Clinical Health Data Repository (CHDR) Modernization

Technical Manual

February 2023

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

NOTE: The revision history cycle begins once changes or enhancements are requested after the document has been baselined.

Date	Revision	Description	Author

Table of Contents

List of Figures

List of Tables

1. Introduction

The Clinical Data Repository (CDR)/Health Data Repository (HDR) is an interagency application used to exchange Allery and Pharmacy domain patient data between the Department of Defense's (DoD) CDR, and the Department of Veterans Affairs (VA) HDR for patients marked as Active Dual Consumers (ADC). Patient data for Allery and Pharmacy domains are maintained in the centralized repository of each agency, CDR and HDR, hence the acronym CHDR.

The CHDR application is the link between the CDR and HDR repositories providing a bidirectional exchange of standards-based, computable data as close to real-time as systems will allow for Veterans and beneficiaries marked as ADC patients

1.1. Purpose

This technical manual will provide information regarding the implementation, maintenance, and system overview for the CHDR software. This guide will be used to help familiarize users with the important features and navigational elements of the CHDR software. With the help of this document, developers and technical personnel will be able to operate and maintain the CHDR software with minimal assistance from product support personnel.

1.2. System Overview

The CDR/HDR is an interagency application used to exchange Allery and Pharmacy domain patient data between the DoD CDR and the VA HDR for patients marked as ADC.

- Clinical Data Repository (CDR) – stores DoD medical records entered and maintained in the DoD TRICARE system and is a component of the Armed Forces Health Longitudinal Technology Application (AHLTA).
- Health Data Repository (HDR) - stores VA medical records entered and maintained in the Computerized Patient Record System (CPRS) and Veterans Information Systems and Technology Architecture (VistA).

VA CHDR was aligned with the legacy VLER CORE architecture and enterprise services and was designed with a Service-Oriented Architecture (SOA), which deploys components called services to perform distinct business functions. To enhance the business processes, CHDR combines existing systems with a service interface. The processes are executed as a sequence of heterogeneous process steps, coordinated by the Enterprise Service Bus (ESB) infrastructure. The ESB is middleware that provides fundamental services for complex architectures such as SOA and CHDR.

Each VA medical center uses the VistA and CPRS applications for patient data registration and management. Each VA Medical Center (VAMC) VistA site has its own local interface engine, which connects with the VAHC enterprise interface engine for enterprise data distribution to the VA CHDR application. Figure one below shows a system overview of the CHDR program.

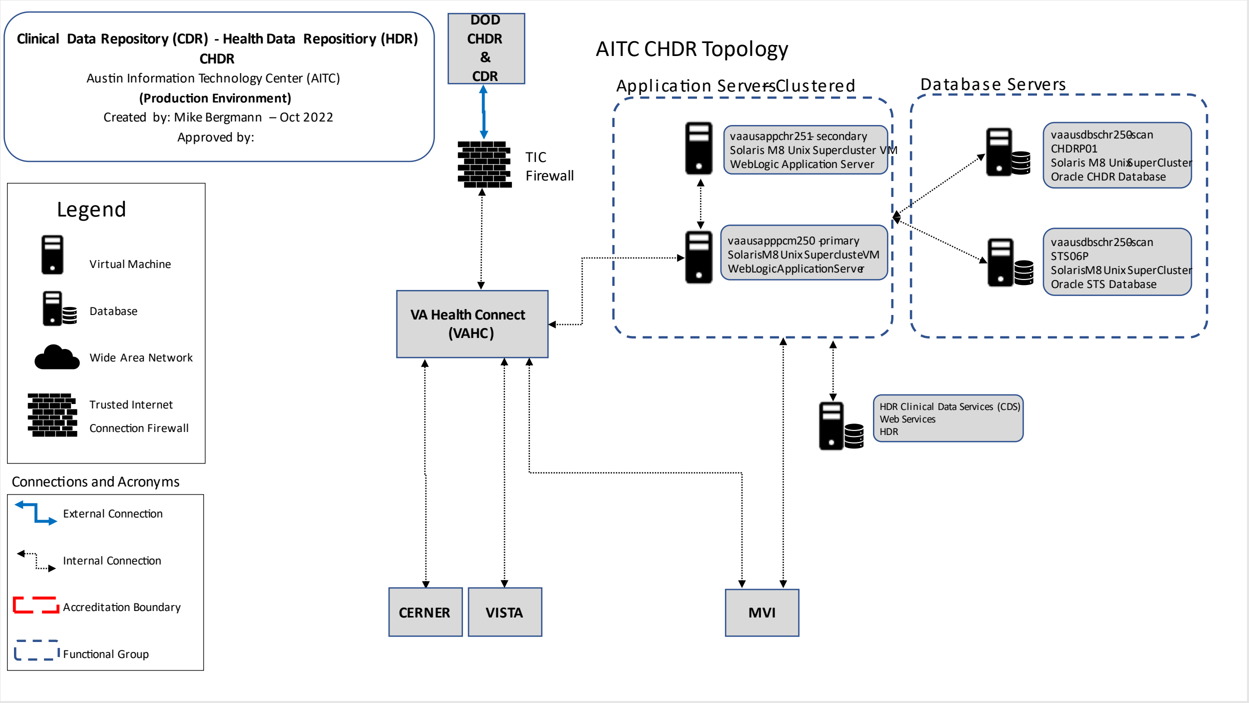

Figure 1: AITC CHDR Topology

1.3. Document Orientation

- *Audience:* The intended audience for this Technical Manual is local IT Support, management, and development personnel for the CHDR software.
- *Assumptions:* As this manual is intended to help support individuals in understanding the CHDR program, the following knowledge is assumed:
    - A strong understanding of the various development, security, and operations programs within the VA Health Sector.
    - A strong understanding of application server technology services and programs, for example, Unix/Linux, Oracle WebLogic, and Oracle Database.

1.3.1. Disclaimers

1.3.1.1. Software Disclaimer

This software was developed at the Department of Veterans Affairs (VA) by employees of the Federal Government in the course of their official duties. Pursuant to title 17 Section 105 of the United States Code, this software is not subject to copyright protection and is in the public domain. VA assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. We would appreciate acknowledgement if the software is used. This software can be redistributed and/or modified freely provided that any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified.

1.3.1.2. Documentation Disclaimer

The appearance of external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs (VA) of this Web site or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of the VA.

1.3.2. References

The following are a list of references and documents that were used in preparation for this technical manual (**Note:** All these documents can be found on the internal VA CHDR SharePoint site.)

- System Requirements Specification (SyRS) for the Department of Defense Clinical Data Repository and the Department of Veterans Affairs Health Data Repository (March 2009)
- VHA Clinical Data Repository/Health Data Repository Business Requirements Document (BRD) (April 2009)
- VistA Interface Engine Interface Control Document (July 2009)
- Transition Plan CHDR Application (August 2017)
- Transition Plan CHDR Architecture (August 2017)
- Transition Plan Environments (August 2017)
- Integration Requirements Specification Document (March 2018)
- Integration Requirements Specification Document (February 2020)
- CHDR Version 2.2 Installation Guide (October 2021)
- CHDR Developer's Guide (July 2021)
- Software Design Document (SDD) CHDR Version 2.2.0 (January 2022)
- Application and Architecture Information (March 2022)

2. Implementation and Maintenance

The CHDR application is a data transfer application without user interface involved. Access to the patient data transferred by CHDR is achieved through VistA and Cerner access to HDR. The CHDR application is transparent to the user and operates continuously transferring data between the DoD and VA.

The implementation of CHDR will require the capability to communicate with external dependencies utilizing various interfaces built into the CHDR application and platform on which CHDR is deployed. Maintenance of the CHDR application will include supporting Austin Information Technology Center (AITC) administration teams, dependent component teams, and the CHDR development/sustainment teams. The CHDR development team will address defects discovered in the application and maintain the CHDR application Technical Reference Model (TRM) and Fortify compliance to satisfy ATO requirements.

Dependent communications to external services use infrastructure and delivery services for messaging based asynchronous communications. The following are brief descriptions of the CORE services used by CHDR in the ESB architecture:

- VHAC service supports the transmission and routing of all HL7 messages by interfacing with the CHDR Java Message Service (JMS) configuration to transfer data to and from the DoD, Master Veteran Index (MVI), and VistA.
- Delivery Service for messaging based asynchronous communications to Master Patient Index (MPI) is a component of the MVI. For MPI Delivery Service communications, the CHDR application uses the DeliveryServiceInboundQueue and the DeliveryServiceOutboundQueue. There exists the Interface Engine Framework (IEF), managed by the VA HealthConnect team that reads and writes to the Delivery Service queues in conjunction with the DefaultNonXAQueueConnectionFactory and DefaultQueueConnectionFactory components of the Java Messaging System (JMS) configuration.
    - **Note:** The MVI is the authoritative source for person identity data. The MVI maintains identity data for persons across VA systems, provides a unique universal identifier for each person, stores identity data for each system where a person is known, provides a probabilistic matching algorithm, and includes the MPI, Person Service Identity Management (PSIM), and Toolkit (TK). It maintains a primary view of the individual's identity data.
- HDR Clinical Data Services (CDS) is the web service used by CHDR to interface with HDR to update allergy and pharmacy data from the DoD. The CDS web services are also used to retrieve the allergy and outpatient pharmacy data updates generated and stored in HDR by VistA.
- Standard Terminology Service (STS) (formerly Standards Data Services (SDS)) manages all content mapping that defines terminology used for VistA applications. CHDR utilizes STS and mediates terminology data received from the DoD into terminology used at the VA, as well as mediates terminology data from the VA into terminology used in the DoD. Access to the content is by service-based queries or service-provided database views via accessing the STS database directly.
- As CHDR only receives data from VistA via VAHC, VistA communications with the CHDR application by using the VistAOutboundQueue. When end users enter allergy and pharmacy data in VistA, the data will then be transferred to VAHC. VAHC will then write the data to HDR and send a copy of the data to the VistAOutboundQueue JMS queue of the VA CHDR application.
- DoD CHDR communicates using the DoDInboundQueue and the DoDOutboundQueue JMS queues. DoDInboundQueue is the queue used to write processed data from VA CHDR to be sent to the DoD. VAHC reads the data on the DoDInboundQueue and delivers it to the DoD. The DoDOutboundQueue reads data messages delivered by VAHC for data incoming from DoD.

- Data Sources are the WebLogic mechanism that connect to the CHDR and STS database schemas. The CHDR WebLogic platform uses three data sources for schema access: *DefaultNonXADataSource*, *DefaultXADataSource*, and the *STS CHDR_Client dataSource*. These data sources are used by various CHDR components for data storage, data reference, and transaction services.

The following graphic illustrates the data flow for the messages exchanged as described in this CHDR application overview.

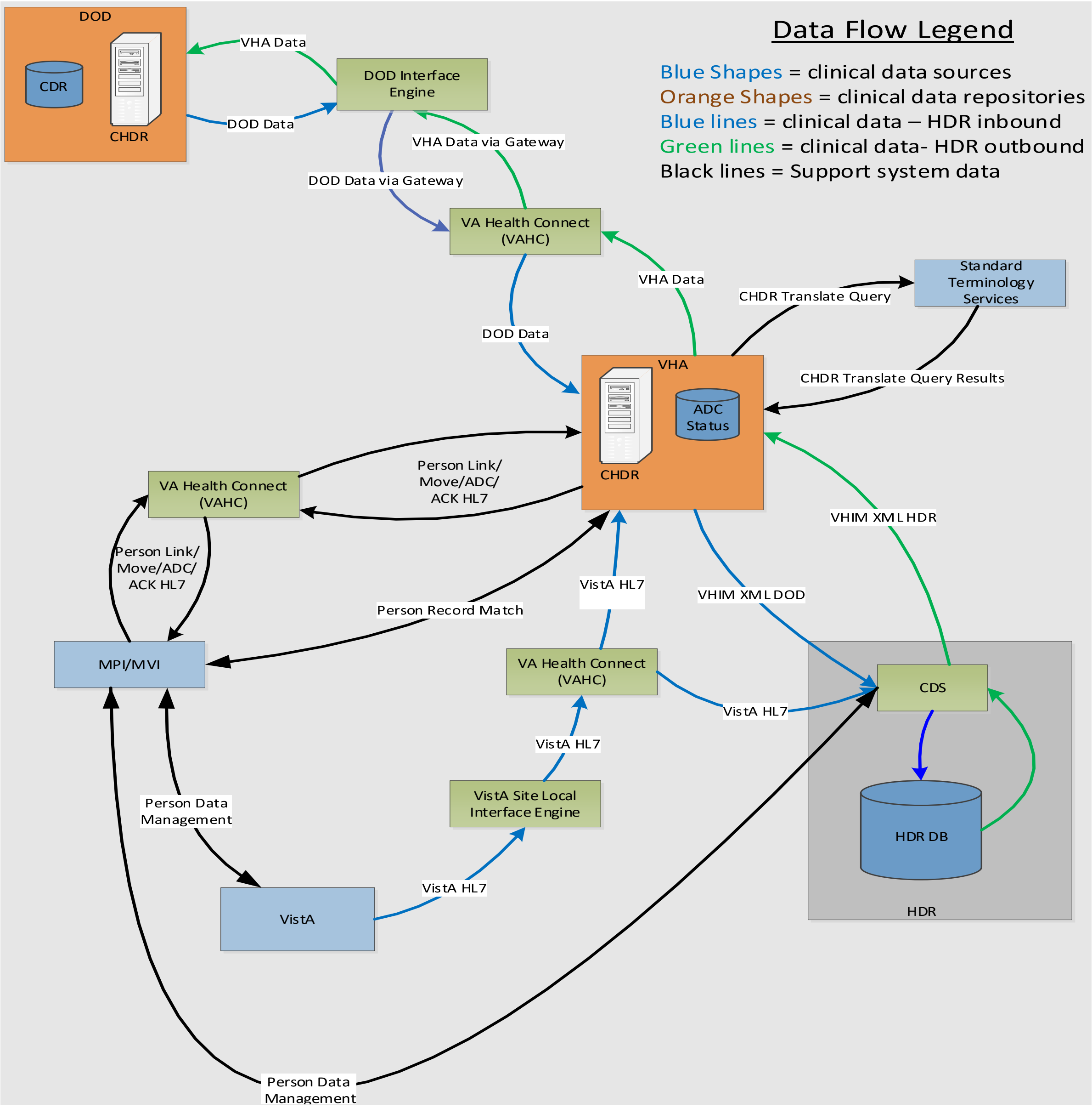

Figure 2: Message Data Flow

Table 1: Production Systems References

Figure Description	Component	Description
VistA	VAMC Sites	Each VA Medical Center uses the VistA system for patient data registration and management.
Enterprise VA Health Connect JMS Interface	Enterprise VAHC JMS Interface	Receives VistA data from field VAMC local VHAC model and writes data to HDR and a copy of the same data to the CHDR Java Message Service (JMS) VistAOutboundQueue as described in the transition plan Architecture Overview document.
HDR	Health Data Repository	VA data repository for all patient data domains.
CHDR Database (DB) and Application Servers	VA CHDR WebLogic domain and database servers	This diagram component represents the servers directly related to the CHDR application. CHDR components consist of the WebLogic Application servers used to manage the CHDR domain. The WebLogic domain is configured with data sources to access the CHDR and STS database schemas.
MPI VA HealthConnect JMS Interface	Enterprise VAHC JMS Interface	VAHC models which control the interface between CHDR and the Master Patient Index (MPI) (inbound/outbound) for patient trait verification, ADC activation requests, link, unlink and move messages as described in the transition plan Application Overview document. The VAHC models read and write to the CHDR JMS DeliverServiceInboudQueue and the DeliveryServiceOutboundQueue queues.
MPI/MVI	VA Production Identity Systems	MVI - The Master Veteran Index (MVI) is the authoritative source for *personal identity data*. It maintains identity data for persons across VA systems, provides a unique universal identifier for each person, stores identity data as correlations for each system where a person is known, provides a probabilistic matching algorithm, and includes the MPI, Person Service Identity Management (PSIM), and Toolkit (TK). It maintains a “gold copy” known as a “Primary View” of the person’s identity data. The MPI also correlates with the Defense Enrollment Eligibility Reporting System (DEERS)/ Defense Manpower Data Center (DMDC) DoD Identity System and assigns station IDs 200DoD and 200CH to indicate patient active dual consumer characteristics. CHDR utilizes the MPI services with a direct connection versus the JMS queues for patient validation and identification.

Figure Description	Component	Description
ETS/STS	Enterprise Terminology Services/Standards Terminology Services	Systems that house terminology mapping used for terminology mediation between DoD and VA data during CHDR data processing. CHDR uses these maps to translate VA allergy and pharmacy terminology into DoD terms as well as translate DoD terminology into VA terms.
HDR CDS Web Services	HDR Clinical Data Services	These web services are administered by HDR and act as the VA CHDR interface to HDR for data queries and updates. CHDR utilizes these services to write processed DoD data to HDR and read historical patient data from HDR to provide to the DoD.
VA CHDR HealthConnect VA to DoD and DoD to VA Models	Enterprise VAHC JMS Interface	VAHC is the interface between DoD CHDR NexGen COTS component and VA CHDR WebLogic JMS DoDInboundQueue and the DoDOutboundQueues.
VA-DoD Gateway	Network component connecting the DoD to the VA.	The VA-DoD Gateway is the network component used to control and secure the connection between the VA and the DoD for various interagency systems including the CHDR connection.
DOD NexGen CHDR Application	DOD Commercial Off the Shelf (COTS) application.	The DOD team has replaced the legacy DOD CHDR application, DOD Data Movement Manager and VA gateway Interface components with a new COTS product that performs all 3 functions in one application.
CDR	Clinical Data Repository	DoD data repository for all patient data domains.
DEERS/DMDC	DoD Production Identity Systems	DoD equivalent system to the VA MPI/MVI system.
AHLTA and CHCS	DoD Medical Facility Site Systems	DoD AHLTA and Composite Health Care System (CHCS) are systems used at DoD medical facilities used for patient registration and data management.

2.1. System Requirements

The CHDR application is a JAVA application centrally deployed in AITC. The high-level system requirements for this application relates to the transmission of allergy and pharmacy payload messages and the acknowledgment of respective from each respective agency. The message pair requirements are described in the HL7 Messages section of this document.

2.1.1. Hardware Requirements

The CHDR application is deployed on the Solaris M8 Unix Supercluster. The CHDR application requires two application servers and a database server for production, and only one application and database server for development and Software Quality Assurance (SQA)/PreProd environments.

Application server requirements are satisfied by using the Oracle WebLogic middleware platform that is capable of load balancing and failover clustered WebLogic virtual machines. The current production environment includes two machines with three managed servers running on each machine. In SQA and development (DEV) environments, only one machine with three managed servers are installed per environment.

In the local CHDR development environment, a government furnished equipment (GFE) Windows-based laptop is configured with Eclipse Integrated Development Environment (IDE), the Oracle WebLogic Server, interfaces with external dependent components when available, and uses a test harness to simulate external dependent components when not accessible.

2.1.2. Software Requirements

The CHDR application is a JAVA-based application and operates on the Oracle Weblogic platform on the Solaris M8 Unix Supercluster. CHDR depends on the DoD, VistA, STS, MVI, and HDR external systems. Parameters used by the CHDR application to support these connections are included in a core.properties file located in the CHDR domain applications directory.

Software version requirements are driven by TRM compliance and Software Assurance (SWA) vulnerability compliance requirements in the VA. The application will be updated and sustained as necessary for any TRM and SWA compliance updates of the OS, JAVA, Oracle WebLogic, and Oracle Database. The software development process includes making changes to the application on a GFE development laptop and performing local testing utilizing the Eclipse IDE, along with the CHDR Junit tests and CHDR test harnesses integrated in the code builder.

The CHDR application uses the VA Enterprise Cloud (EC) version of GitHub to perform code configuration management. Developers utilize the CHDR GitHub repositories to download code branches. Upon successful local testing, the code is delivered back to the respective GitHub site where configuration management can merge multiple change branches into the GitHub master branch.

Along with these data sources, CHDR also utilizes JMS technology to read and write patient messages to external interface engines. These interface engines read and write to the CHDR JMS queues to perform patient messages transfers to their respective endpoints. The CHDR

WebLogic domain is configured with the legacy standard Veterans Health Information Exchange (VHIE) JMS module developed for many applications and used by the CHDR application. The application interfaces with VistA, the DoD, and MVI using the JMS module queues. The CHDR application does not connect directly to the external dependent components; however, it reads from and writes to the internal WebLogic JMS queues where the VAHC team reads and writes messages to the external components. To maintain data/message persistence, the CHDR JMS configuration also utilizes the persistent store functionality included in the WebLogic platform. Persistent Stores are created and associated with a respective JMS server and each JMS server targets a respective WebLogic Managed Server.

The current VA CHDR SQA test environment is integrated with the DOD CHDR SQA components via VAHC for end-to-end testing of the application. It is important to note that the integrated test environments include other test versions of health support systems of the DoD and VA such as AHLTA, VistA, Composite Health Care System (CHCS), CPRS, CDR, HDR, Defense Enrollment Eligibility Reporting System (DEERS)/ Defense Manpower Data Center (DMDC), MPI and Cerner.

2.1.3. Database Requirements

The CHDR application uses the Oracle Database which resided on the Solaris M8 Unix Supercluster located in AITC. The two Oracle databases used are the CHDR database and the STS database. Both reside on separate virtual machines, and both are accessed via the Java Database Connectivity (JDBC) data sources defined in the WebLogic CHDR domain.

The WebLogic domain is configured with three data sources, each configured with a Java Naming Directory Interface (JNDI) used by the code to leverage the WebLogic data sources for accessing each respective database.

CHDR components consist of the WebLogic Application servers used to manage the CHDR WebLogic domain. The WebLogic domain is configured with data sources to access the CHDR database (DB) schema.

In the current production environment, CHDR does not utilize failover data sources and relies on one connection to the CHDR database. SQA and DEV environments are configured with “Multi” data sources and are set up to handle two different database instances in case one fails.

The names of the data sources in production and the Multi data sources in SQA and DEV are:

- `DefaultNonXADataSource`
- `DefaultXADataSource`
- `CHDR_service_1`

2.2. System Setup and Configuration

In production, CHDR requires an application server platform capable of load balancing and failover. To support this requirement, the CHDR platform utilizes Oracle WebLogic to deploy multiple managed servers across multiple machines. The current production environment includes two machines, with three managed servers running on each machine. In SQA and DEV environments, only one machine with three managed servers are installed per environment.

The CHDR application requires access to predefined data sources. WebLogic provides the capability to define these data sources and utilize JNDI technology in the code for reference to these data sources.

Along with these data sources, CHDR also utilizes JMS technology to provide patient messages to external interface engines. These interface engines read and write to the CHDR JMS queues to perform patient messages transfers to their respective endpoints.

The current directory structure on CHDR machines is as follows:

- `APPLICATION_HOME = /u01/app/install` --- contains deployable CHDR applications support files.
- `DOMAIN_HOME = /u01/app/domains/<chdr domain name>` --- contains the WebLogic domain created for the respective environment.
- `DOMAIN_HOME/applications` – contains CHDR application component properties files.
- `WL_HOME  = /u01/app/oracle/<installation directory>` --- contains the WebLogic installation and supporting tools to administer WebLogic domains.
- `JAVA_HOME = /u01/app/oracle/java/latest` --- points to the latest installation of JAVA.

To set up the System, the following must be completed:

1. **WebLogic Installation and configuration**: AITC Administrators and CHDR development and sustainment personnel with approved elevated permissions work together to perform patching and software installations in each respective environment. JAVA is installed in a 'WebLogic' user-owned directory for better versatility if/when JAVA updates are required.
2. To execute any operating system-level procedures, a TRM compliant terminal emulator is used to connect to the respective host. Authentication will take place based on Electronic Permissions Access System (ePAS) approved elevated privileges and credentials. The required switch user command to execute elevated permissions is the 'dzdo' command. Only AITC administrators have exclusive permissions to switch to the root user; however, non-AITC administrators with approved ePAS permissions could prefix system-level commands with the 'dzdo' command to allow system-level maintenance and troubleshooting in the lower environments where and when necessary. Non-AITC administrators can also elevate their permissions to be a 'WebLogic' or 'oracle' user by utilizing the following commands:

   `dzdo su` – WebLogic

   `dzdo su` – oracle

3. **Install JDK**: Following the Continuous Readiness in Information Security Program (CRISP) initiative and TRM compliance requirements, system administrators must identify the appropriate version of JAVA and install it in the */u01/app/oracle/java* directory. After installation, a symbolic link */u01/app/oracle/java/latest* should be

created and point to the desired version of JAVA within the same */u01/app/oracle/java* directory.

   a. ln *-s /u01/app/oracle/java/jdk1.8,0_xxx /u01/app/oracle/java/latest*, the */u01/app/oracle/java/latest* will be used in the WebLogic configurations to minimize impact to JAVA updates and/or changes.

4. WebLogic installation details can be obtained from the Oracle's documentation site. The desired WebLogic 12c installation file will be retrieved from production support to ensure proper licensing.
5. In production, the installation must be performed on both production machines.
6. Oracle has decommissioned command line "console" installations and AITC has restricted the use of graphical user interface support on the Solaris servers. Therefore, a silent install is executed using a response file from the command line. An example of silent install command: *java -jar <distribution_name.jar> -silent -responseFile <response filename>*
7. The WebLogic middleware should be patched as recommended by TRM, CRISP, and Oracle installation requirements. The AITC administrators will retrieve the WebLogic installation and patch files from oracle support since they hold the Oracle support contract credentials.
8. When the WebLogic installation is completed, check for the patches available for the installed version of WebLogic.
9. The new WebLogic server home instance will be in directory: *WLS_HOME = <WL_HOME>/wlserver*
10. A CHDR domain must be created in each environment. Since the Oracle's console mode is no longer available from Oracle, and security restriction prevent AITC servers from X-server configurations, graphical user interface (GUI) tools are no longer available. The current approach to creating CHDR domains is to utilize the WebLogic Scripting Tool (WLST) to create a basic domain. A basic domain will provide access to a WebLogic console where the rest of the CHDR components can be installed manually.

    a. A prerequisite to creating the domain is to obtain or create a domain template jar file to be used in the WLST tool. If an existing domain template cannot be generated from an existing CHDR domain, a default template is provided with the WebLogic software installation.

11. The basic domain template delivered with the WebLogic middleware is:
    `<WLS_HOME>/common/templates/wls/wls.jar`
12. To create the domain, start WLST by executing the following at the unix command prompt:

    ```
    cd <WL_HOME>/oracle_common/common/bin
    ```

    ```
    ./wlst.sh
    ```

13. At the *wls:/offline>* prompt, enter the following command:

createDomain (‘<*path to domain_template*>’, ‘DOMAIN_HOME’, ‘<*weblogic username*>’,’<*weblogic pwd*>’);

```
chdr.12c
```

14. After creating the domain, record the WebLogic username and password. Typically, the default user is ‘WebLogic’, and the password is chosen by the installer. Additional administrator names can be added to the WebLogic Security Realm to avoid generic logins to the console.

Once the domain is created and a WebLogic console is accessible, the following steps can be performed:

1. **Create machines**: In the production create two machines. In DEV and SQA, create one machine per environment.
2. **Create managed servers**: In production create six managed servers:

<*chdr domain name*>.ms1 - <*chdr domain name*>.ms6. Assign <*chdr domain name*>.`ms1` – <*chdr domain name*>.`ms3` to one machine and <*chdr domain name*>.`ms4` - <*chdr domain name*>.`ms6` to the other machine.

3. In the DEV and SQA environments, create three managed servers: <*chdr domain name*>.`ms1` - <*chdr domain name*>.`ms3`. for each environment. Only one machine is created on each DEV and SQA domain.
4. Configure each domain with a cluster and assign all respective managed servers to their respective cluster.
5. For each machine configured in a domain, identify the host name and the Node Manager Listener port.
6. In production, create a template of managed servers for Machine Two based on the machines created in the previous steps. Use the WebLogic ‘pack’ and ‘unpack’ utilities to enroll the machines in the Nodemanager configuration.
7. On Machine One, go to directory *WL_HOME/oracle_common/common/bin* and execute the following command:
    a. **Note:** Command is entered all on one line at command prompt in the UNIX shell.
    b.
    ```
    ./pack.sh –domain=DOMAIN_HOME  -
    template=<APPLICATION_HOME>/chdr.prod.jar       -
    template_name=”chdr.prod” –managed=true
    ```
8. Transfer the newly created chdr.prod.jar file to the <*APPLICATION_HOME*> directory on Machine Two.
    a. On Machine Two, go to directory WL_HOME/oracle_common/bin and execute the following command:
    ```
    ./unpack.sh –template=<APPLICATION_HOME>/chdr.prod.jar –
    domain=DOMAIN_HOME/chdr.prod
    ```
    b. Use the following commands to enroll the Node Manager on Machine Two with the Node Manger running on machine one.
    c. On Machine One, start the Node Manager and the WebLogic administrator server:

```
cd <DOMAIN_HOME>/bin
nohup ./startNodeManager.sh &
cd ..
```

`./startWebLogic.sh` – enter the username and password defined in the domain creation.

d. On Machine Two, perform the enrollment utilizing the WebLogic Scripting Tool (WLST) as follows:

```
cd <WLS_HOME>/common/bin
./wlst.sh

      connect("weblogic", "<password>", 't3://<machine1
      hostname>:<AdminServer  port>')

nmEnroll('<DOMAIN_HOME>','<DOMAIN_HOME>/nodemanger')
exit()
```

e. Start NodeManager on Machine Two as follows:

```
cd <DOMAIN_HOME>/bin
nohup ./startNodeManager.sh &
```

f. Test access to the WebLogic console URL:

http://<machine 1 hostname>:<AdminServer port>/console

g. In production, verify that the Node Manager recognizes both machines as follows:

In the left panel of the console screen:
Expand Environments
Click on Machines
Click on machine two hostname
Click on the Monitoring tab
Node Manager Status should be Reachable

9. In SQA and DEV environments, start the Node Manager and administration server as follows:

   `cd <DOMAIN_HOME>/bin`

   `nohup ./startNodeManager.sh & cd .../startWebLogic.sh` – enter the username and password defined during domain creation

10. Test access to the WebLogic console URL: *http://<hostname>:<AdminServer port>/console*

11. In all environments, from the WebLogic console, perform a shutdown of the AdminServer.

12. Create the `boot.properties` security file so that the AdminServer can start without a user intervention for a user ID and password during WebLogic startup.

13. In all environments, perform the following to create the boot.properties file:

```
cd DOMAIN_HOME/servers/AdminServer
mkdir security
cd security
```

a. **Note**: insert the following lines into a boot.properties file:

```
echo "username=weblogic" > boot.properties

echo "password=<password>" >> boot.properties
```

14. Verify starting the WebLogic AdminServer without user intervention for user ID and password by restarting the respective AdminServer:

```
cd  <DOMAIN_HOME>/bin
nohup  ./startWebLogic.sh &
```

15. Access the console URL *http://<hostname>:<AdminServer port>/console* and log in.

CHDR Application Installation:

The CHDR deployment consists of deploying the Electronic Archive (EAR) file and the core.properties file. The core.properties file exists in three versions, one for each environment: production, SQA, and DEV.

1. Transfer the CHDR EAR to the SQA server/tmp directory where AITC personnel can access it from production.
2. In production, copy the CHDR EAR file to the APPLICATIONS_HOME directory for deployment. Create the applications directory and put the core.properties file in it with the following commands.
3. *mkdir DOMAIN_HOME/applications/chdr-core cp core.properties DOMAIN_HOME/applications/chdr-core*
4. The following files need to be transferred and distributed to the *DOMAIN_HOME/lib* directory for the CHDR application.

```
com.bea.core.apache.commons.logging_1.1.0.jar
log4j-1.2.15.jar
log4j.xml
resolver.jar
serializer.jar
wlcommons-logging.jar
xalan-2.7.1.jar
xercesImpl.jar
xml-apis.jar
```

5. Log into the WebLogic console.
6. Click the Lock & Edit button.
7. In the Domain Structure window select Deployments.
8. Click the Install button in the Summary of Deployments window.
9. Change the path in the Install Application Assistant to APPLICATIONS_HOME.
10. Click Next.
11. Select the chdr-<version>.ear and click Next.
12. Select Install as Application radio button and click Next.
13. Select the domain cluster for the target and click Next.

14. Modify the Name to chdr-<version>
15. Click the Copy this application onto every target for me radio button.
16. Click Next.
17. Click the “No, I will review the configuration later” radio button.
18. Click Finish.
19. Click Activate Changes.
20. Select the chdr-<version> deployment checkbox and click Start.
21. Select Servicing All Requests.
22. Click Yes to start the deployment.
23. Restart the managed servers.

3. Files

Through the Jenkins build server, the CHDR application is compiled by the Maven compiler into an Electronic Archive (.ear) file. This file is generated, delivered, and deployed on the WebLogic platform for operation.

Upon startup, the .ear file uses an application properties file to determine the CHDR application’s operating environment.

The filenames are:

- `chdr.2.2.x.x.ear` (x’s represent version increments of the build)
- core.properties = application environmental properties and is not necessarily delivered with each build and only delivered when property changes are required.

4. Routines

There are no specific Vista routines required for the CHDR application.

5. Exported Options

No additional files nor exports exist or are required for the CHDR application.

6. Mail Groups, Alerts, and Bulletins

The CHDR application itself does not create mail groups, alerts, or bulletins; however, the CHDR application is monitored with the enterprise AppDynamics application supported by AITC Administrators. The AppDynamics monitoring tool generates alerts and sends them to a pre-defined distribution list, including the AITC Application manager assigned to CHDR, and the Administrators assigned to the CHDR application and database.

7. Public Interfaces

All interfaces to CHDR are internal to the VA and are not public facing.

7.1. Integration Control Registrations

This section is not applicable to CHDR as CHDR does not require Integration Control Registrations (ICR) for changes to deployments.

7.2. Application Programming Interfaces

This section is not applicable to CHDR.

7.3. Remote Procedure Calls

This section is not applicable to CHDR.

7.4. HL7 Messaging

The CHDR application uses Health Level 7 (HL7) messages to send and receive information to and from the software. Flow control between MPI and HealthConnect is provided by use of the HL7 Minimal Lower Layer Protocol (MLLP) for data interchange, including acknowledgement messages. The MLLP protocol relies on the Message Header Segment (MSH) to define encoding, routing, and acknowledgement rules that govern message interchange. The sending system will enclose each HL7 message in MLLP blocks.

To support the CHDR system functionality, seven message types are utilized for the exchange of information between the VA and the DoD CHDR systems. The messages have been assigned Z0x titles to identify the type of message content.

- "Z01" and "Z02" messages are exchanged for setting patient ADC status.
- "Z03" and "Z04" messages are exchanged for current allergy and pharmacy domain data updates.
- "Z05," "Z06," and "Z07" messages are exchanged for historical patient allergy and pharmacy domain data.

Each of these messages is exchanged in the form of an eXtensible Markup Language (XML) HL7 message, which is the standard message format for medical record data. Each Z-message may be described as follows:

- **Z01:** The ADC process for each patient is initiated within the CHDR system of either agency via transmission of a Z01 message to the other CHDR system. A payload included in this message includes, but is not limited to, a patient's traits information, including first and last name, date of birth, and social security number. The internal user interface (ICN) and Electronic Data Interchange Personal Identification (EDIPI) are included in the VA Z01; however, only the EDIPI is included in the DoD Z01. Trait information is used by the receiving system to verify the existence of the patient in its respective medical data system.

- **Z02:** This message is transmitted in an acknowledgement response to a Z01 message and comprises a payload including, but not limited to, the successful or unsuccessful status of a patient validation initiated by the Z01. For a successful patient validation from a Z01, the return Z02 will include a 'Single Match' status. For an unsuccessful patient validation from a Z01, the return Z02 will include a 'No Match' status.
- **Z03:** This message initiates an update of an ADC patient's allergy and pharmacy domain medical data on another system. Each time an ADC patient receives care at an agency's medical facility, their clinical data is updated within the treating agency's repository, and a copy of those updates is sent to the CHDR application for a data transfer. The payload of the Z03 message includes, but is not limited to, patient allergy and pharmacy data. Thus, the Z03 message represents a clinical update, with data being exchanged between the agencies' CHDR systems.
- **Z04:** This message is transmitted in response to a Z03 clinical update message. The message verifies receipt of a successful or unsuccessful processing of the Z03 message.
- **Z05:** This message initiates a one-time batch exchange of clinical data. The initiating system sends the Z05 message to the other system to request a patient's medical data. The message payload includes, but is not limited to, a synchronization flag indicating that the receiving system should send a corresponding Z05 message to the initiating system to complete the batch exchange of data for the patient. Upon receiving the Z05 message, the receiving system verifies the existence of the ADC patient to package the patient's clinical data in a Z06 response message.
- **Z06:** This message is transmitted in response to a Z05 message received by either CHDR system. The message payload includes, but is not limited to, all or a portion of the patient's clinical data contained in a data repository of the transmitting system. Due to the potential amount of clinical data for a patient, the size of a message comprising all such data may be large. Due to limitation of the system or network bandwidth restrictions, multiple Z06 messages may be sent in response to a single Z05 batch exchange request to transmit the patient's full medical record.
- **Z07:** This message indicates that the complete medical record of an ADC patient has been received via the Z06 messages. This message completes a batch exchange of clinical data for the patient which was initiated by the receipt of a Z05 message.

The MVI system provides a set of tools and functionality that provide an interface and allows applications to access patient identity data stored in MVI. CHDR utilizes this functionality to validate patients and transfer ADC activation requests to the DoD CHDR. MPI messages are assigned ADT_A## titles. The messages used between MVI and CHDR are as follows:

- **ADT_A24:** Add Person (Add Correlation) Patient ADC Activation Request
- **ACK_A24:** Acknowledgement of the Add Person (Add Correlation) Request
- **ADT_A24:** Insert 200CH Station #
- **ACK_A24:** Acknowledgement of the Insert 200CH Station #
- **ADT_A24:** Link Patient Information
- **ACK_A24:** Acknowledgement of Link Patient Information
- **ADT_A37:** Unlink an ICN from EDIPI (Unlink Request)
- **ACK_A37:** Acknowledgement of Unlink an ICN from EDIPI (Unlink Request)
- **ADT_A40:** Merge Patient Identifier List
- **ACK_A40:** Acknowledgement of Merge Patient Identifier List
- **ADT_A43:** Move Patient Information Patient Identifier
- **ACK_A43:** Acknowledgement of Move Patient Information Patient Identifier

Note: From a clinical user perspective, these actions happen behind the scenes. CHDR's sustainment staff work with the MPI staff to act when certain cases require manual intervention. If patient data correction is needed, corrections are manually evaluated and corrected. Clinical users may be required to validate MVI links, and move actions are correctly handled when data updates are exchanged between agencies. The following figure shows the active dual consumer patients real-time activity flow.

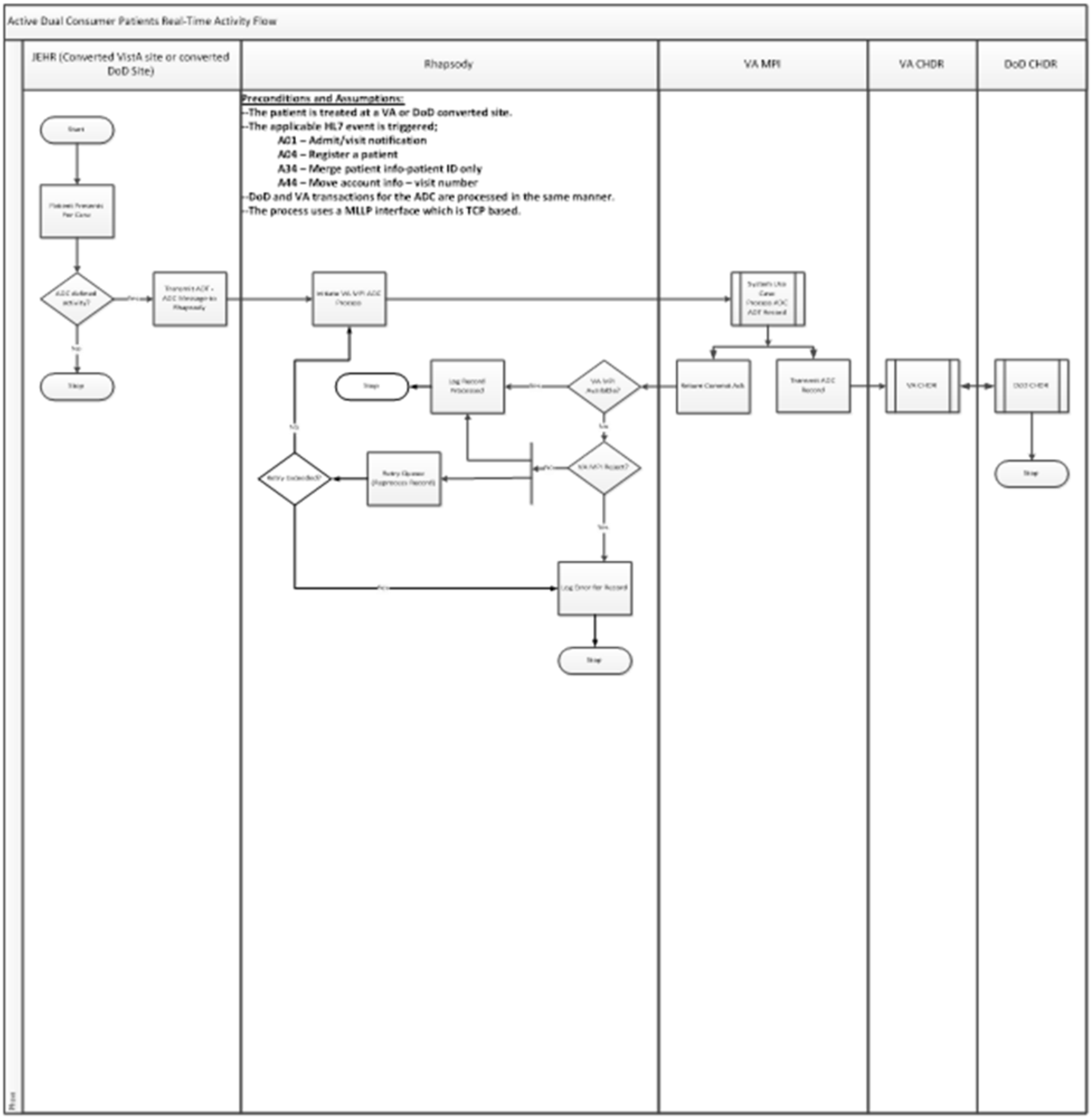
Active Dual Consumer Patients Real-Time Activity Flow
JEHR (Converted VistA site or converted DoD Site)
Rhapsody
VA MPI
VA CHDR
DoD CHDR
Preconditions and Assumptions:
--The patient is treated at a VA or DoD converted site.
--The applicable HL7 event is triggered;
A01 – Admit/visit notification
A04 – Register a patient
A34 – Merge patient info-patient ID only
A44 – Move account info – visit number
--DoD and VA transactions for the ADC are processed in the same manner.
--The process uses a MLLP interface which is TCP based.
Start
Patient Presents For Care
ADC defined activity?
Yes
Transmit ADT - ADC Message to Rhapsody
No
Stop
Initiate VA MPI ADC Process
System Use Case Process ADC ADT Record
Return General Ack
Transmit ADC Record
VA CHDR
DoD CHDR
Stop
VA MPI Available?
Yes
Log Record Processed
Stop
No
VA MPI Reject?
No
Retry Queue (Reprocess Record)
Retry Exceeded?
No
Yes
Log Error for Record
Yes
Stop
Pool

Figure 3: Active Dual Consumer Patients Real-Time Activity Flow

VA MPI ADC Requirements:

1. The VA MPI shall be revised to process HL7 events A34 and A44 in addition to the presently processed A01 and A04 HL7 events.
2. The VA MPI shall transmit the results of the ADC process to the VA and DoD CHDR systems.
3. The VA MPI shall return one of the following results to Cerner:

a. VA MVI ACK

b. MVI Available Error

c. MVI Unavailable

7.5. Web Services

The external systems on which CHDR depends and is integrated with are the DoD, VistA, STS, MVI, and HDR systems. Parameters used by the CHDR application to support these connections are included in a core.properties file located in the CHDR domain applications directory. The CHDR domain specifics can best be exemplified in the CHDR 2.2 Installation guide located on the internal CHDR VA website.

CHDR uses the following web services:

- VA HealthConnect (VAHC) Interface service supports the transmission and routing of all HL7 messages by interfacing with the CHDR JMS configuration to transfer data to from DoD, MVI, and VistA.
- Delivery Service for messaging based asynchronous communications to MPI a component of the MVI. For MPI Delivery Service communications, the CHDR application uses the DeliveryServiceInboundQueue and the DeliveryServiceOutboundQueue. The VAHC component reads and writes to the delivery service queues in conjunction with the DefaultNonXAQueueConnectionFactory and DefaultQueueConnectionFactory components of the JMS configuration.
- HDR Clinical Data Service (CDS) is the web service used by CHDR to interface with HDR by writing allergy and pharmacy data from the DoD into HDR. The CDS web services are also used to retrieve the historical allergy and outpatient pharmacy data from HDR in order to provide it to DoD.
- STS (formerly SDS) manages all content mapping that defines terminology used for VistA applications. CHDR utilizes STS and mediates terminology data received from DoD into terminology used at the VA, as well as mediates terminology data from the VA into terminology used in the DoD. Access to the content is by service-based queries, service-provided database views, or by subscribed updates from STS via a WebLogic data source which connects to the STS database.
- VistA communications with the CHDR application in a single process: VistA to VAHC to the VA CHDR. When end users enter allergy and pharmacy data in VistA, VistA will send that data to HDR via VAHC, and VAHC will send a copy of that same data to VA CHDR via VistAOutboundQueue.
- DoD CHDR communications use the DoDInboundQueue and the DoDOutboundQueue JMS queues via VAHC. DoDInboundQueue is the queue used to write processed data from VA CHDR to be sent to the DoD, while the DoDOutboundQueue is the queue used to read messages from the DoD via VAHC.
- Data Sources are the WebLogic mechanism to connect to the CHDR database schema. There are three WebLogic data sources used by CHDR for data processing and message

transfer: DefaultNonXADataSource, DefaultXADataSource, and the CHDR_service_1. These data sources are used by various CHDR components for data storage and WebLogic transaction services. These data sources are also used for access to the audited events tables and patient identity cross reference tables of the CHDR schema. The audited events table contain all the messages that have been processed and transferred through the CHDR application, while the patient identity cross reference table contains the ADC status and patient ID numbers.

8. Standards and Conventions Exemptions

All CHDR application developers follow a set of guidelines and standards set out in the Standards and Conventions (SAC) document. All steps followed are then reviewed for quality assurance and software is reviewed with respect to SAC guidelines as set forth by the Standards and Conventions Committee (SACC).

CHDR messages will follow the HL7 2.4 standard with ER7 encoding and utilizes an Interface Control Document (ICD) which contains the definitions for CHDR message content. The ICD describes and outlines the requirements for the Message format and content. It provides information regarding the impacts from the sending and receiving applications and illustrates the concept and sequence of operations, and requirements for communication and message construction. The ICD can be found in the VA CHDR SharePoint page via the intranet.

Assumptions:

- All messaging between VA CHDR and the MPI occurs within the AITC; no messaging will be sent over the VA Wide Area Network (WAN).
- The VAHC team will support transfer of messages formatted according to the ICD.
- The current production HL7 messaging specifications may continue to be used within the test environment.
- All new HL7 message patterns will conform to HL7 version 2.4 standards and will be approved by the HL7 administrator.
- Project VA CHDR development teams will be available to support the new CHDR interface.
- VAHC will support extended ASCII characters as defined by the Standards and Conventions Committee (SACC).
- All sending applications will populate the first sub-component of MSH.3, MSH.4, MSH.5, MSH.6 and MSH.15 with valid values before sending.
- All new HL7 messages will be ER7 encoded.
- The VA network has the capacity available and stability to support the CHDR implementation.
- VAHC shall pass the messages with no special processing of payload contents.

- VAHC will detect, troubleshoot, and correct production outages as well as other exceptional circumstances, including, but not limited to, message duplication, message loss, lost connectivity, and when models go down.

8.1. Internal Relationships

This section is not applicable to the CHDR software.

8.2. Software-wide Variables

This section is not applicable to the CHDR software.

9. Security

The CHDR application does not have a user interface, so this section does not apply.

9.1. Security Menus and Options

The CHDR application does not have a user interface, so this section does not apply.

9.2. Security Keys and Roles

The CHDR application does not have a user interface, so this section does not apply.

9.3. File Security

Security will conform to Department of Veterans Affairs Directive 6102 and VA Handbook 6102 (Internet/Intranet Services). The documents are available at the following links.

- Directive: http://www.va.gov/pubs/directives/Information-Resources-Management-(IRM)/6102d.doc
- Handbook: http://www.va.gov/pubs/handbooks/Information-Resources-Management-(IRM)/6102h.doc
- Change 1 to Handbook: http://www.va.gov/pubs/handbooks/Information-Resources-Management-(IRM)/61021h.doc

9.4. Electronic Signatures

This section is not applicable for the CHDR software.

9.5. Secure Data Transmission

To ensure continuity of the existing ADC business process, Cerner will be required to communicate messages with the VA MPI, thus allowing MPI to forward the information to VA CHDR for allergy and medication sharing between the VA and DoD. The existing legacy VA and DoD systems currently support the sharing of allergy and medication information between VA and DoD for ADC patients using each agency's CHDR systems. ADC patients are simultaneously treated by VA and DoD clinicians.

There are 2 basic types of data transferred by the CHDR system:

- ADC activation traits and electronic IDs
- Allergy and Outpatient Pharmacy

Veterans are assigned ADC Active status through an automated ADC process triggered during a patient registration in a DoD or VA medical facility. The ADC process includes the identity systems from both agencies, external to the CHDR application. These identity systems collaborate and correlate patient data to determine if a patient is to be assigned as ADC Active. In each case, the supporting health care and identity systems provide an activation request message to the respective agency CHDR application and initiates the ADC status activation process.

From the VA perspective, when a patient is registered in VistA, VistA will interface with MVI and update MVI records for that patient. If the update indicates the patient is a potential ADC patient, MVI will submit an ADC Activation request to VA CHDR. VA CHDR will send the respective patient trait information (SSN, DOB, first name, and last name), ICN, and the EDIPI number to DoD CHDR. DoD CHDR will then check the CDR and the DoD identity systems for patient existence and attributes to validate the ADC status. Upon validation, a successful acknowledgement is sent to VA CHDR. VA CHDR will mark the patient ADC Active in a CHDR patient cross-reference table and send a message to MVI indicating the patient should be assign station identification 200CH, which indicates the patient is an ADC CHDR patient.

Once the ADC status is established, VA CHDR will extract the historical data from HDR, format a historical message(s) for that patient, and send this information to DOD CHDR where the data will be stored in the CDR.

From the DoD perspective, when a patient is registered in CHCS systems, CHCS systems will interface with DMDC DEERs DoD identity system and update identity records for that patient. The DMDC DEERs identity system will correlate the patients ID with MVI in the VA via the Bidirectional Heath Information Exchange (BHIE) application. The BHIE application utilizes information in MVI, DMDC DEERS, and the CDR to determine if the patient is a potential ADC patient and if so, sends an ADC request to an ADC activation queue. This queue feeds the ADC activation requests to DoD CHDR and DoD CHDR sends the ADC activation request to VA CHDR. VA CHDR will validate the patient traits against the data in MVI and upon successful validation, will send an acknowledgement back to DoD CHDR, set the ADC status active in the VA CHDR cross reference table, and send an ADC acknowledgment to MVI to assign the patient to 200CH as an ADC active patient.

Once the ADC status is established, DoD CHDR will extract the historical data from the CDR, format a historical message(s) for that patient, and send this information to VA CHDR where the data will be stored in the HDR.

When new or updated information for an allergy or outpatient medication is entered using VistA or CPRS, a message is sent to HDR for storage and a copy to VA CHDR. VA CHDR will determine the ADC status of the patient and if the status is Active, will process the data and send it to DoD CHDR for storage in the CDR. If the patient is not ADC active, VA CHDR will not exchange the data.

Conversely, each time new or updated information for an allergy or outpatient medication is entered using AHLTA/CHCS systems, a message is sent to CDR for storage and a copy to DoD CHDR for processing. DoD CHDR will then determine the ADC status of that patient, and if the status is Active, will process the data and send it to VA CHDR for storage in the HDR. VA CHDR receives the data, validates the patient's trait information with the MVI system, and upon validation stores the data in HDR. If the patient is not ADC active, DoD CHDR will not exchange the data.

During the processing of the updated data, terminology mediation is performed to translate VA terminology into DoD terminology. The reverse is performed during processing in DoD CHDR; terminology mediation is performed to translate DoD terminology into VA terminology. Terminology mediation is performed by utilizing a data map maintained by the Veterans Terminology Standards (VTS) team in the VA and the respective terminology team in the DoD. The respective agency terminology team's work together to ensure terminology mapping is as close to 100% as possible, but constant changes to terminology in both the VA and the DOD prevent a 100% mapping

10. Archiving

This section is not applicable to the CHDR software.

11. Non-Standard Cross-References

Reference Document	Web Link to Source Document
Department of Veterans Affairs (VA) Directive 6102 (Internet/Intranet Services)	http://www.va.gov/pubs/directives/Information-Resources-Management-(IRM)/6102d.doc
Department of Veterans Affairs (VA) Handbook 6102 (Internet/Intranet Services)	http://www.va.gov/pubs/handbooks/Information-Resources-Management-(IRM)/6102h.doc
Change 1 to Handbook	http://www.va.gov/pubs/handbooks/Information-Resources-Management-(IRM)/61021h.doc

12. Troubleshooting

Any issues concerning the installation of Oracle's WebLogic middleware or the CHDR application can initially be addressed in the installation, node manager, admin server, or managed server log files that are created upon startup of each component. Any system resource or network issues will have to be addressed by AITC. All other issues will have to be addressed depending on the errors at hand. As there is no detailed list of possible errors, troubleshooting will have to be accomplished according to any issue reported and/or logged.

If there are no installation or startup errors, but there are still functional issues, refer to the managed server logs for possible indicators of an external dependent system being down or inaccessible. For assistance in resolving an issue, attempt to identify the problem system and contact the administration group or individual responsible for that system.

12.1. Special Instructions for Error Correction

This section is not applicable to the CHDR software.

12.2. National Service Desk and Organizational Contacts

Information Assurance Representatives

Tonia M. Dunker (Booz Allen Hamilton) --- Tonia.Dunker@va.gov

Information Security Officer for CHDR

Christopher Wj. Brown --- Christopher.Brown1@va.gov

AITC Application Manager

Reddy Madipadga, (TISTA Science and Technology Corp.) Reddy.Madipadga@va.gov

AITC WebLogic CHDR Administrators

Pablo Orellana (AITC) --- Pablo.Orellana@va.gov

Dinesh Punyala (SMS) --- Dinesh.punyala@va.gov

Production and SQA VAHC Team group

Roger Dowling (AITC) --- Roger.Dowling@va.gov

Mohamed Mohideen (SMS) --- Mohamed.Mohideen@va.gov

HDR/CDS

Ashit Shah (Leidos) --- Ashit.Shah@va.gov

Cody Steadman --- Cody.Steadman@va.gov

Ajay Kumar (SMS) --- Ajay.kumar@va.gov

STS Support Team

Pauline Ramseur (7Delta) --- Pauline.Ramseur@va.gov

John Zizzo (Mantech) --- John.Zizzo@va.gov

Randal Stewart (7Delta) --- Randall.Stewart@va.gov

Violetta Vardanian (7Delta) --- Violetta.Vardanian@va.gov

MPI Support Team

Danny Reed --- Danny.Reed@va.gov

Christine Chesney --- Christine.Chesney@va.gov

Matt Alderman --- Matt.Alderman@va.gov

Brian Ettinger (ByLight) --- Brian.Ettinger@va.gov

VA CHDR Program Management and Sustainment Support team groups

OIT EPMO Product Support Health T3 Clinical Delta --- OITEPMOProductSupportHealthT3ClinicalDelta@va.gov

DOD CHDR Support Team

Brad Howard (DOD DMIX CHDR PM) --- Bradley.Howard@navy.mil

Jennifer Serafini (DOD CHDR Engineer (USA)) --- Jennifer.l.Serafini.ctr@mail.mil

13. Acronyms and Abbreviations

Acronym	Definition
ACK	Acknowledge
ADC	Active Dual Consumers
AHLTA	Armed Forces Health Longitudinal Technology Application
AITC	Austin Information Technology Center
BHIE	Bidirectional Heath Information Exchange
BRD	Business Requirements Document
B2B	Business-to-Business
CDR	Clinical Data Repository
CDS	Clinical Data Services
CHDR	Clinical Health Data Repository
CHCS	Composite Health Care System
CPRS	Computerized Patient Record System
COOP	Continuity of Operations Plan
CRISP	Continuous Readiness in Information Security Program
DB	Database
DMM	Data Movement Manager
DOB	Date of Birth
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DEV	Development
EAR	Electronic Archive
EDIPI	Electronic Data Interchange Personal Identification

Acronym	Definition
ePAS	Electronic Permissions Access Systems
EC	Enterprise Cloud
ESB	Enterprise Service Bus
ETS	Enterprise Terminology Services
EVIE	Enterprise VistA Interface Engine
GFE	Government Furnished Equipment
GUI	Graphical User Interface
HDR	Health Data Repository
HL7	Health Level 7
ICD	Interface Control Document
IDE	Integrated Development Environment
IEF	Interface Engine Framework
ICN	Internal Control Number
JDBC	Java Database Connectivity
JMS	Java Message Services
JNDI	Java Naming Directory Interface
MPI	Master Patient Index
MVI	Master Veteran Index
MSH	Message Header Segment
MLLP	Minimal Lower Layer Protocol
PSIM	Person Service Identity Management
PSIM	Person Service Identity Management
PAD	Product Architecture Document
SMART	Security Management and Reporting Tool
SOA	Service-Oriented Architecture
SSN	Social Security Number
SWA	Software Assurance
SDD	Software Design Document
SQA	Software Quality Assurance
SACC	Standards and Conventions Committee
SDS	Standards Data Services
STS	Standards Terminology Services
SAC	Standards and Conventions
SyRS	System Requirement Specification
TRM	Technical Reference Model
TK	Toolkit
VA	Veterans Affairs
VAHC	VA Health Connect
VAAFI	Veteran Affairs Authentication Federation Infrastructure
VAMC	Veteran Affairs Medical Center
VDL	Veteran Affairs Software Document Library
VHIE	Veteran Health Information Exchange
VistA	Veterans Information Systems and Technology Architecture
VTS	Veterans Terminology Standards
VLER	Virtual Lifetime Electronic Health Record
VIE	Vitria Interface Engine
WAN	Wide Area Network

Acronym	Definition
WLST	WebLogic Scripting Tool
XML	eXtensible Markup Language

Template Revision History

Date	Version	Description	Author
July 2016	1.1	Updated instructional text to simplify content.	OI&T Documentation Standards Committee
June 2016	1.0	Initial version	OI&T Documentation Standards Committee