

**Office of Information and Technology  
Product Development**

**Home Telehealth Capability Enhancements (HTCE)**

**Integrated Home Telehealth Application (IHTA)**

**System Requirements Specification  
(Requirements Specification Document)**



**April 2013  
Version 1.8**



## Revision History

The revision history cycle begins once changes or enhancements are requested to an approved *System Requirements Specification* (SRS).

Date	Revision	Description	Author
04/09/2013	1.8	Updated Figure 2 to include the HT Reports module; removed IVR and added HDR as an external system. Added reference to "HT Reports" to Section 1.2. Updated Figure 3 to remove link to External Systems. Added Kevin Joyner's name to signature page as OTS representative. Updated for 508 compliance (P.A.W. run on 4/9/2013).	
09/10/2012	1.7	Removed DMP Reviewer role (team decision that this would not be an official role in the application) from Table 3.	
10/18/2011	1.6	Added DMP module to Section 1.2; added the System Administrator, DMP Administrator, and DMP Contributor roles to Section 7; removed DMP Development tool from the note that it will be delivered in subsequent releases.	
07/14/2011	1.5	Added text stating that the DMP Development Tool, the Care Coordinator's Common Web Interface, and the Veteran's Web Interface will be delivered in subsequent releases	
4/15/2011	1.4	Changed the project name from HTIE to HTCE; added reference to the HTCE TSPR	
2/3/2011	1.3	Added Section 2.14.2.2 - Preventing Loss of User-Entered Data (CCR 399); added NAC to Section 7	
1/19/2011	1.2	Updated Section 2.14 to include 2.14.1 – Features for each IHTA Module and 2.14.2 – Application-Wide Features (CCR 393)	
10/01/2010	1.1	Updated Figure 3 (removed firewall); updated Software List; changed "Office of Enterprise Development" to "Product Development"; reference the HT SMART Inventory checklist	
09/30/2010	1.0	HTIE 2.5 Release	
07/30/2010	0.3	Updated text and diagrams; added new purchased software components table	
04/16/2010	0.2	Revised Section 2 Overall Specification to reflect George Blankenship's comments	
03/30/2010	0.1	First draft for review	



## Table of Contents

<b>1.</b>	<b>Introduction .....</b>	<b>1</b>
1.1.	Purpose.....	1
1.2.	Scope.....	1
1.3.	Acronyms and Definitions .....	1
1.4.	References.....	2
<b>2.</b>	<b>Overall Specifications.....</b>	<b>3</b>
2.1.	Accessibility Specifications .....	4
2.2.	Business Rules Specifications.....	5
2.3.	Design-Constraints Specifications .....	5
2.4.	Disaster Recovery Specifications .....	5
2.5.	Documentation Specifications .....	5
2.6.	Functional Specifications .....	5
2.7.	Graphical User Interface Specifications .....	5
2.8.	Multi-Divisional Specifications .....	6
2.9.	Performance Specifications .....	6
2.10.	Quality Attributes Specifications.....	6
2.11.	Reliability Specifications.....	6
2.12.	Scope of Integration .....	6
2.13.	Security Specifications .....	6
2.14.	System Features .....	7
2.15.	Usability Specifications.....	8
<b>3.</b>	<b>Applicable Standards .....</b>	<b>9</b>
<b>4.</b>	<b>Interfaces .....</b>	<b>10</b>
4.1.	Communications Interfaces .....	10
4.2.	Hardware Interfaces .....	11
4.3.	Software Interfaces.....	11
4.4.	User Interfaces .....	13
<b>5.</b>	<b>Legal, Copyright, and Other Notices.....</b>	<b>14</b>
<b>6.</b>	<b>Purchased Components.....</b>	<b>14</b>
<b>7.</b>	<b>User Class Characteristics .....</b>	<b>15</b>
<b>8.</b>	<b>Estimation.....</b>	<b>15</b>
	<b>Attachment A - Approval Signatures .....</b>	<b>16</b>

## List of Figures

Figure 1: Home Telehealth Process Flow .....	4
Figure 2: Enterprise Context Diagram .....	10
Figure 3: IHTA Hardware Interfaces .....	11
Figure 4: IHTA Software Interfaces.....	12
Figure 5: IHTA Warning Notice .....	14



---

## List of Tables

---

Table 1: Enterprise Services and Application Summary.....	10
Table 2: Purchased Software Components .....	14
Table 3: IHTA User Class Characteristics .....	15



# 1. Introduction

This section will discuss the purpose and scope of this System Requirements Specification (SRS) document, and provide references to applicable supporting documentation and acronym lists.

## 1.1. Purpose

This SRS will document the non-functional requirements common to all modules of the Integrated Home Telehealth Application (IHTA) being developed as part of the Home Telehealth Capability Enhancements (HTCE) project.

The intended audience for this SRS includes representatives of the Veterans Health Administration (VHA) Patient Care Services (PCS) Office of Telehealth Services (OTS) Care Coordination Home Telehealth (HT) Program, the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T), and the HTCE project team.

## 1.2. Scope

The IHTA modules, considered to be within the scope of this document, include the following: (1) Inventory Tracker; (2) Administration; (3) Disease Management Protocol (DMP) Development Process; (4) HT Reports and (5) My Profile. Each module is considered new development to improve healthcare delivery and mitigate the adverse impact of the potential failure of one of the existing HT vendors. Note this SRS will only document non-functional requirements; functional requirements for IHTA will be documented in the IHTA user stories, per the HTCE Agile Software Development Methodology (SDM). The IHTA user stories will be stored on the HTCE Technical Services Project Repository (TSPR) at the following link:

[REDACTED]

## 1.3. Acronyms and Definitions

For terms, definitions, and acronyms used in this document, please refer to the HTCE Terms, Definitions and Acronyms document available in the HTCE TSPR.

For a listing of all acronyms used by VA, please refer to the VA Acronym Lookup site at the following link: [REDACTED]



## 1.4. References

The following documents are referenced in this SRS:

- Option Years 3 HTCE Performance Work Statement (PWS) (Rev 2012-07-25)
- Option Year 2 HTCE PWS (Rev 2011-04-08))
- HTCE PWS R3094041\_Home Telehealth (Original dated: 2010-06-21)
- Home Telehealth Infrastructure Enhancements, Business Requirements Document, February 2008
- Section 508 Compliance Standards from the Electronic and Information Technology Accessibility Standards Final Rule (Federal Register 21 December 2000, 36 CFR Part 1194)
- NIST 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations
- VA Handbook 6500, Information Security Program
- VA Handbook 6102, Internet/Intranet Services
- *HTCE Software Architecture Document*
- *HTCE Disaster Recovery Plan*
- *IHTA Programming and User Interface Style Guide*
- Agile Modeling v2. Accessed at: <http://www.agilemodeling.com/practices.htm#ApplyModelingStandards>
- Lynch PJ, Horton S. Web Style Guide: Basic Design Principles for Creating Web Sites 3rd Edition. Online version located: <http://www.webstyleguide.com/index.html>
- Code Conventions for the Java™ Programming Language. Accessed at: <http://java.sun.com/docs/codeconv/html/CodeConvTOC.doc.html>
- Java 2 Platform, Enterprise Edition (J2EE) Architecture Standard Website. Accessed at: <http://java.sun.com/j2ee/overview.html>
- Health Level 7 (HL7) Standards Website. Accessed at: <http://www.hl7.com/>



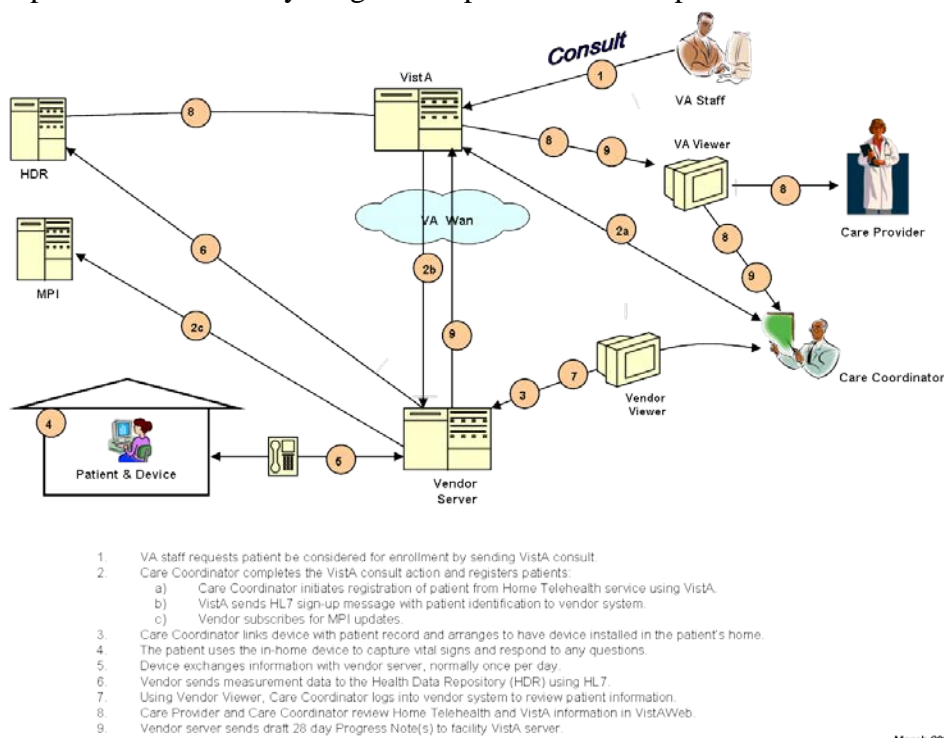
## 2. Overall Specifications

The specifications contained in this SRS have been developed within a specific context. The VHA National Home Telehealth (NHT) platform currently supports the care of 40,000 patients (as of September 2009) with chronic care, acute care, health promotion/disease prevention, and non-institutional care (NIC) needs. These numbers are set to increase to 75,000 by 2011 for VHA to meet NIC requirements and ongoing chronic care, acute care, and health promotion/disease prevention provision. VHA has its own designated NHT Information Technology (IT) platform, which supports data exchanges with HT devices provided under national contract by selected commercial-off-the-shelf (COTS) vendors. Currently, no data interoperability exists between the HT COTS vendors under contract to VHA, VHA's NHT platform, and other VA enterprise IT systems. Current and projected service provision in clinical services provided through this HT platform has raised clinical, cost, and risk management issues that the program office believes warrants urgent consideration. Consequently, VHA has requested additional functionalities to supplement its existing HT IT platform. The VHA request supports the ongoing and emerging business needs of the VHA National Care Coordination/HomeTelehealth Program (CCHT), and the additional functionalities requested under this request comprise the work to be accomplished as part of the HTCE project. This work is defined in PWS R3094041.

VHA's PCS OTS relies upon HT devices from COTS vendors that VA classifies as medical (not IT) technologies. These devices are purchased by VHA and installed in selected patients' homes throughout the United States (US) to maintain a patient's independent living capability. Veterans use the home devices to upload vital sign and other measurements that can help them self-manage health conditions and alert to the need for active care/case management, including urgent referral for clinic and/or hospital care. Vital sign data includes: Blood Glucose, Blood Pressure, Pulse from the Blood Pressure device, Temperature, Weight, Pain, Pulse Oximetry, and Pulse from the Pulse Oximetry device. All these measurements are obtained from peripheral devices (except pain, which is subjective and manually entered on a Likert scale). These peripheral devices are provided with the HT device and link via a wireless or Universal Serial Bus (USB) connection. The monitoring information is typically acted upon the following day and is not collected for the purposes of managing acute life-threatening conditions. The HT devices from COTS vendors that VHA provides in Veteran patients' homes automatically send the data collected each day to the respective vendor server that is situated in a demilitarized zone (DMZ). Each vendor server has its own DMZ, which is a location in the network protected by a double firewall. One firewall faces the device or the Internet and the other faces the VA Intranet. In addition to vital sign data, this same data acquisition/transmission/storage/management system presents patients with a series of questions each day in the form of a DMP. These DMPs help Veteran patients understand their medical condition, communicate symptoms, and modify behaviors to prevent the need for emergency room visits and hospital admissions. To substantiate that Veteran patients who receive care in their own homes are satisfied with this mode of care and do not suffer a diminution of health status, VHA administers a patient satisfaction survey on the HT device and a health status measure (SF-12) every three months.



Vital signs, DMP, patient satisfaction, and SF-12 data are collected on the COTS vendor technologies. The home device initiates the connection to the vendor server. During each connection, the home device presents the data collected that has not been uploaded, and the server may download updates to the software, DMP, disease management parameters, or operating parameters. These bi-directional data communications are effected predominantly via Plain Old Telephone Service (POTS) lines, but may also use broadband. All information (e.g., vitals, DMP values, survey answers, etc.) is stored on the vendor server. The Care Coordinator is expected to review the patient's data every day by using the vendor's desktop application (a set of Web pages providing access to the information on the vendor server). These data are displayed for both panels of patients and individuals. Software algorithms on the vendor servers prioritize patients according to the clinical acuity of their condition based upon responses to the DMPs and relationship of vital sign data to set thresholds. The browser displays are separate for each vendor. OI&T has developed a stable and secure set of processes and environment to support the integration of this data with a Veteran's electronic medical record. These processes have been implemented nationally. Figure 1 represents the HT process flow described above.



March 2008

Figure 1: Home Telehealth Process Flow

## 2.1. Accessibility Specifications

IHTA will adhere to and implement the following standards for accessibility:

- Internet/Intranet Services Standards from the VA Handbook 6102
- Section 508 Compliance Standards from the Electronic and Information Technology Accessibility Standards Final Rule (Federal Register 21 December 2000, 36 CFR Part





1194)

## 2.2. Business Rules Specifications

Applicable business rules will be documented in the IHTA user stories stored on the VA/HTCE SharePoint site.

## 2.3. Design-Constraints Specifications

Design-constraints specifications will adhere to VA standards and will include, but not be limited to, the following:

1. Only tools on the VA-Approved Tools List will be used for developing IHTA.
2. An iterative development approach will be used.
3. The IHTA architecture must comply with One-VA Enterprise Architecture.
4. New features should be scalable to the new technical environment as the Veterans Health Information Systems and Technology Architecture (VistA) transitions into VistA 2.0.
5. Support Internet Explorer (IE) Versions 6 - 8 only.

## 2.4. Disaster Recovery Specifications

For a description of the IHTA Disaster Recovery Specifications, refer to the *HTCE Software Architecture Document* and the *HTCE Disaster Recovery Plan* stored in the HTCE TSPR.

## 2.5. Documentation Specifications

The HTCE team will adhere to Section 508 Compliance Standards<sup>1</sup> regarding IHTA documentation. Additionally, ProPath templates will be utilized for all project documentation.

## 2.6. Functional Specifications

The Functional Requirements for each IHTA module will be elaborated in the user stories for that specific module. Each user story will be a stand-alone document that will be reviewed and approved by the customer. Customer-approved user stories will be stored on the HTCE TSPR.

## 2.7. Graphical User Interface Specifications

IHTA will adhere to Section 508 Compliance Standards for Graphical User Interface (GUI) specifications. IHTA will also adhere to specifications set forth by Agile Modeling's *Apply Modeling Standards*<sup>2</sup> and the *Web Style Guide: Basic Design Principles for Creating Web*

<sup>1</sup> 508 Compliance Standards from the Electronic and Information Technology Accessibility Standards Final Rule (Federal Register 21 December 2000, 36 CFR Part 1194)

<sup>2</sup> Agile Modeling v2. *Apply Modeling Standards*. Accessed at:  
<http://www.agilemodeling.com/practices.htm#ApplyModelingStandards>



*Sites.*<sup>3</sup> The user interface for IHTA will utilize common standards for navigation, site and page structure, page design, typography, editorial style, graphics, and multimedia.

HTCE developed the *IHTA Programming and User Interface Style Guide*, utilizing Agile Modeling and the Web Style Guide references listed above. All specifications will be outlined in this document.

## 2.8. Multi-Divisional Specifications

This section is not applicable to IHTA.

## 2.9. Performance Specifications

No performance specifications for IHTA have been defined at this time. When defined, they will be added to this SRS in a future update.

## 2.10. Quality Attributes Specifications

IHTA Java source code, including, but not limited to, file names, file organization, indentation, comments, declarations, statements, white spaces, and programming practices, will adhere to the Sun Java Coding standard.<sup>4</sup> For more information, reference the *IHTA Programming and User Interface Style Guide*.

## 2.11. Reliability Specifications

No reliability specifications for IHTA have been defined at this time. When defined, they will be added to this SRS in a future update.

## 2.12. Scope of Integration

IHTA will exist in the context of other HT systems, along with external systems. The scope of IHTA integration is described in the IHTA Component Architecture referenced in the Enterprise Context section of the *HTCE Software Architecture Document*.

## 2.13. Security Specifications

All computer systems and sub-systems of the HTCE project must incorporate adequate safeguards for the security of information processed by them. Before a system or sub-system becomes operational, it must undergo a security Certification and Accreditation (C&A) process that results in an Authority to Operate (ATO) or Interim Authority to Operate (IATO).

<sup>3</sup> Lynch PJ, Horton S. *Web Style Guide: Basic Design Principles for Creating Web Sites* 3<sup>rd</sup> Edition. Online version located: <http://www.webstyleguide.com/index.html>

<sup>4</sup> Code Conventions for the Java™ Programming Language. Accessed at: <http://java.sun.com/docs/codeconv/html/CodeConvTOC.doc.html>



According to Office of Management and Budget (OMB) and the Clinger-Cohen Act of 1996, security must be a consideration throughout the System Development Lifecycle (SDLC). This section describes the security specifications that must be included in the development of IHTA. This section will be used as a starting point for security planning.

- **Access Control** (National Institute of Standards and Technology [NIST] SP 800-53<sup>5</sup>). Access control for IHTA is provided agency-wide by OTS. Local, regional, and national IHTA administrators will determine and maintain access controls at the system level for IHTA. This control is managed at the VA level.
  - **Authorization.** IHTA enforces assigned authorizations for controlling access to the system in accordance with applicable policy. For VA users, IHTA uses the existing VHA Enterprise Lightweight Directory Access Protocol (LDAP) domain for authentication storage. For non-VA users, IHTA will utilize the IHTA database tables to store authorization information, such as credentials and successful and failed logon attempts. The administrative IHTA screens are provided for administrative users to assign authorizations to IHTA users with different roles and permissions.
  - **Registration.** The IHTA registration screens capture a user's VA network ID to store it in the IHTA database table.
  - **Registration Approval.** The registration approval process for IHTA is performed by its administrator or a system administrator. The screens of the registration approval process capture and store IHTA database information about user roles, groups, and permissions related to specific application modules of IHTA.
- **Identification and Authentication** (NIST SP 800-53). IHTA uniquely identifies and authenticates VA users using the VA Enterprise LDAP.

HTCE will use the formal, documented policies, and procedures (i.e., VA Directive and Handbook 6500, Security Accreditation Package and Security Management and Reporting Tool [SMART] database) provided by Office of Cyber and Information Security (OCIS) that govern the security requirements set forth by NIST and VA, and must ensure their effective implementation. Please refer to the Home Telehealth SMART Inventory Checklist.

## 2.14. System Features

Under the HTCE Agile SDM, the system features and functional requirements for each module of IHTA will be documented using user stories. Customer-approved user stories will be stored on the HTCE TSPR. For general features and functional requirements that apply across the application, refer to Section 2.14.1.

### 2.14.1. Features for Each IHTA Module

Under the HTCE Agile SDM, the system features and functional requirements for each module of IHTA are documented using user stories. The user stories will be stored on the HTCE TSPR.

<sup>5</sup> National Institute of Standards and Technology Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems, December 2007.



## **2.14.2. Application-Wide Features**

The general features and functional requirements in the following sections apply across the application.

### **2.14.2.1. Maintaining Data Integrity in a Multi-User Environment**

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.

### **2.14.2.2. Preventing Loss of User-Entered Data**

IHTA will display a standard dialog box for all user actions that may result in the loss of user-entered data. The dialog box will provide the user with the option to either continue or discontinue the action, clearly specifying that data loss will occur if the user chooses to continue. The user must confirm the action before continuing to a new IHTA window.

## **2.15. Usability Specifications**

Usability specifications for IHTA have not yet been defined. When defined, they will be added to this SRS in a future update.



### 3. Applicable Standards

IHTA will comply with the following standards:

- Section 508 Compliance Standards from the Electronic and Information Technology Accessibility Standards Final Rule (Federal Register 21 December 2000, 36 CFR Part 1194)<sup>6</sup>
- Code Conventions for the Java™ Programming Language<sup>7</sup>
- Java 2 Platform, Enterprise Edition (J2EE) Architecture standard<sup>8</sup>
- Any messaging implemented to support IHTA will comply with applicable sections of the Health Level 7 (HL7) standard<sup>9</sup>

<sup>6</sup> Electronic and Information Technology Accessibility Standards (Section 508). Accessed at: <http://www.access-board.gov/sec508/standards.htm>

<sup>7</sup> Code Conventions for the Java™ Programming Language. Accessed at: <http://java.sun.com/docs/codeconv/html/CodeConvTOC.doc.html>

<sup>8</sup> Java 2 Platform, Enterprise Edition (J2EE) Architecture Standard Website. Accessed at: <http://java.sun.com/j2ee/overview.html>

<sup>9</sup> Health Level 7 (HL7) Standards Website. Accessed at: <http://www.hl7.com/>

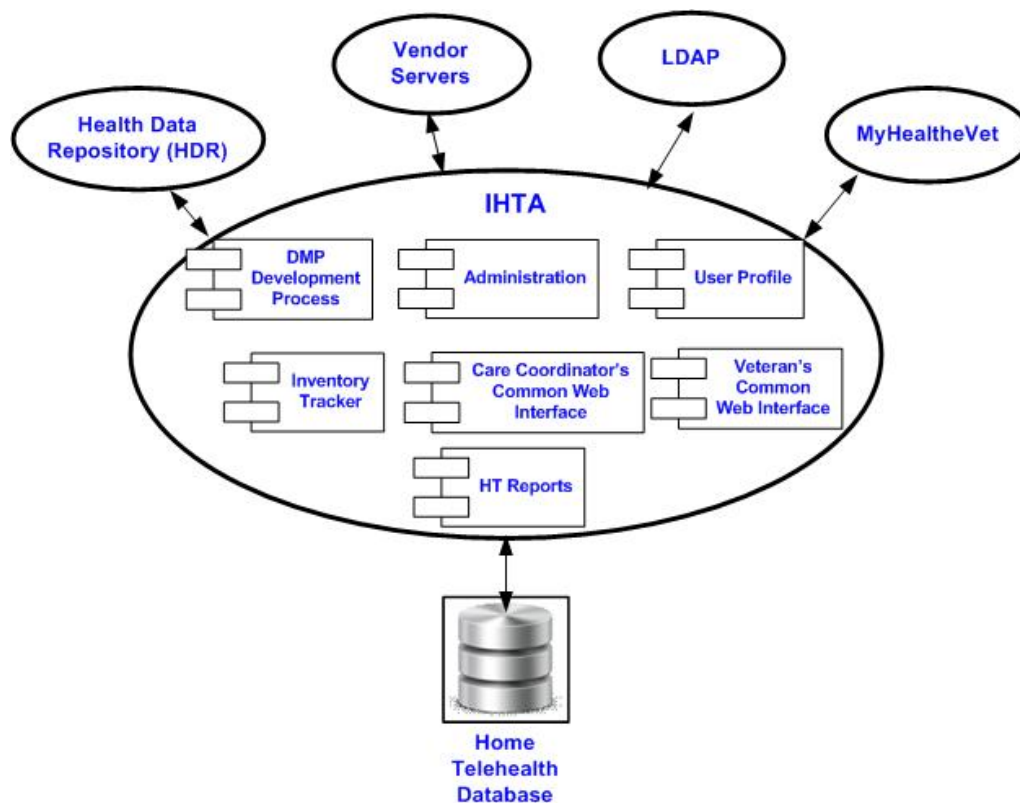


## 4. Interfaces

This section will describe the Communication, Hardware, Software, and User Interfaces that IHTA will support.

### 4.1. Communications Interfaces

Figure 2 illustrates specific enterprise services and systems with which IHTA will communicate.



**Figure 2: Enterprise Context Diagram**

**NOTE:** The Care Coordinator's Common Web Interface and the Veteran's Common Web Interface will be delivered in subsequent releases pending customer approval.

The details of the enterprise services and applications are summarized in Table 1.

**Table 1: Enterprise Services and Application Summary**

Service	Category	Integration Technology	Notes
Vendor Servers	Enterprise	Indirect integration through Home Telehealth database	None
VA Enterprise LDAP	Enterprise	Spring LDAP	Authentication and Authorization



Service	Category	Integration Technology	Notes
My HealtheVet	Enterprise	Portal Server	Host HTCE as a Java Portlet
Home Telehealth Database	Internal	Java Persistence Application Programming Interface (API)	Database for all of HT
Health Data Repository (HDR)	Enterprise	HL7 messaging	Data for the HT Reports module

## 4.2. Hardware Interfaces

Figure 3 illustrates a sample design of the hardware interfaces for IHTA. Network connection between database servers, application servers, and Web servers to the VA local area network (LAN) is facilitated through a HP NC382i Dual Port Multifunction Gigabit Server Adapter installed on each server.

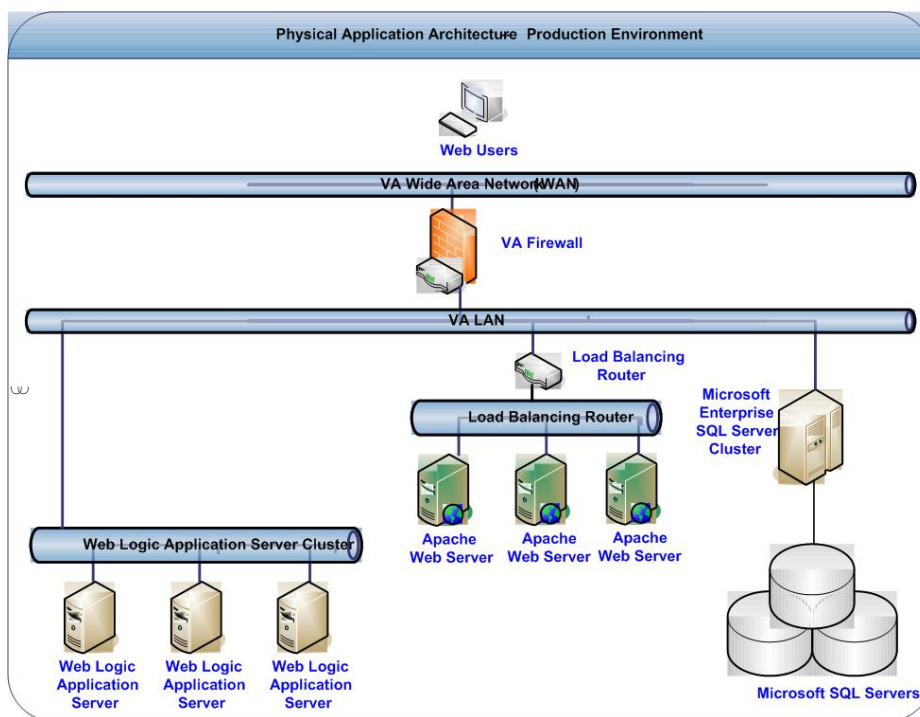


Figure 3: IHTA Hardware Interfaces

## 4.3. Software Interfaces

Figure 4 presents the software interfaces for IHTA's component architecture.

IHTA will be implemented as a Web-based "Integrated Portal". To be compliant with other My HealtheVet (MHV) applications, IHTA will be implemented in Java using both standard and enterprise features. MHV applications will integrate to IHTA using the Java Portlet Application



Programming Interface (API) (to include industry standard protocols such as Java Specification Request (JSR)-168, JSR-286, and Web Services for Remote Portlets (WSRP) 2.0). These standards dictate “java portal and portlet” behavior. MHV applications that do not integrate to these standards (e.g., legacy applications in a different language, etc.) may still be able to be integrated into IHTA, in a looser fashion via a Uniform Resource Locator (URL).

At the current time, IHTA is designed, implemented, and deployed as a portlet on its own dedicated portal server. If the business requirements call for IHTA to be deployed onto the MHV portal system, IHTA will be packaged as a portlet and deployed onto the MHV portal server.

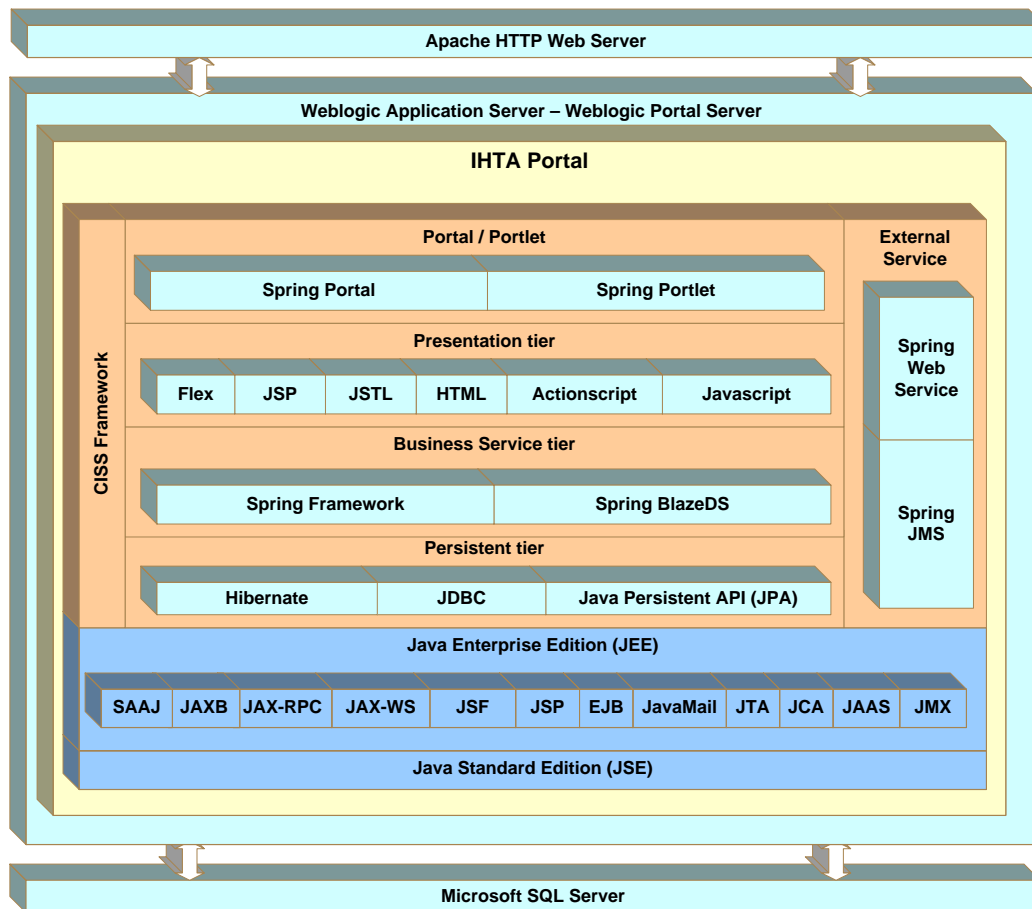


Figure 4: IHTA Software Interfaces

Other core components include: (1) Apache Web Server, (2) Oracle WebLogic Portal Server, and (3) Microsoft SQL Server Database.

#### 4.3.1. Apache Web Server

While the Apache Web Server will be used to process HTTP requests for static content, such as on-line HTML files, the WebLogic Server Apache Plug-In will be installed and configured on the Apache Web Server to forward HTTP requests for dynamic content to a cluster of WebLogic





Portal Server instances. The Apache HTTP Server Plug-In operates as an Apache Web Server's dynamic shared module loaded at start-up time to process HTTP requests to IHTA. The configuration of the WebLogic Server Apache Plug-In involves editing the Apache httpd.conf file to instruct the Apache Web Server to load the WebLogic Portal Server Library for the plug-in as an apache module, to specify application requests that should be handled by the module, to define URL rewrite rules for IHTA URLs, and to define the port and address of the WebLogic Portal Server Cluster and Admin Server. In addition, the WebLogic Apache Plug-in also allows HTTP requests and responses access through a company's firewall, usually referred to as HTTP-tunneling.

### **4.3.2. Oracle WebLogic Portal Server**

The Oracle WebLogic Portal Server will be used as the application platform suite (APS) for developing, integrating, and deploying IHTA's applications, portals, and Websites. The Oracle WebLogic Portal Server bundled with the WebLogic Application Server provides services through JEE components. These components include Enterprise Java Beans (EJB), Java Server Pages (JSP), Java Naming and Directory Interface (JNDI), Java Messaging Services (JMS), Java Authentication and Authorization Services (JAAS), and other enterprise services. Taken together, these WebLogic Application Server services enable personalization, real-time business activity monitoring, business intelligence, identity management, and wireless deployment.

### **4.3.3. Microsoft Enterprise SQL Server Database**

The database management software, Microsoft SQL Server 2005, will be configured on a dedicated server. Data storage will be defined to the local drives. IHTA will be configured to access the database server using the Java Database Connectivity (JDBC) thin driver for Microsoft SQA Server to perform data retrieval and manipulation. Individual user interaction directly with the database will be kept to a minimum and will be restricted by the user profile.

## **4.4. User Interfaces**

All VA users will interface with IHTA via a VA-supported Web-browser. Future updates to this SRS will identify additional supported browsers for both VA and Non-VA users.



## 5. Legal, Copyright, and Other Notices

The warning notice presented in Figure 5 displays each time a user logs in to IHTA. Additionally, a link to the IHTA Access Policy for Patient Sensitive Information is displayed in the IHTA footer located on all IHTA screens.

### Integrated Home Telehealth Application User Agreement

Users are prohibited from allowing ANYONE to use their User Name/Password codes.

**WARNING** - This system may contain Government information which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213(a), 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

Figure 5: IHTA Warning Notice

## 6. Purchased Components

See Table 2 for the purchased software components for IHTA.

Table 2: Purchased Software Components

Software Category	Product	Total Licenses Needed	FY10 Purchase	FY11 Purchase	FY12 Purchase and Beyond
UI Design Tool	Adobe Flex Builder	2	X		
Automated and Performance Test Tool	LoadRunner	1			X
System Monitoring Tool	BMC Patrol	19			X
System Monitoring Tool	JProbe	7	X		
On-Line Help	Robohelp	1	X		
508 Compliant Test	JAWS	2	X		
Interactive Relational Database Tool	TOAD	3	X		
Server Operating System	Red Hat Linux (Dev/SQA)	8		X	
Server Operating System	Red Hat Linux (Production)	8		X	



## 7. User Class Characteristics

Table 3 outlines the general characteristics of the intended users of IHTA, including application experience, IT expertise, and education.

**Table 3: IHTA User Class Characteristics**

User	Education	Experience	IT Expertise
Care Coordinator	RN	Moderate to High	Low
DMP Administrator	Various	High	Low
DMP Contributor	MD, RN	High	Low
Facility Administrator	RN	High	Low
Management	Various	Moderate	Low
Contract Office staff	Various	Low	Low
National Administrator	Program Analyst	High	Low
Program Support Assistant (PSA)	Administration	Moderate to High	Low
System Administrator	Developer	High	High
Vendor	Various	Moderate	Low
VISN Administrator	RN	High	Low

## 8. Estimation

Refer to the *HTCE Project Management Plan* for estimation information.



## Attachment A - Approval Signatures

---

**Signed:**

**Date:**



**Integrated Project Team (IPT) Chair/IT Program Manager**

---

**Signed:**

**Date:**



**Office of Telehealth Services (OTS) Program Analyst**

---

**Signed:**

**Date:**



**HTCE Project Manager**