titles (50-character limit)	"More" Hyperlink Expanded Content (255-character limit)
PATIENT SAFETY Contrast Allergies	JLV is currently not displaying VA allergies for Contrast media entered through the Radiology option "Update Patient Record" [RA PTEDIT]. Until further notice, please use CPRS RDV to check for Contrast allergies from other VA sites.
ISSUE Imaging not available to Claims/CAPRI users	VA images are not currently being displayed in JLV. The issue is being analyzed and a patch to resolve the issue will be deployed as soon as possible. Please use a standalone Advanced Web Image Viewer (AWIV) for VA imaging access. NOTE: Affects VBA (Claims) Only
OUTAGE Community Partner Records	VA is currently unable to retrieve records from community partners. Engineers are working to restore connections as quickly as possible. (add details on anticipated resolution, etc. if available).

2.3.5.1. Placing Announcement Banners

When there is a major system outage, service degradation, scheduled downtime, or patient safety issue, an announcement banner will be placed on the Login page for the affected environment at the T+30 time frame. The announcement banner placement in any environment is accomplished via the DB associated with that environment.



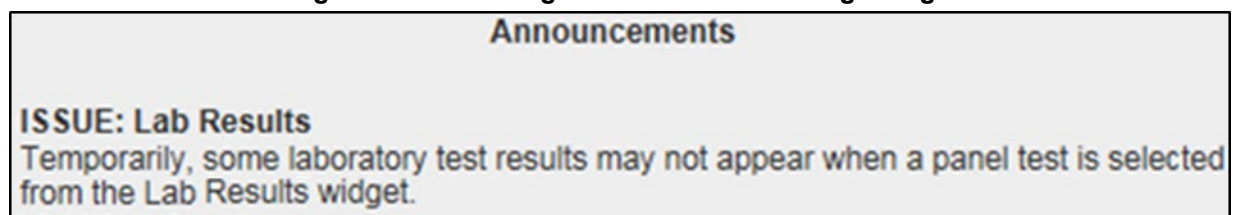
NOTE: Current functionality does not allow for a specific time frame, like 2:00 pm to 8:00 pm, to be provided. At present, the system only allows for an expiration date, formatted as Month/Day/Year.

An example of the script used to place an announcement banner is as follows:

```
execute dbo.createNotification
    @startDate='10/17/2018'
    ,@endDate='10/30/2018'
    ,@announcement='Lab Results'
    ,@userGroup='ALL'
    ,@description='Temporarily, some laboratory test results may not appear when a
panel test is selected from the Lab Results widget.'
```

The resulting announcement banner, as viewed on the application Login page, is shown in [Figure 6](#).

Figure 6: User-facing Banner on the JLV Login Page



2.3.5.2. Removing Announcement Banners

There are two methods used to remove a banner from the application Login page: manual and automatic expiration.

2.3.5.2.1. Manual Removal

The manual removal method is used when a system degradation has been resolved or the planned outage has been completed prior to the designated end date.

Manual removal is accomplished by accessing the DB tables and manually changing the end date (shown in red text below) to match the start date associated with the announcement banner to be removed. Database entries demonstrating the announcement banner prior to ([Table 5](#)) and after ([Table 6](#)) manual removal follow.

Table 5: Database Table Entry Prior to Manual Removal

Start Date	End Date	Title	Announcement Banner Text
2018-10-17	2018-10-30	ISSUE: Lab Results	Temporarily, some laboratory test results may not appear when a panel test is selected from the Lab Results widget.

Table 6: Database Table Entry After Manual Removal

Start Date	End Date	Title	Announcement Banner Text
2018-10-17	2018-10-17	ISSUE: Lab Results	Temporarily, some laboratory test results may not appear when a panel test is selected from the Lab Results widget.

2.3.5.2.2. Automatic Expiration

Automatic expiration of an announcement banner occurs when the designated end date (shown in red text below) of the announcement banner has been reached. Expiration dates are set based on when the issue can be resolved by an authorized member of JLV Support. A DB entry demonstrating a planned maintenance announcement banner is shown in [Table 7](#).

Table 7: Database Table Entry for a Planned Maintenance Announcement Banner

Start Date	End Date	Title	Announcement Banner Text
2018-10-26	2018-10-27	ISSUE: System performance upgrades	System may temporarily be down for system performance upgrades between 8pm ET, 26 October 2018–12am ET, 27 October 2018.

2.3.5.3. Announcement Banner Extensions

If a service degradation or other event will exceed the planned end date (shown in red text below) of an existing announcement banner, JLV Support can manually extend the duration of the announcement banner by changing the end date (shown in red text below) to a date in the future. Database entries demonstrating the announcement banner prior to ([Table 8](#)) and after a date extension ([Table 9](#)) follow.

Table 8: Database Table Entry as Initially Posted

Start Date	End Date	Title	Announcement Banner Text
2018-10-26	2018-10-27	ISSUE: System performance upgrades	System may temporarily be down for system performance upgrades between 8pm ET, 26 October 2018–12am ET, 27 October 2018.

Table 9: Database Table Entry After a Date Extension Update

Start Date	End Date	Title	Announcement Banner Text
2018-10-26	2018-10-29	ISSUE: System performance upgrades	System may temporarily be down for system performance upgrades between 8pm ET, 26 October 2018–12am ET, 29 October 2018.

2.4. System Monitoring, Reporting, and Tools

JLV traces and audits actions that a user executes within the application. JLV audits are provided through 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 (date and time of event, patient identifiers, user identifiers, type of action, and access location) to show system threads of access and the views of patient records. Refer to [Application Error Logs](#) for more information about audit and server logs.

The JLV QoS service monitors the availability of data sources. Refer to [Availability Monitoring](#) for more information.

JLV in VAEC will make use of AppDynamics and AWS CloudWatch for monitoring services and health status of the application. AWS CloudTrail is used for auditing and analyzing application behavior analysis.

2.4.1. Dataflow Diagram

The data retrieval sequence is detailed in the *JLV 3.0.0 System Design Document* (SDD). Once approved, all project documentation is available on the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

2.4.2. Availability Monitoring

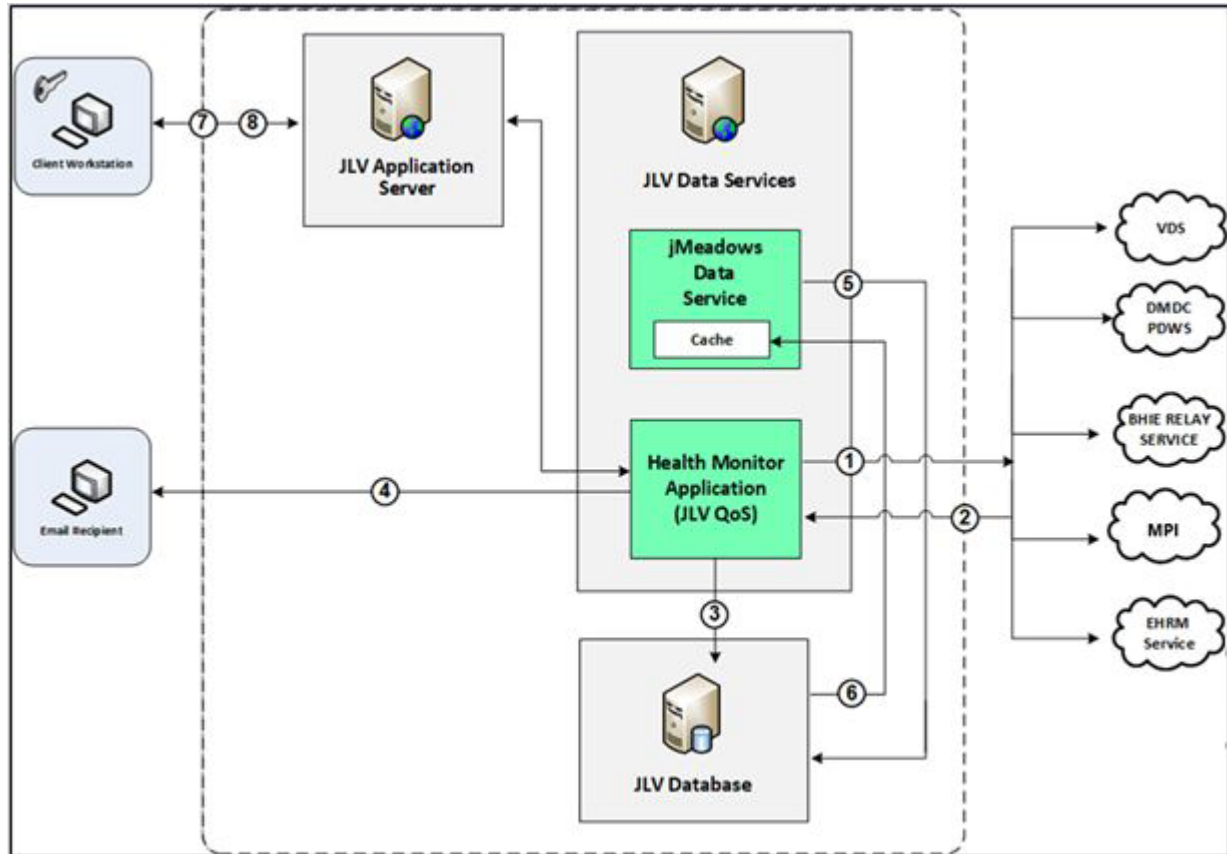
QoS monitors the health of JLV and checks for the availability or disruption of dependent services within the systems in DOD and/or VA environments ([Table 10](#): Services Monitored by QoS).

Table 10: Services Monitored by QoS

Service	Description
DMDC PDWS	Patient look up
MPI (VA)	Retrieves VA patient ID
BRS (DES)	Connects to DES and DOD VLER
JLV DB Server	Contains JLV DB information
jMeadows Data Service	Connects to MPI, PDWS, DB, BRS, EHRM Service, and Report Builder

Service	Description
VDS	VA Log in/Data
EHRM Service	Connects to jMeadows, Joint HIE via Fast Healthcare Interoperability Resources (FHIR), and Cerner Millennium via Cerner FHIR Application Programming Interface (API)

Figure 7: System Status Check Sequence



System status checks ([Figure 7](#)) are performed as follows:

1. The Health Monitor pings the monitored services every 5 minutes
2. The Health Monitor receives a system status from each monitored service and reports the status of JLV systems to JLV Support via e-mail
3. System status events are written to the QOS_LOGS table within the JLV DB
4. The Health Monitor sends an automated e-mail notification every 6 hours, unless a status change is detected
 - a. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset
 - b. The next e-mail is generated after 6 hours if no further system status changes are detected
 - c. When all errors are cleared, an e-mail is sent stating that no errors are detected
5. The jMeadows Data Service pings the JLV DB every 2 minutes for status checks

6. The jMeadows Data Service stores the data returned from the JLV DB in an internal cache, the jMeadows Data Service cache
7. When a user accesses the JLV **Login** page, JLV requests and receives system status data from the jMeadows Data Service cache
8. During active user sessions, JLV requests system status data from the jMeadows Data Service cache every 5 minutes
 - a. Current system status is retrieved from the cache and sent to the JLV GUI

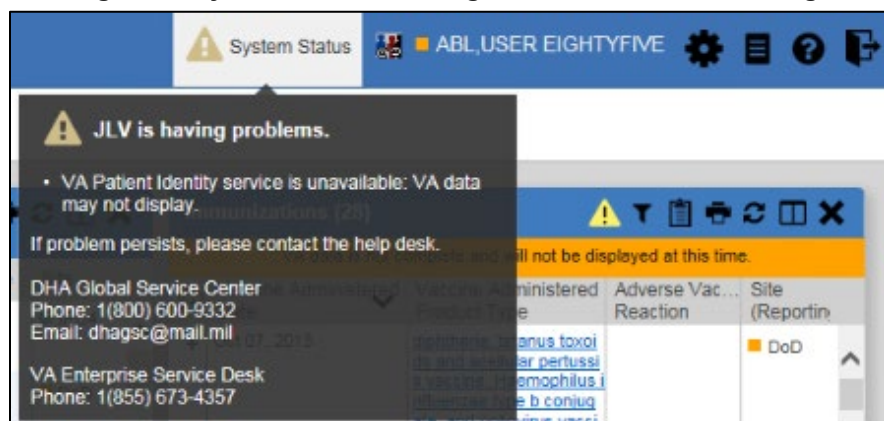
[Figure 8](#) depicts a system status message displayed on the JLV **Login** page.

Figure 8: System Status Message on the JLV Login Page

Figure REDACTED due to PII



[Figure 9](#) shows a system error status displayed on the JLV **Patient** portal page, which presents only if the system status is yellow or red. If the system does not detect a service connection error, no notice displays.

Figure 9: System Status Message on the Patient Portal Page



2.4.2.1. Domain-Level Availability Monitoring

JLV displays interface status icons on the toolbars of multiple Patient portal widgets to communicate the status of the data source for the widget's clinical domain. There are two conditions:

- The information icon  indicates that all sources are available
- The warning icon  indicates one or more data sources are unavailable

Both icons are used to provide status for VA, DOD, and community partner data sources. Clicking the status icon opens interface status details in a separate window, as shown in [Figure 10](#).

Figure 10: Connection Status Details

Connection Status for Outpatient Medications

⚠ Connection Errors

Connections from the following sources are currently unavailable. Most connection errors resolve themselves within a few hours.

Source	Name	Status	Data Domain
DOD	TMDS	FAILURE	Outpatient Medications

[< Hide All Active Interfaces](#)

All Active Connections

Connections to the source systems are successful. Successful status connections are not an indicator that clinical data is being returned to the widget from the source system.

Source	Name	Status	Data Domain
DOD	CDR	SUCCESS	Outpatient Medications
DOD	FEHR	SUCCESS	Outpatient Medications
VA	IPOTEST4	SUCCESS	Medications

2.4.3. Performance/Capacity Monitoring

Query times for each web service call in to the Relay Service, jMeadows, EHRM Service, and VDS are recorded to CloudWatch and the VAEC's Central Logging Solution (CLS) logs. AppDynamics is used for monitoring connections and performance.

2.4.4. Critical Metrics

VA providers, VHA users, or VBA users accessing a DOD-only patient (i.e., no VA identifiers for a patient): JLV records each access of Protected Health Information (PHI) through JLV. This includes the identification of the individual whose PHI was accessed, the identification of the user who accessed the information, and identification of the specific PHI accessed.

User access to sensitive DOD data: DOD and VA users are audited each time a sensitive DOD record (domains: sensitive notes, outpatient encounters, and labs) is viewed, regardless of how many times the user has previously viewed it, including multiple views in the same user session. When a user opens and closes a sensitive record, then reopens the same record and views it a second time, the user is asked to agree to be audited again.

The following information is captured for each attempt to access DOD sensitive data, whether successful or unsuccessful:

- Organization (i.e., VHA, VBA, DOD)
- Username

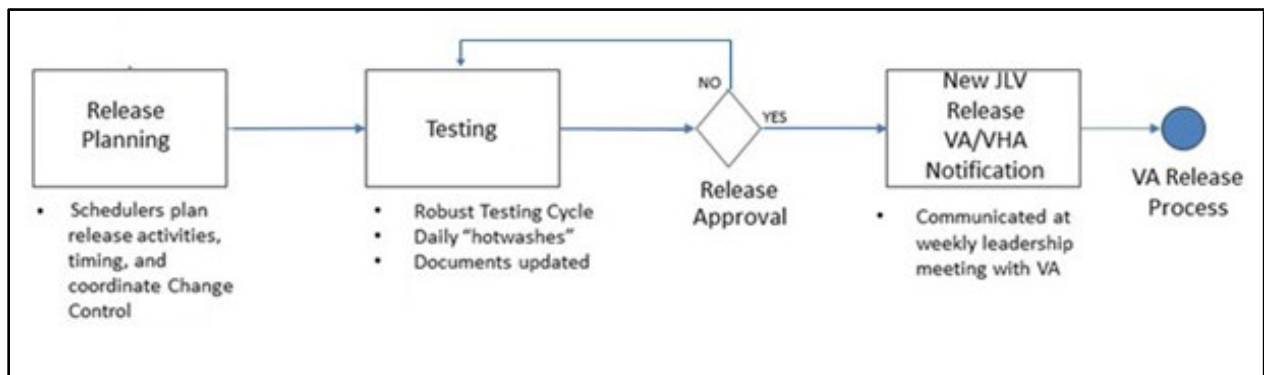
- User SSN
- User PIV, if known, for VA users
- User location
- Patient last name, first name, middle initial (MI), SSN, MPI, date of birth (DOB)
- Sensitive data accessed
- Date/time of access
- Reason for access (emergent care, clinical care, or authorized administrative use)

2.5. Routine Updates, Extracts, and Purges

2.5.1. Routine Updates

Patches and other routine updates follow the JLV patching process, shown in [Figure 11](#).

Figure 11: Patching Process for VA and DOD Components



2.5.2. Extracts

Extracts of the JLV audit logs and server logs are available by request only, on an as-needed basis. The VA Project Manager (PM) must approve requests for extracts. Approvals are dependent on the type of request and the organization of the requester. Once a request is approved, an authorized system administrator extracts the requested data and sends it to the requestor via an encrypted method. Refer to [Application Error Logs](#) for more information on audit and server logs.

2.5.3. Purges

Neither data nor audit log entries, from the JLV DB or other system components, are purged.

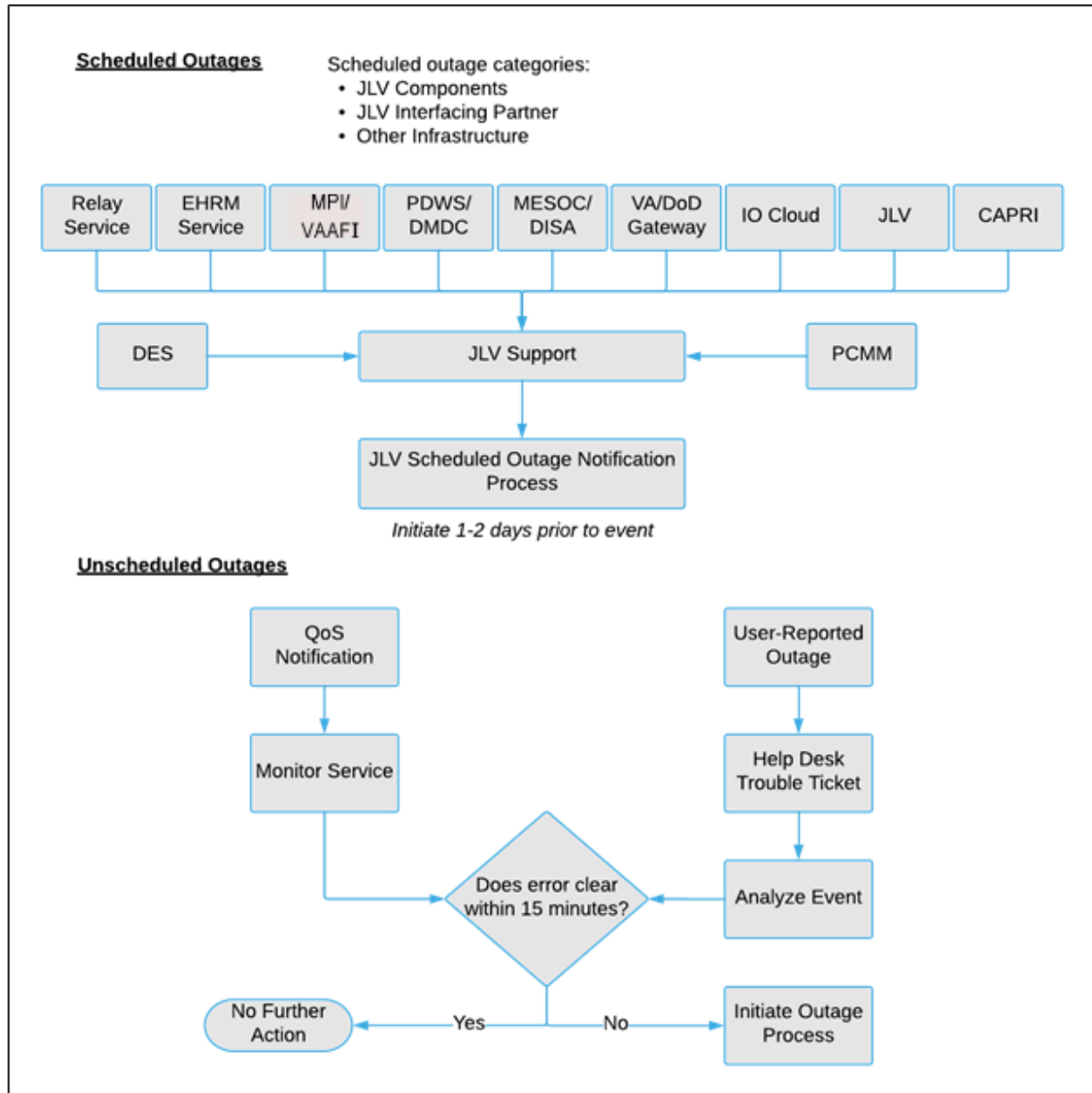
2.6. Scheduled Maintenance

Scheduled downtime typically occurs after 08:00 PM ET, and service is restored by 8:00 AM ET. Any planned downtimes, (within VA control), outside of these hours requires justification and approval by the VHA JLV Team and the Office of Information and Technology (OIT) PM.

[Figure 12](#) depicts the JLV process for monitoring, analyzing, and initiating the notification for an outage.

i **NOTE:** IAM/SSOi Bypass is not monitored in this release.

Figure 12: Scheduled Downtime and Unscheduled Outage Overview



2.7. Unscheduled Outage Triage Process

An unscheduled outage typically occurs when there is a major, unexpected Production issue. As such, the processes in the following sections are triggered (i.e., when the entire JLV application is down and/or a significant number of end users are impacted).

i **NOTE:** The QoS tool is the primary means of monitoring the JLV application. The processes described in the following sections are specific

to the QoS tool and its related incident responses. The VHA JLV team is responsible for notifying end users.

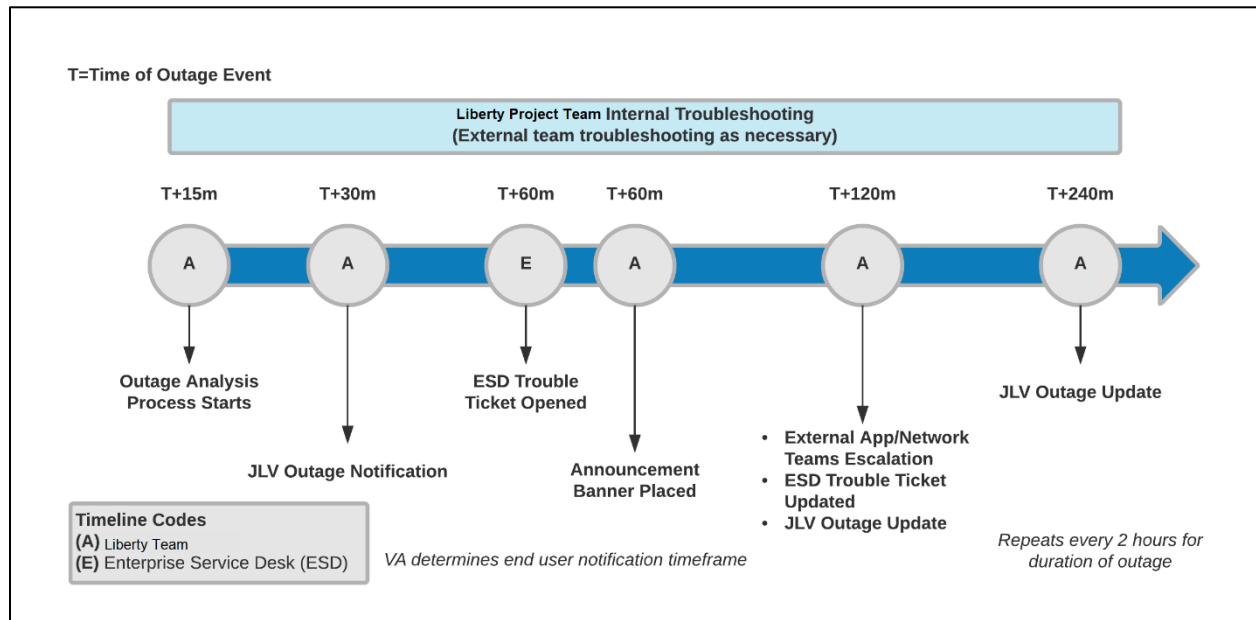
2.7.1. Outage Triage Timeline

The JLV outage triage process is executed by JLV Support in coordination with the VA JLV interface systems teams (e.g., MPI), as necessary.

The following steps represent routine system monitoring:

1. Monitor e-mail to see if the JLV application corrects itself
 - a. Wait 15 minutes to see if a QoS e-mail arrives indicating that there are no errors (e.g., *Cloud—JLVQoS Report: NO ERRORS DETECTED*)
 - b. Check junk e-mail folder for QoS alerts
2. If a QoS e-mail is received indicating “*NO ERRORS DETECTED*,” the system is connected and executing properly

Figure 13: Outage Event Activities and Timeline



2.7.2. Escalation

The escalation process typically follows this progression:

1. The problem is reported
 - a. QoS reports a problem that remains unresolved for over 30 minutes (See [Availability Monitoring](#))
- OR-
- b. A JLV user calls the ESD and opens a trouble ticket

i **NOTE:** There are instances when the user may bypass the ESD and go directly to the VA PM or other program contact. Should this occur, direct the user to the ESD to complete an official trouble ticket.

2. JLV Support analyzes the problem and determines whether to initiate the triage process
3. Once the triage process is initiated, JLV Support follows the analysis and notification timeline and escalation (as necessary) processes, and includes external systems teams ([Figure 13](#))

i **NOTE:** Discoveries made regarding the root cause of an issue and the service restoration time frame are communicated via e-mail to the stakeholders as soon as they come to light.

2.7.3. Issue Resolution and After Action

The following steps are taken after the issue is resolved:

1. After the issue is resolved, determine if the root cause was *internal* to the JLV application
 - a. If the problem was with an *external system/service*, obtain the root cause from the applicable team ([Table 13](#))
2. Send an e-mail to the JLV stakeholders ([Table 3](#)) stating that JLV is back online and available for use
 - a. Include the root cause of the issue and details of the fix required to resolve the issue, if available

2.8. Capacity Planning

JLV uses auto-scaling and automatic failover techniques. data collected from CloudWatch will help inform the team of the potential need for capacity adjustments.

Additionally, JLV monitors the application performance, user onboarding, and user behaviors on a weekly basis. Container resources and JLV application data are collected by the enterprise monitoring group, using the AppDynamics monitoring tools. CA APM monitors and stores data and sends alerts to notify members of an e-mail distribution group when any metric exceeds its upper or lower boundary.

2.8.1. Initial Capacity Plan

Processing capacity forecasts and workload modeling are conducted in an ad hoc manner. These forecasts are used to project server capacity based on Production data, JLV requirements, and JLV application changes planned for future releases. AWS provides the capability for autoscaling to adjust to changing capacity needs.

3. Exception Handling

Like most systems, JLV may generate a small set of errors that may be considered routine, in the sense that they have minimal impact on users and do not compromise the operational state of the system. Most errors are transient in nature and are resolved by the user trying to execute an

operation again. The following subsections describe these errors, their causes, and what, if any, response an operator should take.

3.1. Routine Errors

While the occasional occurrence of errors may be routine, encountering many individual errors over a short period of time is an indication of a more serious problem. In that case, the error must be treated as a significant error. Refer to [Significant Errors](#) for more information.

3.1.1. Security Errors

One possible security error an end user may encounter is an invalid login error. Causes of such an error include the user attempting to access JLV before they are authorized to do so (*Access denied. You are not an authorized user.*) or mistyping their Access and/or Verify code (*Invalid Access/Verify Codes*). A user's login credentials will be locked by the VistA service to which JLV connects after five incorrect login attempts (*Device/Internet Protocol (IP) address is locked due to too many invalid sign-on attempts.*). If this occurs, the user contacts the ESD and opens a service request ticket. The user's local VistA administrator can unlock their account.

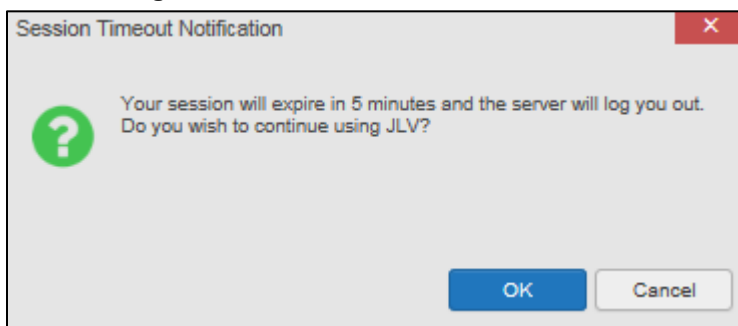
3.1.2. Timeouts

Each subsection describes a possible timeout error.

3.1.2.1. Application Timeout

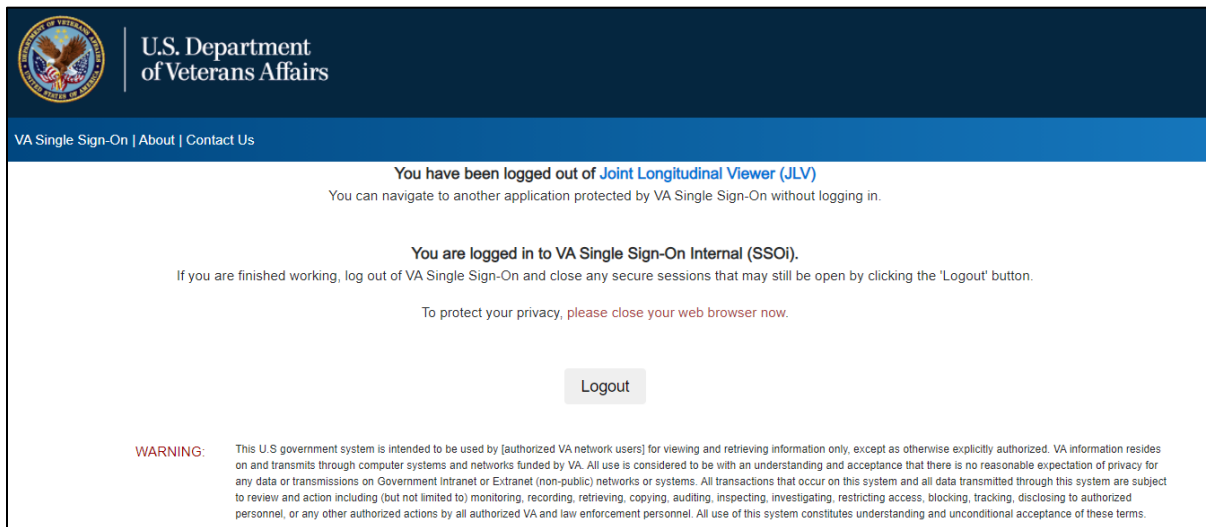
JLV has a timeout feature that is set to 30 minutes of inactivity. If users leave the JLV application idle for 25 minutes, they receive the Session Timeout Notification ([Figure 14](#)). If the user would like to extend the session, they can click the OK button to continue using JLV.

Figure 14: Session Timeout Notification



If the user does not interact with the Session Timeout Notification message within the 30-minute time limit, the JLV session times out ([Figure 15](#)). The user must then close the browser, reopen the browser, and log back in to JLV.

Figure 15: Session Timeout (SSOi)



3.1.2.2. Connection Errors

If users encounter a web browser timeout error or the browser displays, *“This page can’t be displayed,”* when accessing the correct URL, it indicates that JLV application services are either not running or there is a network outage.

Either the JLV Support team or the active site’s system administrators may attempt to remote desktop in to each JLV application server to ensure the Tomcat services are running. If they are running, system administrators contact IO to verify that the GTM is operating correctly.

JLV may also report timeouts to external systems within widgets by displaying a message that one or more data sources could not be connected ([Figure 16](#)).

Figure 16: Connection Error

Documents (66)					
Filtered date range: 3/29/18 - 7/27/18					
	Date	Description	Provider	Image	Site
+	Jul 03, 2018	CONSENT FOR LONG-TERM OPIOIDS FOR PAIN	MCCLAIN, MAE		● IPO4
+	Jul 02, 2018	CONSENT FOR PAIN MANAGEMENT - IMED		📷	● IPO4
+	Jul 02, 2018	CONSENT FOR PAIN MANAGEMENT - IMED			● IPO4
+	Jul 02, 2018	CONSENT FOR PAIN MANAGEMENT - IMED		📷	● IPO4
+	Jun 28, 2018	MOVE BEHAVIORAL HEALTH PROGRESS NOTE	MCCLAIN, MAE		● IPO4
+	Jun 19, 2018	INFECTION CONTROL PROCESS NOTE	MCCLAIN, MAE		● IPO4

i **NOTE:** Connection errors that persist for more than 5 minutes must be investigated by Tier 3 support.

3.1.3. Concurrency

Resolution of concurrent EHR access is handled by the underlying system of record that is being queried. The JLV Engineering team optimizes the stored procedures for user profiles in the DB to avoid concurrency contention, based on application and system metrics, degradation, and user load. Remediation depends on the identified root cause.

3.2. Significant Errors

Significant errors are defined as errors or conditions that affect system stability, availability, performance, or otherwise make the system unavailable to its user base. The following subsections contain information to aid administrators, operators, and other support personnel in the resolution of significant errors, conditions, or other issues.

3.2.1. Application Error Logs

jMeadows retains user actions within JLV. Specific events regarding user transactions are also audited (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 logins, and the identity of the information system component where the event occurred.

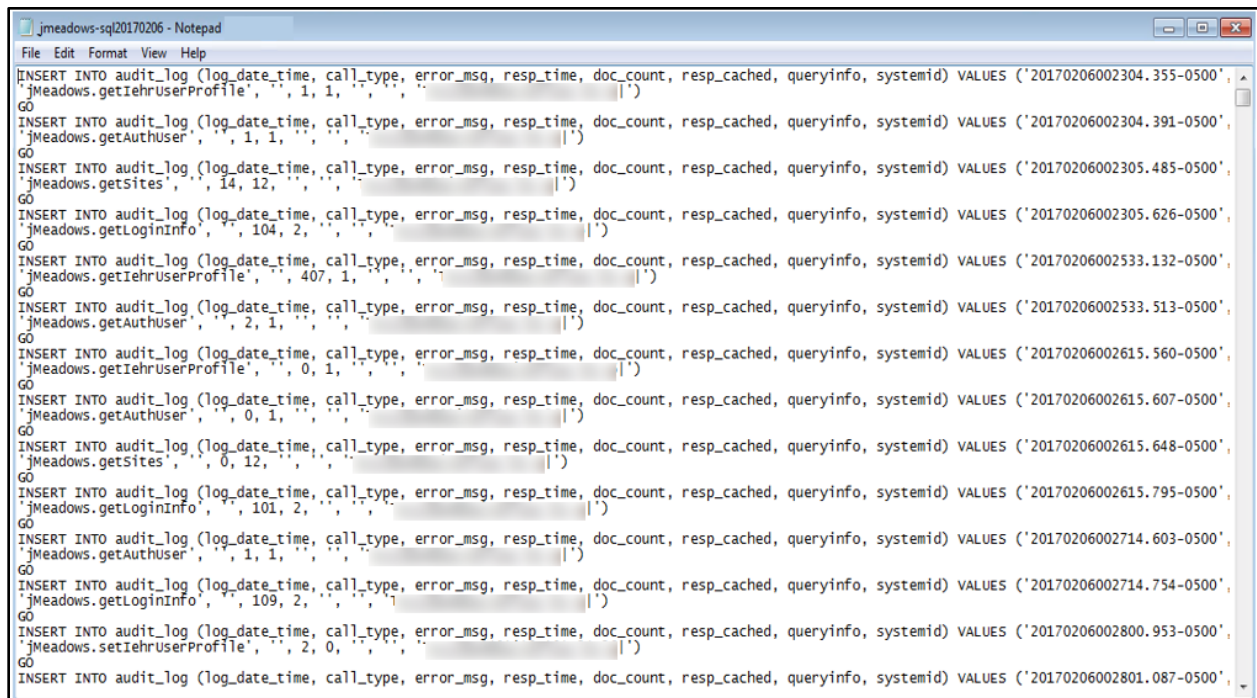
Each time an attempt is made to interface with jMeadows, whether it is a service communication or a user searching for a patient, the activity is logged and stored in the JLV DB. The purpose of retention is for traceability; specifically, to show what calls/actions were made, where, by whom, and when they terminated. Each query for data is audited and each has the user ID linked to it. Only one audit log is produced that contains both VA and DOD user IDs and usernames.

Query times for each web service call in to the Relay Service, jMeadows, and VDS are recorded in CloudWatch and the VAEC's Central Logging Solution (CLS).

Table 11: Response Time Log Location

Data Service	Log File Name
EHRM Service	(hostname)_ehrm-sql.log
jMeadows Data Service	(hostname)_jmeadows-sql.log
Relay Service	bhie-sql.log
VDS	(hostname)_vds-sql.log

Figure 17: jMeadows Log Output



```
File Edit Format View Help
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002304.355-0500',
jMeadows.getIehrUserProfile', , 1, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002304.391-0500',
jMeadows.getAuthUser', , 1, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002305.485-0500',
jMeadows.getSites', , 14, 12, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002305.626-0500',
jMeadows.getLoginInfo', , 104, 2, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002533.132-0500',
jMeadows.getIehrUserProfile', , 407, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002533.513-0500',
jMeadows.getAuthUser', , 2, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.560-0500',
jMeadows.getIehrUserProfile', , 0, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.607-0500',
jMeadows.getAuthUser', , 0, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.648-0500',
jMeadows.getSites', , 0, 12, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.795-0500',
jMeadows.getLoginInfo', , 101, 2, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002714.603-0500',
jMeadows.getAuthUser', , 1, 1, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002714.754-0500',
jMeadows.getLoginInfo', , 109, 2, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002800.953-0500',
jMeadows.setIehrUserProfile', , 2, 0, , , , )
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002801.087-0500',
```

The QoS service deployed with JLV monitors the availability of the services that connect to JLV data sources and other outside systems. Connection errors within the JLV environment are written to the QOS_LOGS table within the JLV DB and are displayed in JLV.

Service interruptions detected by the QoS service are reported to JLV Support via e-mail. An automated e-mail notification is sent every 6 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset. The next e-mail is generated after 6 hours if no further system status changes are detected. The QoS service does not send service interruption notices to external systems or services.

For detailed information on service interruption notifications and sample e-mail messages, please see the system design specifications and diagrams that can be found in the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

3.2.2. Application Error Codes and Descriptions

The JLV Support team utilizes system notifications generated from the QoS service to diagnose service interruptions and troubleshoot potential issues.

Standard SQL Server, Tomcat, Apache httpd, Java, and Hypertext Markup Language (HTML) error codes—generated by the system and recorded in the application logs—are used to identify, triage, and resolve complex issues that may arise during system operation.

3.2.3. Services Infrastructure Errors

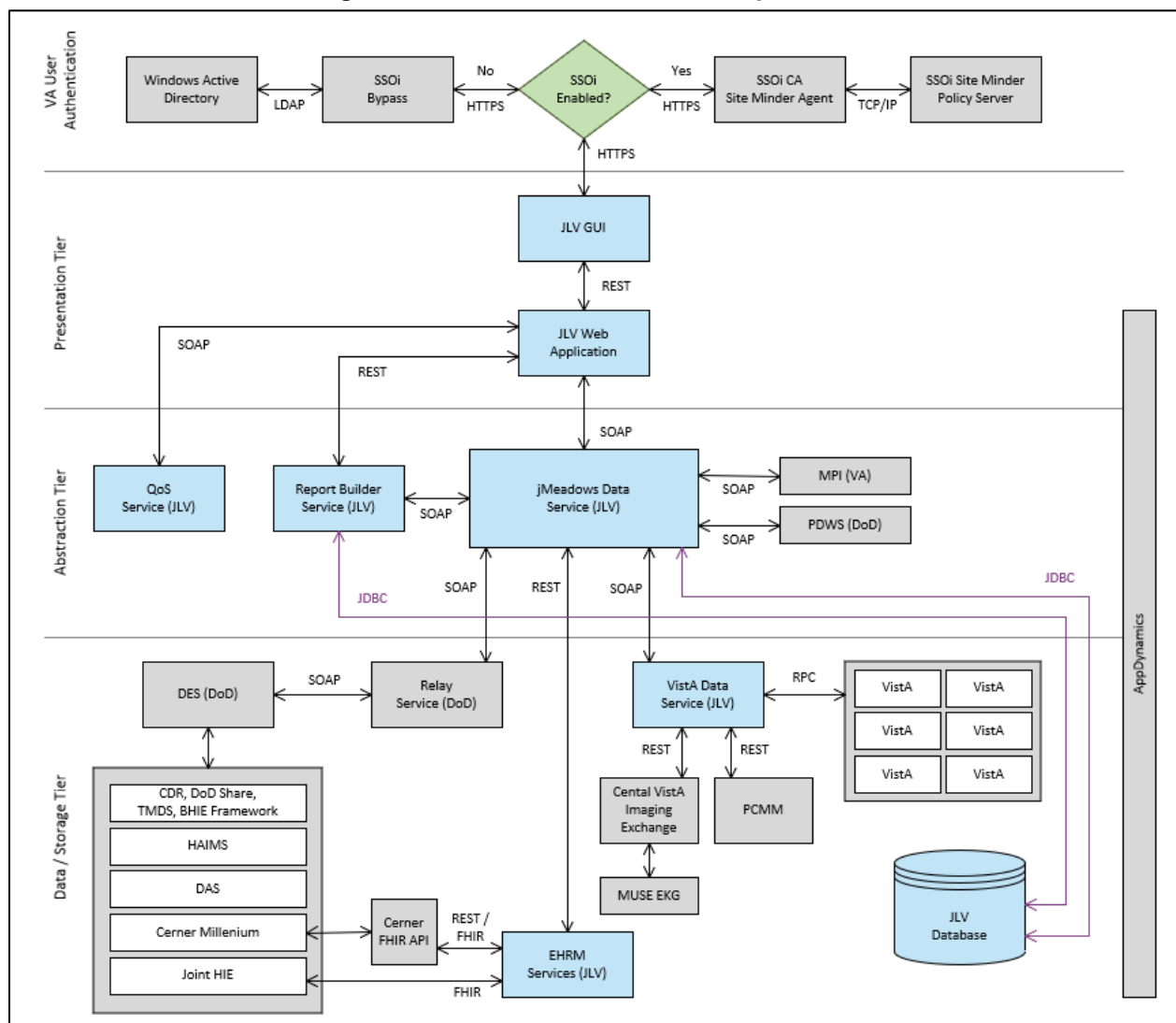
3.2.3.1. DB

The JLV DB is a relational DB used to store user profile information and audit data. It also stores VA and DOD terminology mappings (both local terminology and national standards). The DB does NOT store, neither long term nor temporarily, patient or provider EHRs from VA, DOD, and community partner data through the Joint HIE.

The JLV DB is an Amazon-managed RDS instance running Microsoft SQL Server 2017.

([Figure 18](#)). Only the JLV application and components of the JLV system, including the jMeadows Data Service, connect to and utilize the JLV DB.

Figure 18: JLV Architecture and Components³



³ Active Directory (AD), Computer Associates (CA), Central VistA Imaging Exchange (CVIX), Data Access Service (DAS), Enterprise Common Access Card (CAC) Electronic Health Record Modernization (EHRM),

For detailed information about errors and events for the SQL Server DB Engine, please see the website [MS Developer Network Database Engine Events and Errors](#).⁴

The JLV DB has a table to audit user actions within the application within the AUDIT DB table. This table collects system usage data and provides the JLV Support team the ability to create reports and extract pertinent information from the DB, as needed. A sample of the Audit log can be seen in [Figure 19](#).

Figure 19: Audit Log

Figure REDACTED due to PII

3.2.3.2. Web Server

JLV uses Apache Tomcat as its web server in the VA environment. JLV does not implement any custom Tomcat error handling or reporting. Please refer to the REDACTED⁵ for more information.

3.2.3.3. Application Server

JLV uses Apache Tomcat as its application server in the VA environment. JLV does not implement any custom Tomcat for error handling or reporting. Please refer to the Apache Tomcat Troubleshooting and Diagnostics guide for more information. See [Web Server](#) for the link to the resource.

3.2.3.4. Network

JLV utilizes the network infrastructure provided by VAEC. Any network errors that arise are corrected by the VAEC team.

3.2.3.5. Authentication and Authorization (A&A)

Users must provide their PIV and PIN to log in via SSOi. If credentials are not found the message, “*Not a valid Access Code/Verify Code pair*” displays.

A&A error messages are:

- Smart Card Required: The user has not inserted their PIV card into the card reader
- ActivClient: The user’s PIV PIN was entered incorrectly
- Missing Code: The user has not entered their Access/Verify code(s)
- Invalid Access Code: The user has entered an incorrect Access/Verify code

A detailed overview of the login process from the user’s perspective is provided in the *JLV 2.9.4 User Guide*. Once approved, all project documentation is available on the VA JLV Product

Healthcare Artifact and Image Management Solution (HAIMS), HyperText Transfer Protocol Secure (HTTPS), Java DB Connectivity (JDBC), Lightweight Directory Access Protocol (LDAP), Military Health System (MHS), Remote Procedure Calls (RPCs), Representational State Transfer (REST), Simple Object Access Protocol (SOAP), Transmission Control Protocol (TCP)

⁴ REDACTED

⁵ REDACTED

Repository on GitHub. See [Administrative Procedures](#) for the link to the repository and refer to [Security/Identity Management](#) for detailed information.

3.2.3.6. Logical and Physical Descriptions

System design specifications and diagrams can be found in the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

3.3. Dependent System(s) and Services

[Table 12](#): JLV Dependent Systems and Services lists the other VA systems upon which JLV depends. It also includes the errors related to each dependent system and remedies available to system administrators. Tier 3 system engineers follow a triage process to determine the root cause of the error and coordinate with the Point of Contact (POC) for the external systems, as needed.

Table 12: JLV Dependent Systems and Services

Other VA System	Related Error(s)
BRS	DOD, Federal EHR, and Community Partner data in widgets is currently unavailable. The source connection is down and DOD, Cerner, and community partner records of all types from all sites may not display.
Cerner FHIR API	Federal EHR (Cerner) is currently unavailable. The source connection is down, and some Federal EHR data may not display.
CVIX	If the CVIX service is not available, a message states, <i>“There was an issue retrieving the CVIX URL.”</i>
LDAP	This service is used between the SSOi Bypass Service and Windows Active Directory within VA environments for the purposes of authenticating PIV cards and PINs when SSOi is unavailable.
MPI	The JLV QoS Service monitors MPI availability. When MPI is unavailable, the message, <i>“MPI Service may be offline or unavailable,”</i> is shown in System Status. Refer to Domain-Level Availability Monitoring .
Primary Care Management Module (PCMM)	If PCMM is unavailable, JLV displays the error message: “The connection to PCMM is unavailable. The patient’s assigned clinical teams may not display.”
Site VistA instances	VistA connection errors are reported through interface status notifications for each clinical domain. Refer to Domain-Level Availability Monitoring .
SSOi	If this service is enabled and the SSOi Policy Server is not available, VA users cannot gain access to JLV.

3.4. Troubleshooting

Tier 1 troubleshooting contact information can be found in CA SNow by searching for *JLV* in the **Knowledge** tab. Tier 1 troubleshooting support is handled through the ESD at 855-673-4357. Refer to [Table 13](#) for additional contact information.

Tier 2 issues are handled by Health Product Support (HPS).

Tier 3 support and troubleshooting is handled directly by JLV Support.

3.5. System Recovery

The following subsections define the processes and procedures necessary to restore the system to a fully operational state after a service interruption. Each of the subsections starts at a specific system state and ends with a fully operational system.

3.5.1. Restart After an Unscheduled System Interruption

The simplest way to bring the system back to normal operations after the crash of a component is to restart the affected server(s). See [System Startup from Emergency Shutdown](#) for guidance.

3.5.2. Restart after DB Restore

Refer to [System Startup](#) for the system startup procedures.

3.5.3. Backout Procedures

Backout procedures vary depending on the specific release. Please see the *JLV Deployment, Installation, Backout, and Rollback Guide* specific to the version to be backed out for more information. Once approved, all project documentation is available on the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

3.5.4. Rollback Procedures

Rollback procedures are dependent on each specific release. Please see the *JLV DIBRG* specific to the version to be rolled back for more information. Once approved, all project documentation is available on the VA JLV Product Repository on GitHub. See [Administrative Procedures](#) for the link to the repository.

4. Operations and Maintenance Responsibilities

Operations and maintenance roles and responsibilities for JLV are summarized in [Table 13](#).

Table 13: Operations and Maintenance Responsibility Matrix

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
VA ESD	Tier 1 support for VA Users	REDACTED	REDACTED
DOD MHS Service Desk	Tier 1 support for DOD Users	REDACTED	REDACTED
VA JLV Project Office	VA OIT and VHA Stakeholders		
REDACTED	JLV PM	REDACTED	REDACTED
REDACTED	Program Specialist	REDACTED	REDACTED
REDACTED	Senior JLV Analyst	REDACTED	REDACTED
REDACTED	Program Analyst	REDACTED	REDACTED
REDACTED	Senior Clinical Subject Matter Expert		REDACTED
REDACTED	CLIN 3		REDACTED

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
DOD JLV Project Office	DMIX Stakeholders		
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
Liberty Team	JLV Support		
REDACTED	Contract Program Manager (PgM)	REDACTED	REDACTED
REDACTED	Contract PM	REDACTED	REDACTED
REDACTED	Contract PM	REDACTED	REDACTED
REDACTED	JLV Product Owner	REDACTED	REDACTED
REDACTED	JLV Operations Lead	REDACTED	REDACTED
REDACTED	JLV DevOps Lead	REDACTED	REDACTED
REDACTED	JLV Operations	REDACTED	REDACTED
REDACTED	JLV Operations	REDACTED	REDACTED
DMDC	PDWS Technical Issues and Support Contacts	REDACTED	
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
DES	DOD Adapter Technical Issues and Support Contacts		
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
DOD DISA	Technical Issues and Support Contacts		
REDACTED		REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
VAAFI	Data Power Technical Issues and Support Contacts		
REDACTED	VAAFI Lead	REDACTED	REDACTED
REDACTED	Deputy PM SSOi	REDACTED	REDACTED
REDACTED	VAAFI	REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
MPI (VA)	Technical Issues/ Support Contacts	N/A	REDACTED

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
REDACTED	Lead Developer/ Architect	REDACTED	REDACTED
REDACTED	MPI point of contact	REDACTED	REDACTED
REDACTED	MPI point of contact	REDACTED	REDACTED
REDACTED		REDACTED	REDACTED
REDACTED	Vista Imaging		REDACTED
VA Network— NSOC	Technical Issues/Support Contacts	REDACTED	REDACTED
REDACTED	Triple-I/VA-NSOC	REDACTED	REDACTED
DOD Network Space & Naval Warfare Systems (SPAWAR) Virtual Private Network (VPN)	Technical Issues and Support Contacts		In VA Remedy: SPAWARVPN
REDACTED			REDACTED
DOD NSOC	Technical Issues and Support Contacts	REDACTED	
REDACTED			REDACTED

Appendix A. Approval Signatures

Signed: _____
REDACTED, Project Manager/Receiving Organization

Signed: _____
REDACTED, Product Owner

Appendix B. Acronyms and Abbreviations

[Table 14](#) lists the acronyms and abbreviations used throughout this document and their descriptions.

Table 14: Acronyms and Abbreviations

Acronym	Description
A&A	Authentication and Authorization
AD	Active Directory
AITC	Austin Information Technology Center
API	Application Program Interface
APM	Application Performance Management
AWIV	Advanced Web Image Viewer
AWS	Amazon Web Services
BHIE Relay Service (BRS)	Bidirectional Health Information Exchange
BPE	Business Partner Extranet
BRS	BHIE Relay Service
CA	Computer Associates
CAC	Common Access Card
CAPRI	Compensation and Pension Records Interchange
CCOW	Clinical Context Management Specification
CDR	Clinical Data Repository
CHCS	Composite Health Care System
CLI	Command Line interface
CLS	Central Logging Solution (VAEC)
CHG	Change Order
CPRS	Computerized Patient Record System
CVIX	Central VistA Imaging Exchange
DAS	Data Access Service
DB	Database
DES	Data Exchange Service
DIBRG	Deployment, Installation, Backout, and Rollback
DISA	Defense Information Systems Administration
DMDC	Defense Manpower Data Center
DMIX	Defense Medical Information Exchange
DOB	Date of Birth
DOD	Department of Defense
ECR	Elastic Container Registry
ECRS	Enterprise CAC Registration Service

Acronym	Description
ECS	Elastic Container Service
EDIPI	Electronic Data Interchange Personal Identifier
EHR	Electronic Health Record
EHRM	Electronic Health Records Modernization
EKG	
ESD	Enterprise Service Desk
FEHR	Federal Electronic Health Record
FHIR	Fast Healthcare Interoperability Resources
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GB	Gigabytes
Github	Github is a web-based hosting service for software development projects that use the Git revision control system
GUI	Graphical User Interface
GTM	Global Traffic Manager
HAIMS	Healthcare Artifact and Image Management Solution
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
HPS	Health Product Support
HTML	Hypertext Markup Language
HTTPD	Apache HyperText Transfer Protocol (HTTP)
HTTPS	HyperText Transfer Protocol Secure
ICAM	Identity, Credential, and Access Management
IAM	Identity and Access Management
ICN	Integration Control Number
IEN	Internal Entry Number
ID	Identification
IO	Infrastructure Operations
IP	Internet Protocol
ISO	Information Security Officer
IT	Information Technology
JDBC	Java Database Connectivity
Joint HIE, JHIE	Joint Health Information Exchange
JLV	Joint Longitudinal Viewer
LDAP	Lightweight Directory Access Protocol
MedCOI	Medical Community of Interest
MESOC	MHS Enterprise Services Operations Center

Acronym	Description
MHS	Military Health System
MI	Middle Initial
MS	Microsoft
MS SQL	Microsoft Structured Query Language
MPI	Master Person Index
NSC	Network Support Center
NSOC	Network Security Operations Center
OIT	Office of Information Technology
ORR	Outage Readiness Review
OS	Operating System
PAAS	Platform as a service
PCMM	Primary Care Management Module
PDWS	Patient Discovery Web Service
PHI	Protected Health Information
PIN	Personal Identification Number
PITC	Philadelphia Information Technology Center
PIV	Personal Identity Verification
PM	Project Manager
POC	Point of Contact
POM	Production Operations Manual
QoS	Quality of Service
RAM	Random Access Memory
RDS	Amazon Relational Database Service
REST	REpresentational State Transfer
RPC	Remote Procedure Call
SAS	Statement on Auditing Standards-70
SDD	System Design Document
SDM	Service Desk Manager
SNOW	Service Now
SOAP	Simple Object Access Protocol
SPAWAR	Space and Naval Warfare Systems
SQL	MS Structured Query Language
SSMS	SQL Server Management Studio
SSN	Social Security Number
SSOi	Single Sign on Internal
TBD	To be determined
TCP	Transmission Control Protocol
TMDS	Theater Medical Data Store

Acronym	Description
URL	Universal Resource Locator
VA	Department of Veterans Affairs
VAAFI	VA Authentication Federation Infrastructure
VAEC	VA Enterprise Cloud
VBA	Veterans Benefits Administration
VDD	Version
VDS	VistA Data Service
VHA	Veterans Health Administration
VistA	Veterans Information Systems and Technology Architecture
VM	Virtual Machine
VPS, VPC's	Virtual Private Cloud(s)
VPN	Virtual Private Network