

**Home Telehealth Reporting Enhancements (HTRE)
Phase 3**

Integrated Home Telehealth Application (IHTA)

Production Operations Manual (POM)



September 2019

Version 4.0

Department of Veterans Affairs (VA)

Revision History

Date	Version	Description	Author
09/16/2019	4.0	Updated WebLogic Server Version	Liberty IT Solutions
03/04/2019	3.0	Updated Cross-References	Liberty IT Solutions
12/11/2018	2.0	Updated for Build 2	Liberty IT Solutions
09/17/2018	1.0	Initial Version	Liberty IT Solutions

Table of Contents

1. Introduction	1
1.1. Operational Priority and Service Level	1
1.2. Logical System Description	4
1.2.1. Application Components	6
1.3. Physical System Description	6
1.3.1. Database System Description	7
1.4. Software Description	7
1.4.1. Background Processes	8
1.4.2. Job Schedules	8
1.4.3. Dependent Systems	8
2. Routine Operations	9
2.1. Administrative Procedures	9
2.1.1. System Start-up	9
2.1.1.1. Database Start-Up	10
2.1.1.2. Application Start-Up	10
2.1.1.3. System Start-Up from Emergency Shut-Down	10
2.1.2. System Shut-down	10
2.1.2.1. Application Shut-down	10
2.1.2.2. Database Shut-down	11
2.1.2.3. Emergency System Shut-down	11
2.1.2.4. Back-Up Procedures	11
2.1.2.5. Restore Procedures	11
2.1.2.6. Back-Up Testing	12
2.1.2.7. Storage and Rotation	12
2.2. Security / Identity Management	13
2.2.1. Identity Management	13
2.2.2. Access Control	17
2.3. User Notifications	18
2.3.1. Unscheduled System Outage Procedure	19
2.4. System Monitoring, Reporting & Tools	19
2.4.1. Dataflow Diagram	19
2.4.2. Availability Monitoring	20
2.4.3. Performance/Capacity Monitoring	20
2.4.4. Critical Metrics	20
2.5. Scheduled Maintenance	21
2.6. Capacity Planning	21
2.6.1. Initial Capacity Plan	21
3. Exception Handling	21
3.1. Routine Errors	21

3.1.1.	Security Errors.....	21
3.1.2.	Time-outs.....	21
3.1.3.	Concurrency.....	22
3.2.	Significant Errors.....	22
3.2.1.	Application Error Logs.....	22
3.2.2.	Application Error Codes and Descriptions.....	23
3.2.3.	Infrastructure Errors.....	23
3.2.3.1.	Database.....	23
3.2.3.2.	Web Server.....	23
3.2.3.3.	Application Server.....	24
3.2.3.4.	Network.....	24
3.2.3.5.	Authentication and Authorization.....	26
3.2.3.6.	Logical and Physical Descriptions.....	27
3.3.	Dependent System(s).....	28
3.4.	Troubleshooting.....	28
3.5.	System Recovery.....	29
3.5.1.	Restart After Non-Scheduled System Interruption.....	29
3.5.2.	Restart After Database Restore.....	29
3.5.2.1.	Database Start-Up.....	29
3.5.2.2.	Application Start-Up.....	29
3.5.3.	Rollback Procedures.....	30
3.5.3.1.	Backup Selection.....	30
3.5.3.2.	Database Recovery Preparation.....	30
3.5.3.3.	Database Point In Time Restore.....	31
3.5.3.4.	Database Recovery Follow-up – Restart Mirroring; Open Database to User Access.....	31
4.	Operations and Maintenance Responsibilities.....	31
4.1.	Support Structure.....	32
4.1.1.	Support Hierarchy.....	32
4.1.2.	Division of Responsibilities.....	32
4.2.	Support Procedures.....	32
5.	Approval Signatures.....	33

List of Figures

Figure 1: IHTA Architectural Layers.....	4
Figure 2: IHTA Technology Stack.....	5
Figure 3: IHTA Components	6
Figure 4: Environment Overview	6
Figure 5: Dependent Systems	9
Figure 6: IHTA Outage E-mails	18
Figure 7: Current Home Telehealth Interface/Dataflow Diagram	20
Figure 8: IHTA Hardware Architecture.....	28
Figure 9: Overview of IHTA Support.....	32
Figure 10: IHTA Support Levels	32

List of Tables

Table 1: IHTA Incident Priority Levels and Time Frame for Response.....	2
Table 2: IHTA Server Hardware.....	7
Table 3: IHTA Production Software.....	8
Table 4: Enterprise Service and Application Summary.....	9
Table 5: IHTA Permissions	13
Table 6: IHTA Roles.....	14
Table 7: IHTA Authentication and Authorization for Registration Action	27
Table 8: IHTA Authentication and Authorization for Login Action	27
Table 9: IHTA Online Help Files	30

1. Introduction

The Integrated Home Telehealth Application (IHTA) is a web-based system, providing a flexible, maintainable, and resilient platform for Home Telehealth (HT) business functions. IHTA facilitates the management of the Department of Veteran Affairs (VA) Quality Improvement Reports (QIR). IHTA is also used for the development, storage, and retrieval of Veteran Health Administration (VHA) data. Finally, the HT Reports module of IHTA allows users to review and search HT Census and Survey data via various management report options. There are eighteen (18) Veteran Integrated Service Networks (VISN), providing centralized information technology (IT) support to 168 medical centers. IHTA will be used by all VISNs, to ensure a standard way of managing QIRs at all VA facilities.

IHTA is composed of a primary and secondary operational environment. The primary environment is housed at the Austin Information Technology Center (AITC) located in Austin, TX. The secondary environment is housed at the Philadelphia Information Technology Center (PITC) located in Philadelphia, PA. AITC will serve as the main operating site with PITC serving as the failover site as necessary to support the failover of AITC. Each operational environment has the same capacity and is capable of supporting users as if it is the primary site. IHTA is accessible from all VISNs and VHA facilities.

Only authorized users that have been approved by the Home Telehealth National Administrators will be able to access IHTA. Role-based access control is set up and maintained by the administrator at the National/VISN/Facility level ensuring users have access to the appropriate level of information.

1.1. Operational Priority and Service Level

Support will be performed by the REDACTED

The following team members are included in this list: REDACTED

Tier 1 Support will be provided by the ESD Your IT Services. IHTA users with problems that cannot be resolved locally will call the ESD to open a Service Request ticket or report an issue online by using the Your IT desktop icon. Issues not resolved by the Tier 1 Support Team will be assigned to Tier 2 Support. Tier 2 Support for IHTA will include assistance from the Office of Information and Technology (OI&T) Enterprise Program Management Office (EPMO) Health Product Support (HPS) team. Issues not resolved by the Tier 2 support team will be assigned to Tier 3 support. Tier 3 support is the highest level of support for IHTA, which includes business analyst, software testers, system administrators, developers, and database administrators who have specialized technical knowledge of IHTA. Tier 3 support will provide services, such as issue resolution and defect management on all issues/defects that have not been resolved by the Tier 1 and 2 support teams. Any defect found will be logged by Your IT Services and in Rational Tools Concert (RTC) Jazz (as required).

Table 1 outlines the incident priority levels and the time frame period for response:

Table 1: IHTA Incident Priority Levels and Time Frame for Response

Priority Level	Call Received and Time Frame for Response	Priority Level Description
Urgent	<p>During business hours: Service Provider will directly contact Requester.</p> <p>During non-business hours: N/A</p>	<p>An urgent incident is a catastrophic incident of an operating environment where production systems are severely impacted, down or not functioning. Under this scenario, one of the following situations may exist:</p> <ul style="list-style-type: none"> • Loss of production data and no procedural work around exists. • Patient care and/or safety are at risk or damage is incurred. • Complete loss of a core organizational or business process where work cannot reasonably continue.

Priority Level	Call Received and Time Frame for Response	Priority Level Description
High	<p>During business hours: Service Provider will directly contact Requester.</p> <p>During non-business hours: N/A</p>	<p>A high incident is a problem where a system is functioning but in a severely reduced capacity. The situation is causing:</p> <ul style="list-style-type: none"> • Significant impact to portions of the business operations and productivity. • No loss of production data and / or a procedural work around exists. • The system is exposed to potential loss or interruption of service. Includes incidents that significantly impact development and/or production, but where an alternative operation is available.
Medium	<p>During business hours: Average of two (2) business hours or less.</p> <p>During non-business hours: No After Hours Coverage will be provided.</p>	<p>A medium incident is a medium-to-low impact problem, which involves partial non-critical functionality loss. A medium incident impairs some operations but allows the user or an application to continue to function. This may be a minor incident with limited loss or no loss of functionality or impact to the user's operation and incidents in which there is an easy circumvention or avoidance by the end user.</p>
Low	<p>During business hours: Average of eight (8) business hours or less.</p> <p>During non-business hours: No After Hours Coverage will be provided.</p>	<p>A low incident has no impact on the quality, performance, or functionality of the system. Low incidents have minimal organizational or business impact.</p>

1.2. Logical System Description

Application layering generalizes the various functional layers in the architecture (see Figure 1). For IHTA, its HTML-rendered content implements the standard Struts2 web framework, injected with Spring components called business services. IHTA uses HTML 5 and JavaScript to render its content and HTTPS requests are tunneled through a servlet (BlazeDS) connected to a Spring controller. The Spring controller will then interact with a Spring business service, rules engine, workflow engine, and Java Persistence Application Programming Interface (JPA) persistent component.

Figure 1: IHTA Architectural Layers

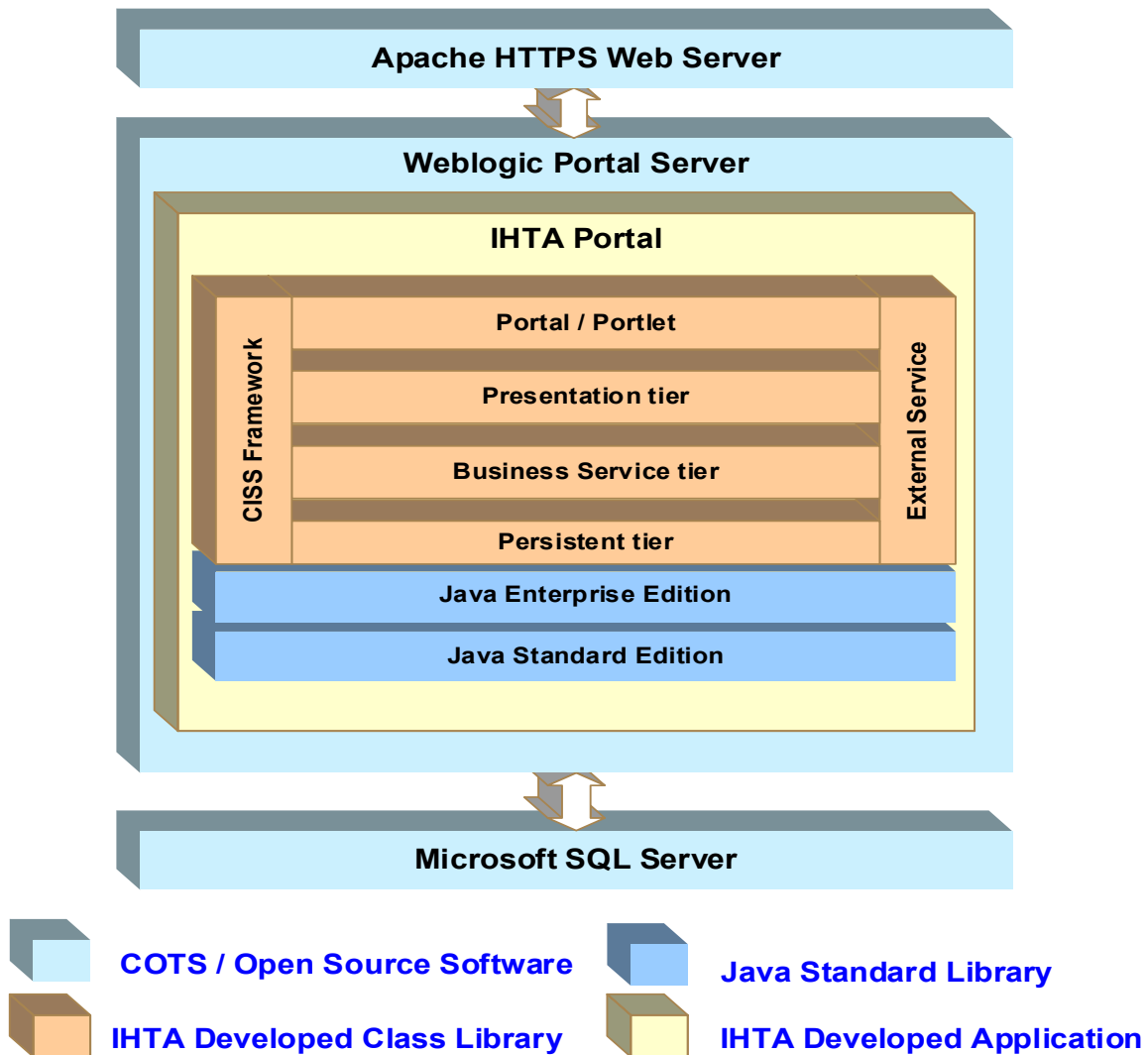
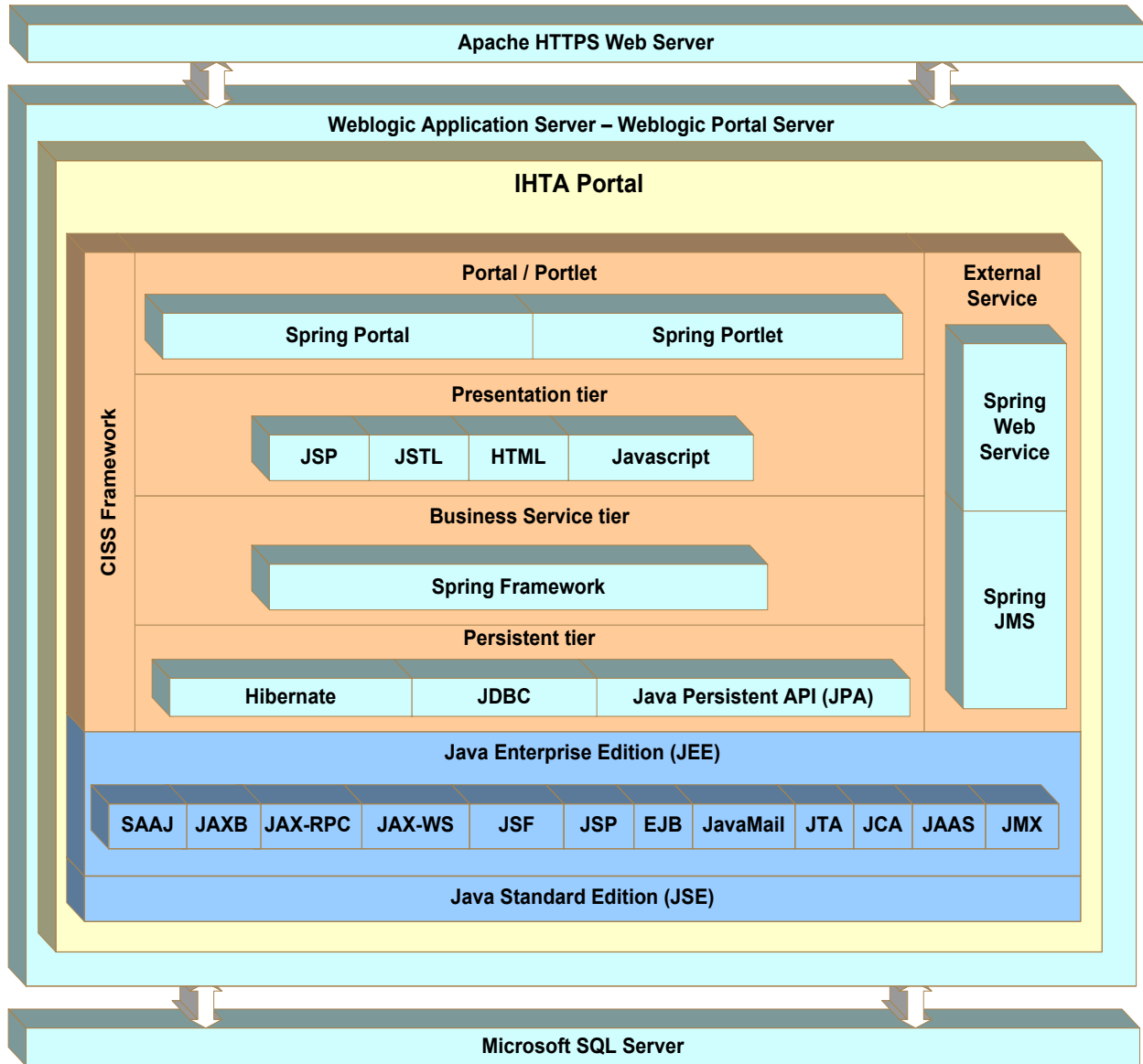


Figure 2 identifies and groups core IHTA technologies.

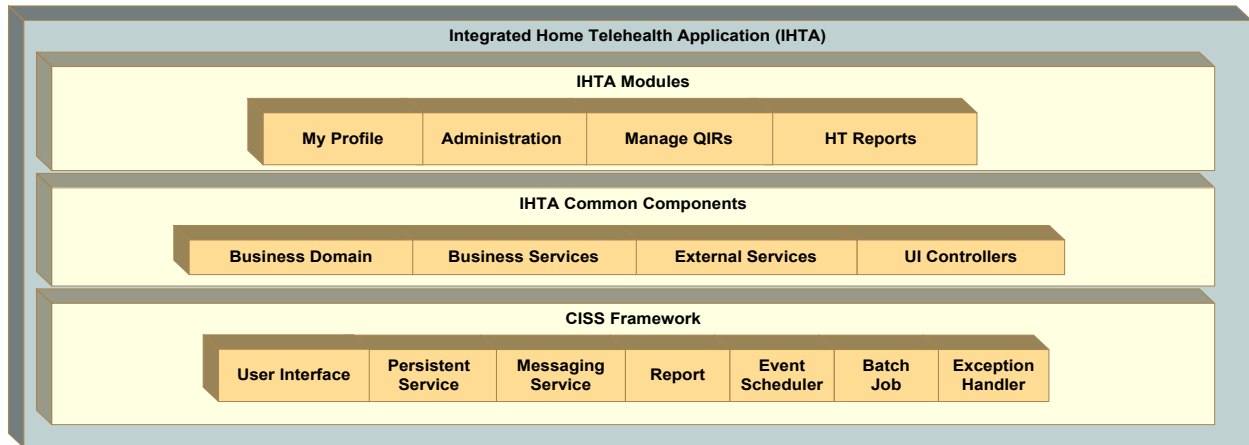
Figure 2: IHTA Technology Stack



1.2.1. Application Components

IHTA modules represent a logical grouping of Java classes and components that are implemented to perform the same or similar business functions. IHTA module codebase uses the IHTA common codebase to ensure a consistent User Interface (UI), well-defined business entities through domain classes, and centralized business logic defined in business services. Figure 3 depicts IHTA modules and components.

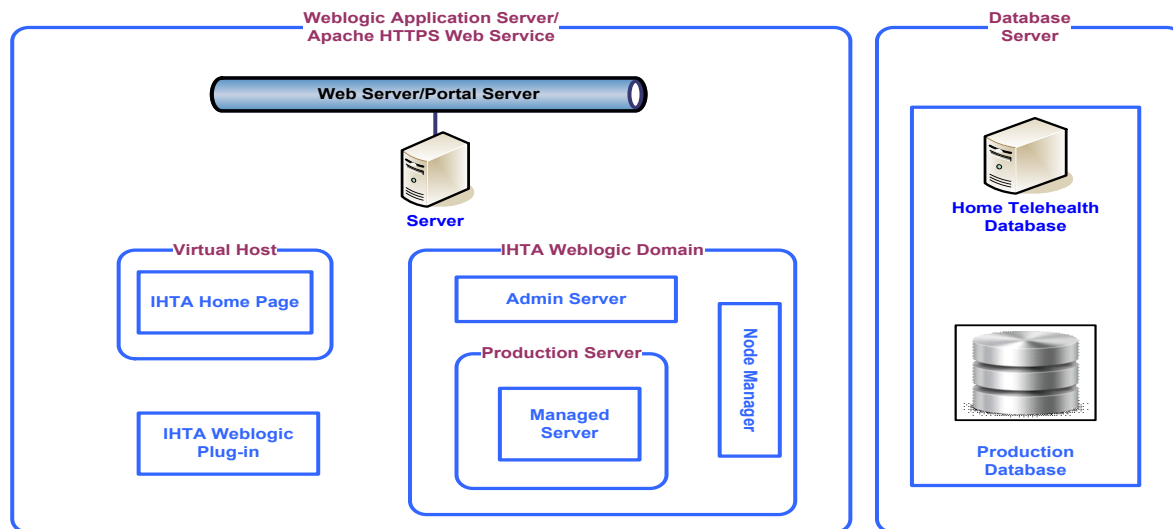
Figure 3: IHTA Components



1.3. Physical System Description

Figure 4 provides a high-level overview of the IHTA production environment.

Figure 4: Environment Overview



The computer hardware for the production servers at both AITC and PITC are virtual machines within and hosted Information Operations (IO).

NOTE: These facilities alternate as the Primary and Secondary IHTA production sites.

Table 2 lists the IHTA Server Hardware at the Production sites.

Table 2: IHTA Server Hardware

Production Site	Manufacturer	Purpose	Qty
AITC	NA	Web/Application Server	1
AITC	NA	SQL Server Database Server	1
PITC	NA	Web/Application Server	1
PITC	NA	SQL Server Database Server	1

1.3.1. Database System Description

The IHTA database architecture is configured for complete redundancy. During operational hours, the data is replicated from the Primary to the Secondary Facility, at near real-time. This process ensures that in the event of a catastrophic failure, if the production database cannot be restored, the secondary database can replace the primary database.

Using SQL Server ‘Always On’ technology between the database servers, data creation and manipulation is maintained asynchronously between the primary and secondary facilities and is configured for minimal data loss and quick database recovery in case of failure. In the event that the database at the Primary Facility goes down, the primary database can be shifted to the database at the secondary Facility via the ‘Always On’ tool of Microsoft SQL Server. The switch to the redundant database will require manual intervention. A user who is signed in at the time of the switch to the alternate site will be impacted.

1.4. Software Description

Table 3 lists the current software for the IHTA production environment.

NOTE: The links below to the SOP – Unix Baseline Configuration and Security Technical Implementation Guides (STIGS) are used by Information Operations for the hardening and baseline configuration to secure RHEL version 7.x.

SOP Unix Baseline SOP

https://vaww.vashare.oit.va.gov/sites/io/EO/Director/Deputy/EDO/DEDO/TIS/UNIXSupp/_layouts/15/WopiFrame2.aspx?sourcedoc=/sites/io/EO/Director/Deputy/EDO/DEDO/TIS/UNIXSupp/SupportDocs/Special%20Projects/CRISP/OIG%20Audit/FY17%20OIG%20Audit/SOP-Unix_Baseline_Configuration.doc&action=default&DefaultItemOpen=1

DISA STIGs Applied After Baseline

<https://iase.disa.mil/stigs/Pages/index.aspx>

Table 3: IHTA Production Software

Required Software	Version	Manufacturer
Microsoft SQL Server	2012	Microsoft
Oracle WebLogic Server	Version 12.2.1.3.0	Oracle
Apache Server	Version 2.4.6	Apache
Red Hat Enterprise Linux (RHEL)	7.5	Red Hat

1.4.1. Background Processes

The background processes utilized in IHTA are described in the following subsections.

1.4.2. Job Schedules

Quartz Scheduler is used to manage the scheduled job feature of IHTA. This feature allows administrators to set up and automatically execute various pre-defined scheduled jobs. IHTA currently executes the following scheduled jobs at periodic intervals:

- Purge Completed Reports: Deletes all reports in the application that have expired.
- QIR Vendor Response Due: Generates a notification to the Vendor when the *Vendor Response Due Date* has passed in the QIR functionality.

Java Messaging Services (JMS) is utilized for internal communication between IHTA components to invoke asynchronous tasks, including, but not limited to, user registration, the vendor response due notice, and to schedule reports. The JMS Subscriber distributes e-mails for notification.

1.4.3. Dependent Systems

Figure 5 illustrates the enterprise systems that interface with IHTA. The details of the enterprise services and applications are summarized in Table 4.

Figure 5: Dependent Systems

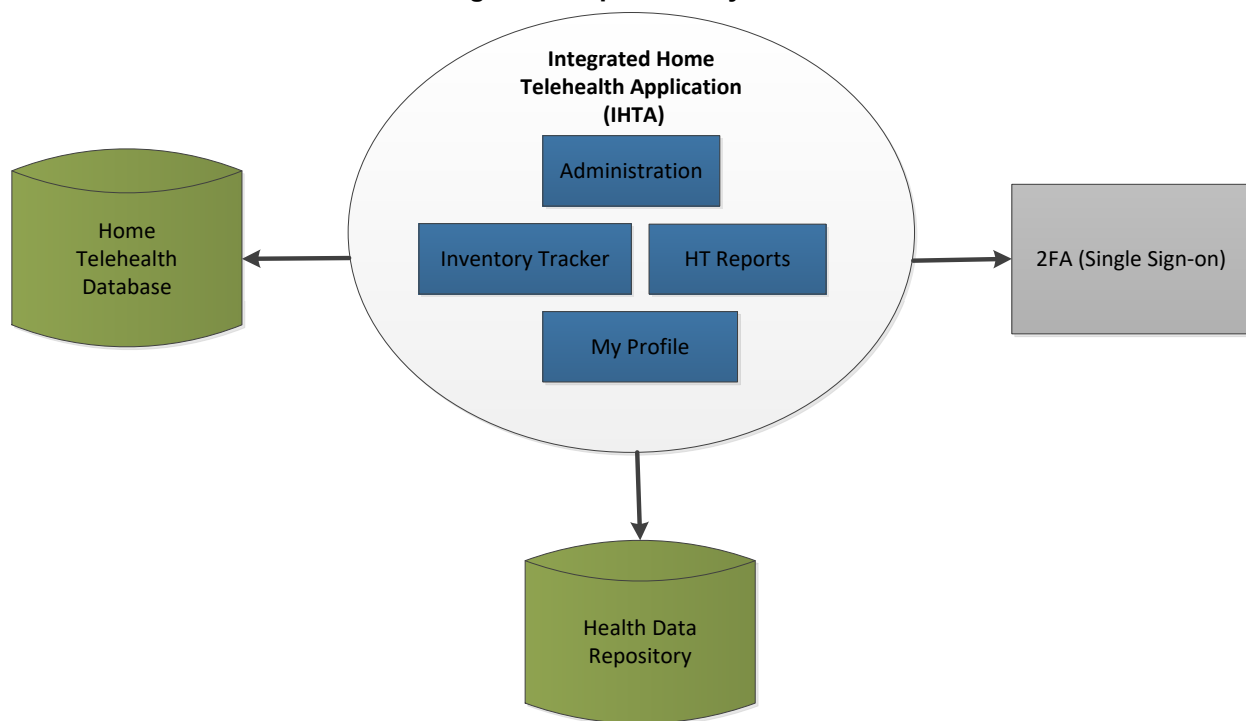


Table 4: Enterprise Service and Application Summary

Service	Category	Integration Technology
Two Factor Authentication (2FA)	Authentication and Authorization	Single Sign-on (SSO)
HT Database	Database for all of HT	Hibernate Java Persistence API (JPA)
Health Data Repository	System of record for HT data	HL7

2. Routine Operations

This section describes, at a high level, what is required of an operator / administrator or other non-business user to maintain the system at an operational and accessible state.

2.1. Administrative Procedures

This section describes the administrative procedures for system start-up and shutdown.

2.1.1. System Start-up

The following subsections outline the steps for how IHTA is started and brought to an operational state.

2.1.1.1. Database Start-Up

1. Coordinate with the database administrator (DBA) on duty of the data center hosting the primary Home Telehealth database to validate its operational state.
2. If the Home Telehealth database instance is down, have the DBA start it up.
3. Have the DBA validate that the instance has fully started successfully and all SQL Server ancillary operations are performing as expected.
4. Validate that the WL1036_Telehealth and Telehealth Database are running and accessible by the users.

2.1.1.2. Application Start-Up

1. Start Apache Web Server.
2. Start Oracle WebLogic Admin Server.
3. Start Oracle WebLogic Node Manager Service.
4. Start Oracle WebLogic Java Virtual Machine (JVM) for IHTA.

2.1.1.3. System Start-Up from Emergency Shut-Down

Refer to section 2.1.1 for the system start-up.

2.1.2. System Shut-down

The following subsections outline the steps for shutting down IHTA.

2.1.2.1. Application Shut-down

The details to shut down IHTA in Production are listed below.

NOTE: The below Linux commands end with a semicolon, and the Linux command support information notes are in parenthesis.

- WebLogic Administrator as weblogic user:
 - `cd;` (make sure user is in the weblogic home directory)
 - `getstatus.sh prod.properties;` (output shows Admin and MS1 running)
 - `appstatus.sh prod.properties;` (output should say ACTIVE)
 - `stopserver.sh prod.properties MS1;` (Shutdown JVM/IHTA Application)
 - `appstatus prod.properties;` (output should say NEW)
 - `getstatus prod.properties;` (output shows only Admin server is running)
 - `killall java;` (Kill the remaining Nodemanager and Admin Server Java Processes)
 - `ps -ef | grep java;` (confirm no Java processes running)
- Linux Administrator with sudo privledge:
 - `systemctl stop httpd;` (IO Linux System Administrator restarts Apache Web Server)

2.1.2.2. Database Shut-down

1. Coordinate with the database administrator (DBA) on duty of the data center hosting the primary Home Telehealth database to validate its operational state.
2. If the Home Telehealth database instance is running have the DBA shut it down (stop).
3. Validate that the WL1036_Telehealth and Telehealth databases are no longer running.

2.1.2.3. Emergency System Shut-down

Refer to section 2.1.2 for the system shut-down.

2.1.2.4. Back-Up Procedures

AITC backs up the Home Telehealth databases (WL1036 Telehealth and Telehealth) as follows:

- Full database backups are conducted during the weekends.
- Incremental database backups are conducted daily.
- Transaction log backups are also scheduled for all user databases and occur hourly.
- All backups are performed while the database is in use. The database instance does not have to be in the shutdown state to perform any of the backups described.

The backups are written to a designated backup folder on the database server from which they are collected for off-site storage.

2.1.2.5. Restore Procedures

Home Telehealth product development team members will coordinate with AITC staff DBA's to perform database recovery. The form of database recovery followed will depend on the type of database failure that requires a recovery effort to be initiated.

2.1.2.5.1. Database Restore – Physical Failure

The HT database is fully replicated between servers located in two different data centers. At any given time, one of the database servers serves as the primary database in support of the production application. The secondary database maintains a replicated copy of the primary database. If the primary database loses functionality due to hardware failure, the Home Telehealth DBA will work with AITC DBA's to activate the secondary database server as the primary database. Once the failed server is brought back online, additional coordination between HT DBA and AITC DBA's will occur to re-establish replication between the two server sites.

2.1.2.5.2. Database Restore – Data Failure

Data failures will impact both the primary and secondary databases. Recovery will require full restore of the primary database from the full and transaction log file backups. The database recovery will be to a point in time prior to the start of the data failure and with minimum data loss as possible. Refer to the Rollback Procedures section of this document for information on recovering the database to a prior point in time.

2.1.2.6. Back-Up Testing

2.1.2.6.1. Database Restore Testing – Hardware Failure

Since this type of database restore represents database server failover, it should be practiced using production. This is an exception to the normal practice of performing the testing in a separate environment. Performing database failover in production ensures that the participating environments are available to function as expected, which is not something that can be duplicated using a test environment. Database failover must be coordinated with the dependent HT applications and conducted during production off hours.

2.1.2.6.2. Database Restore Testing – Data Failure

This recovery test should be performed in a non-production environment using a SQL Server database instance of equivalent release and configuration. Perform a full recovery of the HT database using the most recent full production backup and any transaction logs that apply.

- Test Case #1:
 - Capture all data from the dbo.CENSUS table where the 'date_loaded' value is within ten days of the 'CURRENT_TIMESTAMP' value. Take note of the date stamp information provided. Using the date_loaded values, pick a point in time that occurs prior to the most recent value. This will be the point that you want to recover to in your practice test.

Follow the instructions for performing a point-in-time database recovery as outlined in section 3.5.3. At the completion of the recovery, test to the point in time that you picked in Test Case #1. Perform the following test case to validate your efforts:

- Test Case #2:
 - Capture all data from the dbo.CENSUS table where the 'date_loaded' value is within ten days of the 'CURRENT_TIMESTAMP' value. Take note of the information given in the 'date_loaded' column. To be successful, there should be no date_loaded values past the point in time that was picked for recovery.

2.1.2.7. Storage and Rotation

Refer to the Standard Operating Procedures (SOP) in place at the Primary and Secondary Facilities for procedures on storage and rotation.

2.2. Security / Identity Management

This section provides a high-level description of IHTA’s security and user management.

2.2.1. Identity Management

For VA users, the IHTA Registration Screens capture a user’s VA network ID to store it in the designated IHTA database table. Once a user has registered, the application notifies the Facility / VISN Administrator and the National Administrator. The Facility, VISN, or National Administrator will approve the registration and assign roles according to the user’s job description (see Table 6). The user is then notified by e-mail that his / her registration has been approved. The screens of the Registration Approval Process capture and store IHTA database information about user roles and permissions related to the specific application module of IHTA. Table 5 lists the various roles and the assigned permissions.

Table 5: IHTA Permissions

Module	Permission Name
Administration	Manage Users Manage Roles Manage Batch Jobs Manage Registrations Create QIR Update QIR Read QIR Approve QIR Close QIR Withdraw QIR Reply QIR Agree QIR
All	Administer system components
HT Reports	Generate Patient Survey Reports Generate Census Activity Reports

Table 6: IHTA Roles

Role ID	Role Name	Description	Module	Assigned Permission(s) (See Table 5, IHTA Permissions)
2010	Application Administrator	An individual who is responsible for unlocking users who have locked themselves out of the application by entering their password incorrectly three times.	Administration	Unlock Users
2011	National Administrator	An individual in the Office of Telehealth Services (OTS) HT Program who is primarily responsible for the administration of IHTA.	Administration	<ul style="list-style-type: none"> • Manage Registrations • Manage Users • Manage Scheduled Jobs
2011	National Administrator	An individual in the Office of Telehealth Services (OTS) HT Program who is primarily responsible for the administration of IHTA.	HT Reports	Generate Patient Survey Reports Generate Census Activity Reports
2011	National Administrator	An individual in the Office of Telehealth Services (OTS) HT Program who is primarily responsible for the administration of IHTA.	Manage QIRs	Manage QIRs* Approve a QIR Read a Closed or Withdrawn QIR Update a QIR Close a QIR Export List of QIRs *The National Administrator role cannot create/withdraw a QIR in the application.

Role ID	Role Name	Description	Module	Assigned Permission(s) (See Table 5, IHTA Permissions)
2012	VISN Administrator	A Care Coordinator at the VISN level who has been assigned the additional duties of supervising the administration of IHTA for the VISN.	Administration	Manage Registrations Manage Users
2012	VISN Administrator	A Care Coordinator at the VISN level who has been assigned the additional duties of supervising the administration of IHTA for the VISN.	Manage QIRs	Manage QIRs Create a QIR Agree to a Vendor's response to a QIR Withdraw a QIR Update a QIR Read a Closed or Withdrawn QIR
2012	VISN Administrator	A Care Coordinator at the VISN level who has been assigned the additional duties of supervising the administration of IHTA for the VISN.	HT Reports	All functionality
2013	Facility Administrator	A Care Coordinator at a facility who has been assigned the additional duties of supervising the administration of IHTA for that facility.	Administration	Manage Registrations Manage Users
2013	Facility Administrator	A Care Coordinator at a facility who has been assigned the additional duties of supervising the administration of IHTA for that facility.	Manage QIRs	Search Device by Activation Date Search Device by Serial Number Summary Device Inventory Report Vendor Compliance Reports

Role ID	Role Name	Description	Module	Assigned Permission(s) (See Table 5, IHTA Permissions)
2013	Facility Administrator	A Care Coordinator at a facility who has been assigned the additional duties of supervising the administration of IHTA for that facility.	HT Reports	Generate Patient Survey Reports Generate Census Activity Reports All functionality
2014	Care Coordinator	A registered nurse who manages care across the health care continuum for a panel of HT patients.	Manage QIRs	Search Device by Activation Date Search Device by Serial Number Summary Device Inventory Reports
2014	Care Coordinator	A registered nurse who manages care across the health care continuum for a panel of HT patients.	HT Report	All Functionality
2015	Program Support Assistant	An individual who is responsible for establishing and maintaining inventory of all HT equipment at the facility.	Manage QIRs	Search Device by Activation Date Search Device by Serial Number Summary Device Inventory Reports
2015	Program Support Assistant	An individual who is responsible for establishing and maintaining inventory of all HT equipment at the facility.	HT Reports	All functionality
2017	Vendor	One or more individuals who are the authorized representative for a supplier of HT equipment.	HT Reports	All functionality

Role ID	Role Name	Description	Module	Assigned Permission(s) (See Table 5, IHTA Permissions)
2018	OTS Contract Manager	Office of Telehealth Service (OTS) Contract Manager.	Manage QIRs	Manage QIRs Read a QIR
2018	OTS Contract Manager	Office of Telehealth Service (OTS) Contract Manager.	HT Reports	All Functionality
2020	System Administrator	An individual assigned to be a super user of IHTA with access to all functionality in IHTA.	Administration, Manage QIRs, HT Reports	All functionality
2022	QIR Originator	An individual responsible for submitting Quality Improvement Reports (QIR) in the application to document quality and patient safety issues related to HT devices.	Manage QIRs	Create QIR Update QIR Agree QIR Withdraw QIR Read QIR
2023	Reports Only	An individual within Telehealth Services who needs to access Census and Survey reports.	HT Reports	All functionality

2.2.2. Access Control

VA network credentials assigned to the IHTA user are used for IHTA access control. The IHTA architecture leverages the existing Two Factor Authentication (2FA) Single Sign-On (SSO) service to authenticate the IHTA user.

Access to IHTA will be granted upon successful 2FA authentication. It is important to note that logging into IHTA will not grant access to all application modules or embedded systems in IHTA. There will be authorizations that govern access to each of the application modules or embedded systems. There will also be authorizations that govern access within each application module.

2.3. User Notifications

All routine IHTA maintenance will be performed off-hours (not during the normal workweek of Monday through Friday) to minimize impact to IHTA users. A System 404 message, “Application Out of Order”, will display when a user attempts to log into IHTA and the application is down. In cases of an extended unscheduled system outage, the IHTA Administrator will distribute a notification via e-mail as soon as practicable notifying all users of the system outage and the efforts that are being made to correct it. A second e-mail will be distributed when the system has returned to a normal operational state (refer to Figure 6).

Figure 6: IHTA Outage E-mails

<p>1 - Extended Unscheduled System Outage</p> <p>TO: <HT/CCHT VISN and Facility Leads, Care Coordinators, Program Support Assistants> FROM: IHTA Support RE: URGENT: IHTA Unavailable - Unscheduled System Outage</p> <p>The Integrated Home Telehealth Application (IHTA) is currently down. The IHTA Support staff is currently researching the issue. Please look for another e-mail when the application has returned to an operational state.</p> <p>IHTA Support Team</p>
<p>2 - Status Update – System Outage (After 4 Hours) (If Applicable)</p> <p>TO: <HT/CCHT VISN and Facility Leads, Care Coordinators, Program Support Assistants> FROM: IHTA Support RE: URGENT: Status Update – IHTA Outage</p> <p>The Integrated Home Telehealth Application (IHTA) continues to be down. The IHTA Support staff continues to research the issue. Please look for another e-mail when the application has returned to an operational state.</p> <p>IHTA Support Team</p>
<p>3 – Outage Resolved</p> <p>TO: <HT/CCHT VISN and Facility Leads, Care Coordinators, Program Support Assistants> FROM: IHTA Support RE: URGENT:IHTA Now Available - Outage Resolved</p> <p>The Integrated Home Telehealth Application (IHTA) is now available. The outage has been resolved. Please contact the IHTA Support Team if you experience any issues with accessing the application.</p> <p>IHTA Support Team</p>

2.3.1. **Unscheduled System Outage Procedure**

1. The IHTA Support Team is notified that the application is unavailable.
2. After being notified, the IHTA System Administrator (SA) Charles (Chuck) Lee verifies the unscheduled outage.

The IHTA Support Team sends the **Extended Unscheduled System Outage** e-mail message to the VISN, Facility, and National Administrators. The following subject line is used in the e-mail:

URGENT: IHTA Unavailable – Unscheduled IHTA Outage

3. The VISN and Facility Administrators notify their users that IHTA is unavailable and keep them apprised as they receive status updates.
4. The IHTA SA researches the problem and either resolves it or escalates it to the Database Administrator (DBA).
5. The IHTA SA sends the **Outage Status Update** (see Figure 6) e-mail message to the VISN and Facility Administrators and the National Administrator. The message is sent when the technical staff has an estimated time of system restoration or when four hours has passed since the prior message, whichever comes first.
6. The following subject line is used in the **Outage Status Update** e-mail message:

URGENT: Status Update – IHTA Outage

When the problem is resolved, the IHTA SA sends the **Outage Resolved** e-mail message to the VISN and Facility Administrators and the National Administrator. The following subject line is used in the e-mail:

URGENT: IHTA Now Available – Outage Resolved

Refer to the *Home Telehealth O&M Plan, Standard Operating Procedures (SOPs), Disaster Recovery Plans (DRP), and Contingency Plans (CP)* at the Primary and Secondary facilities for the standard user notifications in effect.

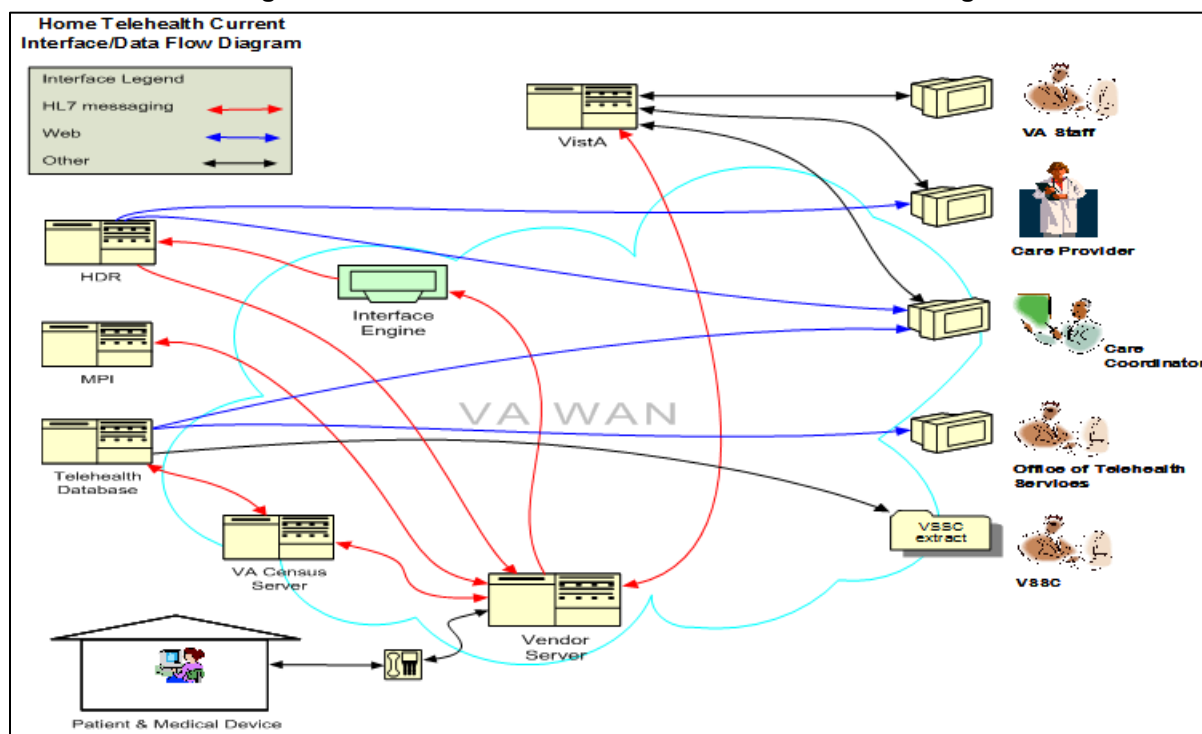
2.4. **System Monitoring, Reporting & Tools**

We are currently in the Process of Migrating to Information Operations (IO) Monitoring Services.

2.4.1. **Dataflow Diagram**

Figure 7 describes the interfaces to the HT application, which are messaging-based for data collection and information sharing, web-based for application access to data, and data extraction for information sharing with other business groups.

Figure 7: Current Home Telehealth Interface/Dataflow Diagram



2.4.2. Availability Monitoring

This section is not applicable for IHTA.

2.4.3. Performance/Capacity Monitoring

IHTA monitors system performance utilizing the Unified Infrastructure Manager (UIM) Monitoring Software.

2.4.4. Critical Metrics

IHTA is in the process of identifying and collecting Metric and defining alerts to quickly inform the team if there is a system problem. Routine Updates, Extracts, and Purges

Database updates and manual extracts are currently performed manually by the DBA upon request. The HTRE Phase 3 DBA will do any required database reorganizations and data purges manually.

2.5. Scheduled Maintenance

Following the VA's Monthly OS patching Schedule, the SA, in collaboration with the IHTA Development team and Information Operations SME's, verifies and updates (as required) operating system (OS) patches. All necessary IHTA production maintenance will be performed during off-hours. A "System Not Available" page displays when the application is down. Also, refer to the SOPs in place at the Primary and Secondary facilities.

2.6. Capacity Planning

HTRE Phase 3 will perform a capacity review as part of the planning for each release at three-month intervals. The HTRE IHTA SA/DBA will be responsible for these reviews.

2.6.1. Initial Capacity Plan

Existing capacity has been deemed adequate for this release of IHTA.

3. Exception Handling

This section provides a high-level overview of how system problems are handled.

3.1. Routine Errors

Like most systems, IHTA may generate a small set of errors that may be considered routine in the sense that they have minimal impact on the user and do not compromise the operational state of the system. Most of the errors are transient in nature and only require the user to retry an operation. The following subsections describe these errors, their causes, and what, if any, response an operator needs to take.

While the occasional occurrence of these errors may be routine, getting a large number of an individual error over a short period of time is an indication of a more serious problem. In that case, the error needs to be treated as an exceptional condition.

3.1.1. Security Errors

Please refer to section 3.2.3.5 for the security errors related to registration and login.

3.1.2. Time-outs

The application automatically logs a user out after 15 minutes of inactivity. Note that this is a system feature, not an error, but is mentioned here for completeness. A warning message displays, counting down from 60 seconds or until the user logs off the application. A user can click the OK button to stop the countdown and continue working.

3.1.3. Concurrency

As a web-based application, IHTA allows users to share data in a multi-user environment. Data is stored in database tables on a database server (Microsoft SQL Server). In a multi-user environment, more than one person may work with the same record at the same time. Since other users can change or even delete the same data that another user is trying to edit, users may occasionally conflict with others as they work. IHTA keeps track of the status of records as users edit them, and makes sure a user is using the latest data. When two or more people try to edit the same record, IHTA will display a suitable error message to assist with resolving the conflict. In most cases, users will respond to one of these errors by attempting their action again. The concurrency errors in IHTA include the following:

- **optimistic.locking.text**=Database operation failed because object was changed by another session. You will have to re-load it and re-apply your changes.
- **optimistic.locking.title**=Optimistic Locking Error.
- **patient.optimistic.locking.text**=Changes to record could not be saved because it was changed by another user. Please re-submit.
- **role.optimistic.locking.text**=Changes to role could not be saved because it was changed by another user. Please re-submit.

3.2. Significant Errors

Significant errors can be defined as errors or conditions that affect the 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 errors, conditions, or other issues.

3.2.1. Application Error Logs

Tool: Text editor

Name/Location: DOMAIN_HOME/ccht.log

Configuration file: /ccht_common/src/main/resources/env/ccht_log4j.xml

Info from configuration file:

Max size: 10MB

Growth rate: dependent on log level. Default is ERROR with negligible growth.

Rotation: after Max file size is reached

Retention: 10 iterations of rotation.

Specific configuration from ccht_log4j.xml:

```
<appender name="ccht.file.appender.detailed"
class="org.apache.log4j.RollingFileAppender">
  <param name="append" value="true" />
  <param name="file" value="ccht.log" />
  <param name="maxFileSize" value="10MB" />
  <param name="maxBackupIndex" value="10" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="[%p] %d{yyyyMMdd hh:mm:ss
aa SSS} %t [%c]%n%m%n%n" />
  </layout>
</appender>
```

3.2.2. Application Error Codes and Descriptions

Error codes and descriptions are found on the vendor(s) website and referenced as needed.

3.2.3. Infrastructure Errors

The following subsections outline the errors for the various components of IHTA.

3.2.3.1. Database

IHTA processing will include exception handling of database errors, providing user feedback, and logging the error on the application server for troubleshooting support and process traceability.

The HT database is configured to log the appropriate level of detail when an error occurs. Staff administrators will use the logged error information to conduct an evaluation of the database error and perform resolution to make the database software or hardware operational.

3.2.3.2. Web Server

The two log files for the IHTA web server are listed below:

1. **access_log**: Logs information related to general IHTA access (e.g., IP address, user, timestamp, etc.).
2. **error_log**: Logs error information related to displaying an IHTA web page.

NOTE: Refer to the log files for the VA Enterprise Lightweight Directory Access Protocol (LDAP) and the HT Database.

3.2.3.3. Application Server

On each application server, errors are logged into a set of log files for each managed server. The seven log files and their descriptions are listed below:

1. The ccht.log file contains log information generated by the IHTA application codes.
2. The MS1.log file contains log information generated by the Manage Server 1.
3. The MS1.out file contains log information directed to the console output of Manage Server 1.
4. The adminServer.log contains log information generated by the Admin Server.
5. The adminServer.out contains log information directed to the console output of the Admin Server.

3.2.3.4. Network

The following Linux commands are used for identifying errors and resolving network errors:

```
Command in BOLD BLACK
Command prompt in light grey
Output from command in red.
Highlighted are key areas to look for Possible problems.
BLUE UPPERCASE ITALIC are comments

[root@vhacrbwebihta91 ~]# mii-tool -v
eth0: negotiated 100baseTx-FD, link ok
product info: vendor 00:50:ef, model 60 rev 8
basic mode: autonegotiation enabled
basic status: autonegotiation complete, link ok
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
eth1: no link - This could be a Problem if there was an expectation of a ethernet
connection established, not an issue in this case, no ethernet connected to this NIC
product info: vendor 00:50:ef, model 60 rev 8
basic mode: autonegotiation enabled
basic status: no link
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control

[root@vhacrbwebihta91 ~]# ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full

    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full

    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full - This could be a Problem if set to Half.
    Port: Twisted Pair
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: on
    Supports Wake-on: g
    Wake-on: d
```

Link detected: yes

```
[root@vhacrbwebihta91 ~]# lsof -Pni; ### Depending on the issue, the output is important
```

```
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
httpd 2878 apache 3u IPv6 15015 0t0 TCP *:80 (LISTEN)
httpd 4429 apache 3u IPv6 15015 0t0 TCP *:80 (LISTEN)
portmap 4653 rpc 3u IPv4 9593 0t0 UDP *:111
portmap 4653 rpc 4u IPv4 9594 0t0 TCP *:111 (LISTEN)
sshd 4725 root 3u IPv4 1857407 0t0 TCP XXX.XXX.XXX.XX:22->YYY.YYY.YYY.YYY:55277 (ESTABLISHED)
rpc.statd 4734 rpcuser 3u IPv4 9894 0t0 UDP *:673
rpc.statd 4734 rpcuser 6u IPv4 9884 0t0 UDP *:670
rpc.statd 4734 rpcuser 7u IPv4 9905 0t0 TCP *:676 (LISTEN)
hpiod 6351 root 0u IPv4 14654 0t0 TCP 127.0.0.1:2208 (LISTEN)
hpssd.py 6356 root 4u IPv4 14672 0t0 TCP 127.0.0.1:2207 (LISTEN)
sshd 6369 root 3u IPv6 14708 0t0 TCP *:22 (LISTEN)
cupsd 6378 root 4u IPv4 14750 0t0 TCP 127.0.0.1:631 (LISTEN)
ntpd 6403 ntp 17u IPv6 14822 0t0 UDP *:123
ntpd 6403 ntp 18u IPv6 14823 0t0 UDP [fe80::7a2b:cbff:fe24:4e68]:123
ntpd 6403 ntp 19u IPv6 14824 0t0 UDP [::1]:123
ntpd 6403 ntp 20u IPv4 14825 0t0 UDP 127.0.0.1:123
ntpd 6403 ntp 22u IPv4 14827 0t0 UDP XX,XXX,XXXX,XXX,XX69:123
sendmail 6421 root 4u IPv4 14917 0t0 TCP 127.0.0.1:25 (LISTEN)
snmpd 6733 root 9u IPv4 15632 0t0 TCP 127.0.0.1:199 (LISTEN)
snmpd 6733 root 10u IPv4 15633 0t0 UDP *:161
snmpd 6733 root 12u IPv4 16481 0t0 TCP 127.0.0.1:199->127.0.0.1:50913 (ESTABLISHED)
dsm_sa_sn 6989 root 4u IPv4 16480 0t0 TCP 127.0.0.1:50913->127.0.0.1:199 (ESTABLISHED)
```

```
[root@vhacrbwebihta91 ~]# ifconfig -a
```

```
eth0 Link encap:Ethernet HWaddr 78:2B:CB:24:4E:68
inet addr:XX.XXX.XXXX.XXX.XX Bcast:XX.XXX.XXXX.XXX.XX Mask:255.255.255.192
inet6 addr: fe80::7a2b:cbff:fe24:4e68/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2573375 errors:0 dropped:0 overruns:0 frame:0
TX packets:2565790 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:211822483 (202.0 MiB) TX bytes:324341582 (309.3 MiB)
Interrupt:98 Memory:d6000000-d6012800

eth1 Link encap:Ethernet HWaddr 78:2B:CB:24:4E:69
inet addr:XX.XXX.XXXX.XXX.XX Bcast:XX.XXX.XXXX.XXX.XX Mask:255.255.255.192
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:106 Memory:d8000000-d8012800
```

```
[root@vhacrbwebihta91 ~]# ethtool -S eth0
```

```
NIC statistics:
rx_bytes: 211807772
rx_error_bytes: 0
tx_bytes: 324314543
tx_error_bytes: 0
rx_ucast_packets: 2568178
rx_mcast_packets: 0
rx_bcast_packets: 4993
tx_ucast_packets: 2565576
tx_mcast_packets: 6
tx_bcast_packets: 3
tx_mac_errors: 0
tx_carrier_errors: 0
rx_crc_errors: 0
rx_align_errors: 0
tx_single_collisions: 0
tx_multi_collisions: 0
tx_deferred: 0
```

```

tx_excess_collisions: 0
tx_late_collisions: 0
tx_total_collisions: 0
rx_fragments: 0
rx_jabbers: 0
rx_undersize_packets: 0
rx_oversize_packets: 0
rx_64_byte_packets: 423920
rx_65_to_127_byte_packets: 2109535
rx_128_to_255_byte_packets: 17144
rx_256_to_511_byte_packets: 491
rx_512_to_1023_byte_packets: 1241
rx_1024_to_1522_byte_packets: 20840
rx_1523_to_9022_byte_packets: 0
tx_64_byte_packets: 420077
tx_65_to_127_byte_packets: 1708868
tx_128_to_255_byte_packets: 11393
tx_256_to_511_byte_packets: 422519
tx_512_to_1023_byte_packets: 886
tx_1024_to_1522_byte_packets: 1842
tx_1523_to_9022_byte_packets: 0
rx_xon_frames: 0
rx_xoff_frames: 0
tx_xon_frames: 0
tx_xoff_frames: 0
rx_mac_ctrl_frames: 0
rx_filtered_packets: 1740100
rx_ftq_discards: 0
rx_discards: 0
rx_fw_discards: 0

[root@vhacrbwebihta91 ~]# ping vha.med.va.gov
PING vha.med.va.gov (XXX.XXX.XXX.XXX) 56(84) bytes of data.
64 bytes from vhaxxxdcvl.vha.med.va.gov (XXX.XXX.XXX.XXX): icmp_seq=1 ttl=119 time=11.0 ms
64 bytes from vhaxxxdcvl.vha.med.va.gov (XXX.XXX.XXX.XXX): icmp_seq=2 ttl=119 time=13.7 ms

--- vha.med.va.gov ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 11.037/12.398/13.760/1.366 ms
### Depending on the time in ms, greater than 70-100 is minor concern, 100+ is
medium concern, 150+ beginning of major network latency issues.
### Same applies to the traceroute command.

[root@vhacrbwebihta91 ~]# traceroute <HOSTNAME/IP>

```

3.2.3.5. Authentication and Authorization

Table 7 and Table 8 list IHTA-specific implementation of the authentication and authorization component(s) as it relates to errors, error reporting, and other pertinent information on causes and remedy of errors.

Table 7: IHTA Authentication and Authorization for Registration Action

IHTA Registration Action	Error Message
User has previously registered and tries to register again.	user.found=User Name already exists. Please contact your Facility Administrator. registration.approved=You have previously registered. Your registration was approved. Click here to login.
User has previously registered, registration was denied, and tries to register again.	registration.denied=You have previously registered. Your registration was denied. Please contact your Facility Administrator.
User has previously registered, the registration has not been approved, and tries to register again.	registration.pending=You have previously registered. Your registration is pending. Please contact your Facility Administrator.

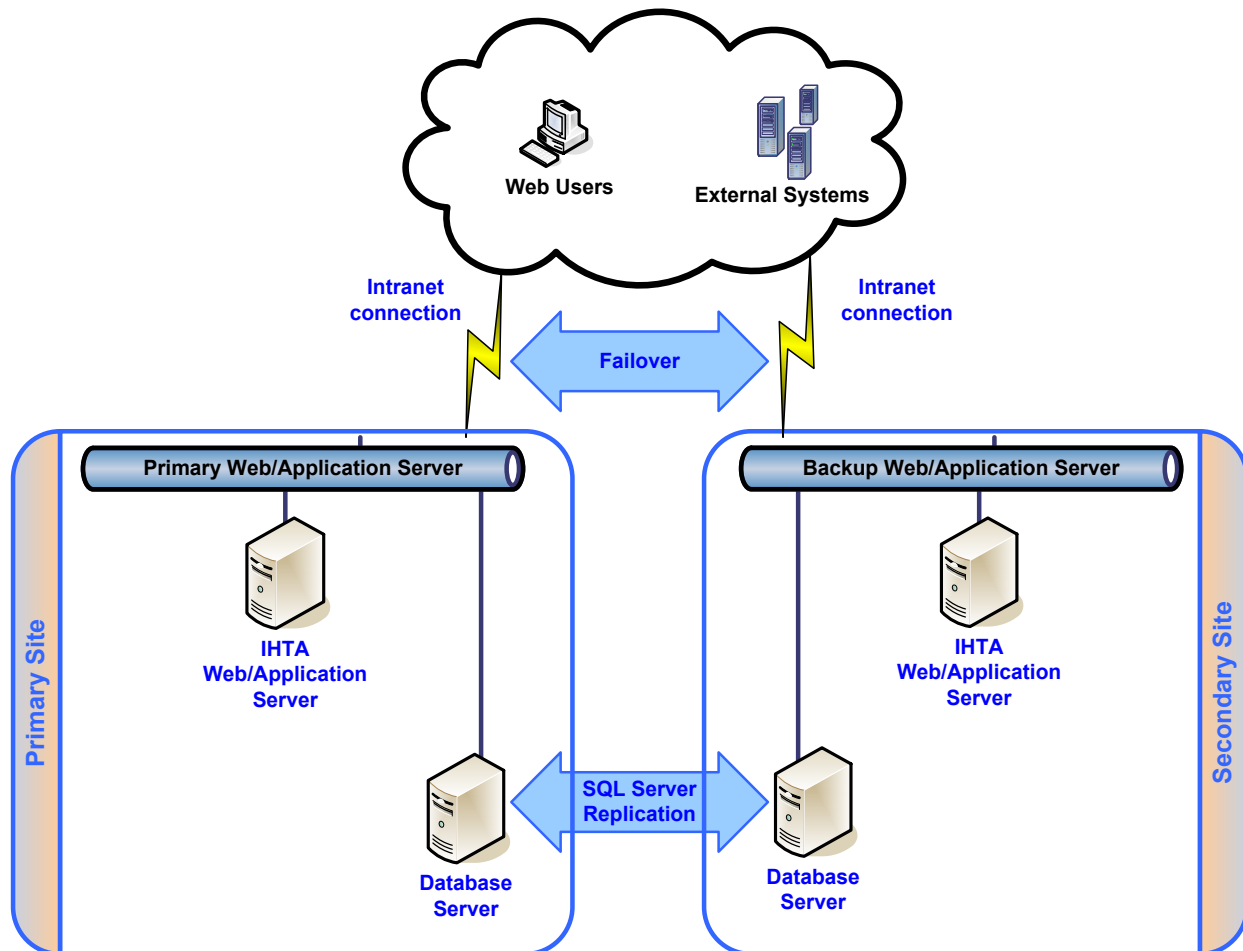
Table 8: IHTA Authentication and Authorization for Login Action

IHTA Login Action	Error Message
User is locked out of the system and tries to log in.	account.locked=You are currently locked out of the system. Please contact your Facility Administrator.
User is inactive in the system and tries to log in.	account.inactive=You are currently inactive in the system. Please contact your Facility Administrator.
User has not registered nor has been approved and tries to log in.	insufficient.privileges=You are not authorized to login to IHTA. Please contact your Facility Administrator.

3.2.3.6. Logical and Physical Descriptions

IHTA and Census and Survey (CNS) employ a standard deployment model, which has one active deployment at the production site and an inactive deployment at the secondary site as Figure 8 depicts. In the event of catastrophic failure at the primary site, incoming requests to the primary site will be failed over to the secondary site, and the application will be activated manually to process incoming requests. Future enhancement will be to implement a database cluster across the production and Disaster Recovery (DR) sites so that the application, deployed at the secondary site, will be automatically activated in the event of failure at the primary site.

Figure 8: IHTA Hardware Architecture



The IHTA architecture implements a standard, standby DR deployment in which near-real-time data replication across the primary and secondary sites is ensured. Although IHTA is deployed to both the primary and secondary sites, IHTA deployment is only activated at the secondary site when there is catastrophic failure of IHTA at the primary site. In the event of catastrophic failure, incoming requests to the primary site's load balancers will be failed over to back-up load balancers at the secondary site. The primary site's main data store is synchronized with the secondary site's back-up data store through database mirroring to ensure near, real-time data replication.

3.3. Dependent System(s)

As a rule, if 2-Factor Authentication (2FA) Single Sign-on Internal (SSOi) or Health Data Repository (HDR) goes down for any reason, a Your IT Services ticket gets filed. Doing so will route the problem to the correct group so that the issue can be remediated.

3.4. Troubleshooting

Refer to section 3.2.3.4 for the following Linux commands that are used for identifying errors and resolving network errors.

3.5. System Recovery

The following subsections define the process 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 up with a fully operational system.

3.5.1. Restart After Non-Scheduled System Interruption

Below are the steps for starting IHTA to Production.

NOTE: The below Linux commands end with a semicolon, and the Linux command support information notes are in parenthesis.

- WebLogic Administrator as weblogic user:
 - `cd;` (make sure user in weblogic home directory)
 - `ps -ef | grep java;` (should be no java processes running)
 - `domains/ihta_prod1035/startWeblogic.sh;` (Start the WebLogic Admin Server)
 - `appstatus.sh prod.properties;` (output should show NEW meaning application is deployed but not running)
 - `startserver.sh prod.properties MS1;` (Start the JVM/IHTA Application)
 - `appstatus prod.properties;` (output should say ACTIVE)
 - `getstatus prod.properties;` (output shows Admin and MS1 running)
- Linux Administrator with sudo privilege:
 - `systemctl restart httpd;` (IO Linux System Administrator restarts Apache Web Server)

3.5.2. Restart After Database Restore

Refer to section 3.5.1 for the steps to restart IHTA in Production after a database restore.

3.5.2.1. Database Start-Up

1. Coordinate with the database administrator (DBA) on duty of the data center hosting the primary Home Telehealth database to validate its operational state.
2. If the IHTA Database instance is down, have the DBA start the database instance.
3. Validate that the WL1036 Telehealth and Telehealth Database are running and accessible by the users.

3.5.2.2. Application Start-Up

1. Start Apache web server on each web server.
2. Start Oracle WebLogic Node Manager Service on each application server in the cluster.
3. Refer to the *HTRE Phase 3 Deploy Install BackOut Rollback Guide*; located on the HT VDL; <https://www.va.gov/vdl/application.asp?appid=154>, for software installation and configuration.
4. Start Oracle WebLogic Domain for IHTA.

Table 9 lists the IHTA Online Help files for the application.

Table 9: IHTA Online Help Files

Help File Name	Zip File Name	Help File Link
General IHTA Help File	ihta.zip	https://vaww.sqa.iht.aac.va.gov/help/ihta/index.html
Administration Help File	admin.zip	https://vaww.sqa.iht.aac.va.gov/help/admin/index.html
Manage QIRs Help File	qir.zip	https://vaww.sqa.iht.aac.va.gov/help/qir/index.html
Manage Registrations Help File	register.zip	https://vaww.sqa.iht.aac.va.gov/help/admin/index.html
My Profile Help File	profile.zip	https://vaww.sqa.iht.aac.va.gov/help/profile/index.html
HT Reports Help File	reports.zip	https://vaww.sqa.iht.aac.va.gov/help/reports/index.html

3.5.3. Rollback Procedures

Recovery of the database to a prior point in time will require restoring the database from a full backup and applying the transaction logs necessary to bring the database state to the decided upon point in time. All due consideration should be given to the impact that this form of database recovery will have as data will be lost. Performing a database rollback recovery should only be considered after all other possible approaches to data correction have been found to potentially have a better outcome than a point-in-time recovery. The following subsections describe the process for rolling back a database to a desired point in time.

3.5.3.1. Backup Selection

Select the full database backup that is prior to and closest to the point in time that the database will be recovered to. If the backup is on external medium, transfer it to a folder on the primary database server so that it is directly available to the database software. Select all transaction log backups that were taken twenty-four hours prior to the database backup you have selected, and all transaction log backups taken up to and include the point in time that you have targeted, to recover the database to. If the transaction log backups are on external medium, transfer all to a folder on the primary database server so that they are directly available to the database software.

3.5.3.2. Database Recovery Preparation

1. Make sure all application use of the database is shutdown. Place the database in the restricted access mode and clear all current user connections.
2. Shutdown database replication to the secondary server. Since the secondary database is also affected by the same data issue that is impacting the primary, the replicated database will need to be rebuilt once the recovery is completed.
3. Though it is the database that needs to be corrected, it also represents the starting point if the recovery effort fails for any reason. Take a full backup of the database. Save the backup in a file just in case it is needed to rebuild and restart the recovery.

3.5.3.3. Database Point In Time Restore

1. Coordinate with the Database Administrator (DBA) on duty at the data center hosting the primary Home Telehealth database to perform the database restore.
2. Provide the data center DBA with the point in time that the database will be recovered.
3. Support the data center DBA as they collect DB backup and transaction log files and perform database recovery procedures.

3.5.3.4. Database Recovery Follow-up – Restart Mirroring; Open Database to User Access

1. Once recovery is completed, provide the data center DBA scripts to:
 - a) validate the database functionality.
 - b) identify the last HL7 messages processed to the database.
 - c) determine the last data built to the database from the IHTA application.
2. Have the data center DBA:
 - b) Create a full database backup and a backup of the transaction log. Copy the backups to the secondary database server.
 - c) Perform the steps above to recover the database on the secondary database server.
 - d) Restart database replication.
3. Follow up with CNS sustainment team members to collect and run any lost HL7 survey or census messages. Notify users of any lost IHTA data.

4. Operations and Maintenance Responsibilities

An understanding of how IHTA is supported by various organizations within the VA is important to operators and administrators of the system. If you are unable to resolve an issue, then it is necessary to understand how to obtain support through OI&T's system support organizations. The following sections describe the support structure and provide procedures on how to obtain support.

The Operations and Maintenance (OM) section defines the roles and responsibilities of each party involved in the delivery and support of the application/service. Precise definition of roles and responsibilities is necessary in a typical shared responsibility environment to avoid confusion over which party is responsible for a specific task or action.

It is not necessary to restate and redefine roles and responsibilities in the OM section for conventional products and services in the Service Strategy and Service Design activities, as they are known. It is only necessary to explicitly state roles and responsibilities in the Service Operation and Continued Service Improvement activities.

Once participating offices have been identified as having an active role in the Operations and Maintenance of IHTA, columns in the linked matrix should be reviewed, updated, and removed as necessary. A detailed RACI (R – Responsible A- Accountable, C – Consulted, I – Informed) Matrix is to be developed for each OM section to show specific roles and responsibilities by environment.



IHTA OM RACI.xlsx

4.1. Support Structure

This section describes the systems support structure as seen from the perspective of operations personnel. The first section defines the support hierarchy through which a support request may navigate. The second section defines the responsibilities for each level of support.

4.1.1. Support Hierarchy

Support for IHTA will be provided REDACTED.

Figure 9: Overview of IHTA Support

REDACTED

4.1.2. Division of Responsibilities

REDACTED

4.2. Support Procedures

REDACTED

Figure 10: IHTA Support Levels

REDACTED

NOTE: REDACTED

5. Approval Signatures

REVIEW DATE: September 17, 2019

SCRIBE: REDACTED

Signed: _____

REDACTED

Signed: _____

REDACTED

Signed: _____

REDACTED

Signed: _____

REDACTED