Oracle® Health Sciences Information Gateway

Secure Health Email Installation and Configuration Guide

Release 2.0.1

E37028-02

October 2013

ORACLE®

Oracle Health Sciences Information Gateway Secure Health Email Installation and Configuration Guide, Release 2.0.1

E37028-02

Contents

K References

Glossary

Index

Preface

This guide provides information on how to install and configure Oracle Health Sciences Information Gateway (OHIG) Secure Health Email, which securely sends and receives encrypted Email.

Audience

This document is intended for users who have to install and configure OHIG Secure Health Email.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documentation sets:

Oracle Health Sciences Information Gateway

- *Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter Installation and Configuration Guide*
- *Oracle Health Sciences Information Gateway Cross Community Access Installation and Configuration Guide*
- *Oracle Health Sciences Information Gateway Cross Community Access User Guide*
- *Oracle Health Sciences Information Gateway Secure Health Email Installation and Configuration Guide*
- *Oracle Health Sciences Information Gateway Security Guide*
- *Oracle Health Sciences Information Gateway Release Notes*

Oracle Health Sciences Information Manager

- *Oracle Health Sciences Information Manager Health Record Locator Installation and Configuration Guide*
- *Oracle Health Sciences Information Manager Policy Engine Installation and Configuration Guide*
- *Oracle Health Sciences Information Manager Policy Monitor Installation and Configuration Guide*
- *Oracle Health Sciences Information Manager Health Record Locator User Guide*
- *Oracle Health Sciences Information Manager Security Guide*
- *Oracle Health Sciences Information Manager Release Notes*

Oracle Healthcare Master Person Index

- *Oracle Healthcare Master Person Index Australia Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index United States Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index United Kingdom Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index Provider Index User's Guide*
- *Oracle Healthcare Master Person Index User's Guide*
- *Oracle Healthcare Master Person Index Installation Guide*
- *Oracle Healthcare Master Person Index Working With IHE Profiles User's Guide*
- *Oracle Healthcare Master Person Index Analyzing and Cleansing Data User's Guide*
- *Oracle Healthcare Master Person Index Data Manager User's Guide*
- *Oracle Healthcare Master Person Index Configuration Guide*
- *Oracle Healthcare Master Person Index Standardization Engine Reference*
- *Oracle Healthcare Master Person Index Configuration Reference*
- *Oracle Healthcare Master Person Index WebLogic User's Guide*
- *Oracle Healthcare Master Person Index Command Line Reports and Database Maintenance User's Guide*
- *Oracle Healthcare Master Person Index Loading the Initial Data Set User's Guide*
- *Oracle Healthcare Master Person Index Match Engine Reference*
- *Oracle Healthcare Master Person Index Message Processing Reference*

Conventions

The following text conventions are used in this document:

boldface - Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

italic - Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

`monospace` - Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Getting Started

This chapter describes the minimum hardware and software requirements for installing Oracle Health Sciences Information Gateway (OHIG) Secure Health Email.

This chapter includes the following sections:

1.1 Hardware Requirements

The following are the hardware requirements for installing OHIG Secure Health Email:

- 2 GB (2048 MB) of RAM
- 12 GB of disk space
- 16 GB of disk space for 64 bit

1.2 Software Requirements

The following are the software requirements for installing OHIG Secure Health Email:

- Java 1.6 executable in path
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files (jce_policy-6.zip)
- Oracle Database 10+ (11g Release 1)
- Oracle Enterprise Linux 5.5 or higher

Configuration Requirements

Apache Ant 1.8.2 executable in path

```
PATH=$PATH:<install_dir>/apache-ant-1.8.2/bin
```

Oracle Software Requirements

- Oracle Health Sciences Information Manager (OHIM) Record Locator 2.0 or higher
- Oracle Health Sciences Information Manager (OHIM) Policy Monitor 2.0 or higher
- Oracle Healthcare Master Person Index (OHMPI) 2.0.1 or higher

- Oracle Healthcare Transaction Database (HTB) 6.1 or higher

1.3 Downloading the Oracle Health Sciences Information Gateway Secure Health Email

To download the Oracle Health Sciences Information Gateway Secure Health Email, perform the following tasks:

1. Navigate to `http://edelivery.oracle.com`.
2. Enter your Registration information, accept the Agreement Terms by selecting the checkboxes, then click **Continue**.
3. From the **Select a Product Pack** drop-down menu, select **Health Sciences**.
4. From the **Platform** drop-down menu, select **Linux x86**.
5. Click **Go**.
6. Select **Oracle Health Sciences Information Gateway Media Pack**.
7. Click **Continue**.
8. Click **Download** for the following and save the files to your system:
   - **Oracle Health Science Information Gateway 2.0.1 Secure Health Email**
9. Extract the files to view the *Oracle Health Sciences Information Gateway Secure Health Email Installation and Configuration Guide* and get the compressed tar file (`*.tgz`).

2

Installing and Configuring OHIG Secure Health Email

Oracle Health Sciences Information Gateway (OHIG) has implemented the National Health Information Network (NHIN) to provide a secure, scalable, standards-based method of sending authenticated and encrypted health information to known and trusted recipients over the internet. OHIG Secure Health Email interacts with Oracle Health Sciences Information Manager (HIM) services, such as Oracle Healthcare Master Person Index (OHMPI), Document Registry, Repository, Policy Engine, and Audit Record Repository (ARR).

This chapter leads you through the steps to install, set up, and configure the James Mail Enterprise Server (James) version 2.3.2 to use with OHIG and Oracle Health Sciences Information Manager (OHIM). OHIG Secure Health Email is built on top of the Apache James Mail Server.

This chapter includes the following sections:

> **Note:** For a high-level overview of the Secure Health Email network, see Appendix J, "High-level Network Diagram."

2.1 Preparing the Databases

2.1.1 Preparing the Apache James Mail Server Database

To prepare the Apache James Mail Server database tables for Oracle:

Note: Because the Apache James Mail Server Database stores sensitive data, it should be set up with encryption turned on.

1. Copy the files under `<install_dir>/addons/direct/config/files/database/oracle` to a machine with Oracle SQL*Plus installed.
2. Update the script `create-james-user-oracle.sql` with TABLESPACE parameters matching your environment. Also assign a password for the James database user by assigning a value to variable *JAMES_USER_PASS*. Remember to clear the value after you execute the script.
3. To create the Apache James Mail Server database user load the script `create-james-user-oracle.sql` into the database.

   Example:

   ```
   > sqlplus system@<SID>
   SQL> @create-james-user-oracle.sql
   ```

4. To create the Apache James Mail Server database load the script `create-james-tables-oracle.sql` into the database.

   Example:

   ```
   > sqlplus <JAMESUSER>@<SID>
   SQL> @create-james-tables-oracle.sql
   ```

2.1.2 Preparing the Secure Health Email Database

To prepare the OHIG Secure Health Email database tables for Oracle:

1. Copy the files under `install_dir>/addons/direct/config/files/database/oracle` to a machine with Oracle SQL*Plus installed.
2. Update the script `create-direct-user-oracle.sql` with TABLESPACE parameters matching your environment. Also assign a password for the OHIG Secure Health Email database user, by assigning a value to the variable *DIRECT_USER_PASS*. Remember to clear the value after you execute the script.
3. To create the OHIG Secure Health Email database user load the script `create-direct-user-oracle.sql` into the database.

   Example:

   ```
   > sqlplus system@<SID>
   SQL> @create-direct-user-oracle.sql
   ```

4. To create the OHIG Secure Health Email database load the script `create-direct-tables-oracle.sql` into the database.

   Example:

   ```
   > sqlplus <DIRECTUSER>@<SID>
   SQL> @create-direct-tables-oracle.sql
   ```

2.2 Installing the Apache James Mail Server

Execute the following commands to install the Secure Health Email:

1. `$ tar -zxvf ohig_direct_installer.tgz`
2. `$ cd ohig_direct_installer`
3. `$ java -jar ohig_direct_installer.jar`

   To follow the prompts, refer to Appendix A, "Running the Oracle Health Sciences Information Gateway Secure Health Email Installer".

2.3 Configuring the Apache James Mail Server

This provides the settings for configuring OHIG Secure Health Email, the Apache Mail Server for SSL, and the Remote Manager:

- Configuring Apache James Mail Server for SSL
- Configuring Oracle Health Sciences Information Gateway Secure Health Email Properties
- Configuring the Remote Manager

2.3.1 Configuring Oracle Health Sciences Information Gateway Secure Health Email Properties

From this release of OHIG, you are not required to manually edit the file. You will be prompted through the script. Execute the following code to configure the OHIG Secure Health Email Properties

> **Note:** Before configuring the OHIG secure health email properties, update the install_dir>/addons/direct/config/install.properties file with the James installation path.

1. `> cd <install_dir>/addons/direct/config`
2. `> ant create-config-properties-file`

```
[input] Enter james_domain
[input] Enter james_postmaster_email
[input] Enter james_system_email
[input] Enter james_manual_email
[input] Enter james_remotemanager_username
[input] Enter james_remotemanager_password
[input] Enter james_db_host
[input] Enter james_db_port
[input] Enter james_db_sid
[input] Enter james_db_username
[input] Enter james_db_password
[input] Enter direct_db_host
[input] Enter direct_db_port
[input] Enter direct_db_sid
[input] Enter direct_db_username
[input] Enter direct_db_password
[input] Enter arr_host
[input] Enter arr_port
[input] Enter xds_registry_url
[input] Enter xds_pnr_repository_url
```

```
[input] Enter xds_docretrieve_repository_url
[input] Enter xds_repository_id
[input] Enter xds_document_oid_root
[input] Enter xds_submission_set_oid_root
[input] Enter assigning_authority_id
[input] Enter mpi_service_url
[input] Enter mpi_system_code
[input] Enter assigning_authority_oid
[input] Enter assigning_authority_name
[input] Enter pix_service_url
[input] Enter pdq_service_url
[input] Enter mpi_system_oid
[input] Enter mpi_system_name
[input] Enter property_file_name
```

Note: The Apache James Mail Server must be stopped prior to running `> ant config-james`.

3. `> stop`
4. `> ant config-james`

For advanced configuration properties, see Appendix F, "Advanced Oracle Health Sciences Information Gateway Secure Health Email Property Reference".

To edit a password in a properties file:

```
> ant update-config-properties-file-password
```

To edit a property in a properties file:

```
> ant update-config-properties-file-property
```

For more information, refer to Appendix H, "Password Encoding".

2.3.2 Loading Initial Data into Secure Health Email Database

Using the OHIG Secure Health Email Configuration Tool, update the tables with initial data as listed below. See Appendix B, "Oracle Health Sciences Information Gateway Secure Health Email Configuration Tool" for instructions on tool usage.

Note: A version of Open SSL is available in the VM, and, if needed, you may want to use it.

- Add a domain corresponding to your Secure Health Email Server's host name.

  For example, `ant direct-add-domain -Ddomain_name=secure.health-enterprise.org`

- Add trusted anchors which could include trusted Certificate Authorities.

  For example, `ant direct-add-anchor -Ddomain_name=secure.health-enterprise.org -Dcert_file=certs/oracle-cacert.der`

- Add trusted public certificates associating public certificates with external trusted email addresses.

For example, `ant direct-add-public-cert -Ddomain_name=secure.health-enterprise.org -Demail_address=Patient1@live.com -Dcert_file=certs/patient1-cert.der`

- Add trusted private certificates associating public or private certificate pairs with system secure email addresses. Note The email address used in this step should be used to update config parameter `james_init.systemEmailAddress` in the next section.

> **Note:** The email address used in this step should be used to update config parameter `james_init.systemEmailAddress` in the next section, "Configuring Apache James Mail Server for SSL".

Example: `ant direct-add-private-cert -Ddomain_name=secure.health-enterprise.org -Demail_address=direct@secure.health-enterprise.org -Dcert_file=certs/direct-cert.der -Dkey_file=certs/private/direct-key.der`

- Add trusted private certificates associating public/private certificate pairs with internal secure email addresses.

  Example: `ant direct-add-private-cert -Ddomain_name=secure.health-enterprise.org -Demail_address=Dr.John.Doe@secure.health-enterprise.org -Dcert_file=certs/DrJohnDoe-cert.der -Dkey_file=certs/private/DrJohnDoe-key.der`

- Add addresses mapping internal secure email addresses to internal corporate email addresses and to a domain.

  Example: `ant direct-add-address -Ddomain_name=secure.health-enterprise.org -Ddisplay_name="Dr. John Doe" -Demail_address=Dr.John.Doe@secure.health-enterprise.org -type=XD -Dendpoint=Dr.John.Doe@ health-enterprise.org`

2.3.3 Configuring Apache James Mail Server for SSL

1. `> cd <james_install_dir>/apps/james/SAR-INF`

   Edit the `config.xml` file.

   a. Search for "pop3server" and uncomment:

   ```
   <!--
   <useTLS>true</useTLS>
   --!>
   ```

   b. Search for "smtpserver" and uncomment:

   ```
   <!--
   <useTLS>true</useTLS>
   --!>
   ```

   c. Search for "server-sockets" and ensure the correct values are supplied below after un-commenting the tag *<factory name="ssl"..>* :

```
<factory name="ssl"
class="org.apache.avalon.cornerstone.blocks.sockets.TLSSer
verSocketFactory">
 <ssl-factory>
  <keystore>
   <file>keystore/keystore.jks</file>
   <password>changeit</password>
   <key-password>changeit</key-password>
   <type>JKS</type>
   <protocol>SSLv3</protocol>
   <algorithm>SunX509</algorithm>
   <authenticate-client>false</authenticate-client>
  </keystore>
 </ssl-factory>
</factory>
```

Note: If connecting to remote SMTP gateway or SMTP server also thru SSL, makes sure to specify `javax.net.ssl.SSLSocketFactory` to use as socket factory by "ExtendedRemoteDelivery" mailet.

For example:

```
<mailet match="RecipientIsRemote" class="ExtendedRemoteDelivery">
    …
    …
<mail.smtp.socketFactory.class>javax.net.ssl.SSLSocketFactory</mail
.smtp.socketFactory.class>
    …
    …
</mailet>
```

2.3.4 Configuring the Remote Manager

1. `cd <james_install_dir>/apps/james/SAR-INF`

   Edit the `config.xml` file.

   a. Search for "remotemanager", and edit the following two lines:

      ```
      <port>4555</port>
      <account login="root" password="root"/>
      ```

   b. To enable secure telnet, uncomment:

      ```
      <!--
      <useTLS>true</useTLS>
      --!>
      ```

2.3.5 Configuring Logging

Configuring Apache James Mail Server Logging

```
> cd <james_install_dir>/apps/james/SAR-INF
```

Edit the "log-level" settings in the `environment.xml` file.

Configuring Application Code Logging

1. Create a JDK `logging.properties` file in the `<james_install_dir>/bin` directory.

   Example of a `logging.properties` file:

```
handlers= java.util.logging.ConsoleHandler, java.util.logging.FileHandler

.level= INFO

java.util.logging.ConsoleHandler.level = INFO
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter

#java.util.logging.FileHandler.level = ALL
java.util.logging.FileHandler.formatter = java.util.logging.SimpleFormatter
java.util.logging.FileHandler.pattern = logs/direct%g.log
java.util.logging.FileHandler.limit = 50000
java.util.logging.FileHandler.count = 10
```

   Note: You must create the **logs** directory under <james_install_dir>/bin before starting the server.

2. Start the Apache James Mail Server with the system property:

```
-Djava.util.logging.config.file=logging.properties
```

2.4 Managing the Apache James Mail Server

This section provides steps to start the Apache James Mail Server, and to connect to the Remote Manager and then manage the Apache James Mail Server:

- Starting the Apache James Mail Server
- Connecting to the Remote Manager

2.4.1 Starting the Apache James Mail Server

Note: For the default SMTP email ports to open, the James Email Server should be started by the root user.

Before starting the Apache James Mail Server, turn off the sendmail process as follows:

1. Stop the sendmail process.

```
# service sendmail stop
Shutting down sm-client:   [  OK  ]
Shutting down sendmail:    [  OK  ]
```

2. Turn off the sendmail service.

```
# chkconfig --list sendmail
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
# chkconfig sendmail off
# chkconfig --list sendmail
sendmail        0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

To start the Apache James Mail Server, execute the following command:

```
# <james_install_dir>/bin/phoenix.sh start
```

2.4.2 Stopping the Apache James Mail Server

To stop the Apache James Mail Server run the command

```
# <james_install_dir>/bin/phoenix.sh stop
```

2.4.3 Connecting to the Remote Manager

This section provides details for connecting to the Remote Manager and then managing the Apache James Mail Server. It also provides an example of adding a user.

`> telnet localhost <`*PORT*> (Default: 4555)

JAMES Remote Administration Tool 2.3.2

Please enter your login and password

Login id:

<*USERNAME*> (Default: root)

Password:

<*PASSWORD*> (Default: root)

Welcome root. HELP for a list of commands

HELP

Currently implemented commands:

- `help`

  Displays this help.

- `listusers`

  Displays existing accounts.

- `countusers`

  Displays the number of existing accounts.

- `adduser [username] [password]`

  Adds a new user.

- `verify [username]`

  Verifies if a specified user exists.

- `deluser [username]`

  Deletes the existing user.

- `setpassword [username] [password]`

  Sets a user's password.

- `setalias [user] [alias]`

  Locally forwards all email for 'user' to 'alias'.

- `showalias [username]`

  Shows a user's current email alias.

- `unsetalias [user]`

  Unsets an alias for 'user'.

- `setforwarding [username] [emailaddress]`

  Forwards a user's email to another email address.

- `showforwarding [username]`

  Shows a user's current email forwarding.

- `unsetforwarding [username]`

  Removes a forward.

- `user [repositoryname]`

  Changes to another user repository.

- `shutdown [repositoryname]`

  Kills the current JVM (convenient when James is run as a daemon).

- `quit [repositoryname]`

  Closes the connection.

2.4.3.1 Example of Add User

`adduser` <*USERNAME*> <*PASSWORD*>

Create system user (`james_init.systemEmailAddress`) and manual processor or error (`james_init.manualEmailAddress`) email user accounts configured earlier.

For example:

```
adduser direct directpass
adduser error errorpass
```

2.5 Configuring Oracle Health Sciences Information Gateway Secure Health Email

See Appendix B, "Oracle Health Sciences Information Gateway Secure Health Email Configuration Tool" for configuration instructions.

2.6 Additional Configuration

2.6.1 Editing the System Email Templates

```
> cd <james_install_dir>/bin/templates
```

Edit the files in the `templates` directory (see Appendix D, "System Email Template Reference").

2.6.2 Creating Test Certificates

```
> cd <install_dir>/addons/direct/config/openssl_starter
```

Follow the instructions in the `README.txt` file.

2.6.3 Setting Up Components

2.6.3.1 Setting Up a New Source System in Oracle Healthcare Master Person Index for Secure Health Email Server

1. In the OHMPI Oracle Database, create an OHMPI source system and the corresponding IHE domain for the Secure Health Email Server to create new patients.

   Note: Make sure to enable patient feed from OHMPI to OHRL as described in Enabling Assigning Authority Patient Feed from Oracle Healthcare Master Person Index to Oracle Health Sciences Information Manager Health Record Locator on page 2-10.

2. Execute SQL (below) in the OHMPI database using OHMPI DB user account.

   Note: The value for "systemcode" in the "sbyn_systems" table should match the value for "namespaceid" in the "ihe_domains" table. Record the value for "namespaceid" and "universalid". These two values correspond to "mpi_system_name" and "mpi_system_oid" (see the next section), respectively.

```
INSERT INTO sbyn_systems (systemcode, description, status, id_length,format,
input_mask, value_mask, create_date, create_userid) VALUES ('ORCL_DIRECT',
'ORCL_DIRECT', 'A', 23, '[0-9]{23}', 'DDDDDDDDDDDDDDDDDDDDDDD',
'DDDDDDDDDDDDDDDDDDDDDDD', sysdate, 'MPI');
INSERT INTO ihe_domains (namespaceid, universalid, universalidtype,
description) VALUES ('ORCL_DIRECT', '1.1.1', 'ISO', 'Source System for Oracle
Direct');
```

2.6.3.2 Enabling Assigning Authority Patient Feed from Oracle Healthcare Master Person Index to Oracle Health Sciences Information Manager Health Record Locator

1. Log into the OHMPI machine.
2. Edit the file `<config_ohmpi_dir>/ohmpi-ihe.properties`. See Table 2–1, " List of Properties in the ohmpi-ihe.properties File" for a list of the `ohmpi-ihe.properties` properties.

   GlassFish example:

   ```
   <glassfish_install_dir>/domains/<domain_
   name>/config/ohmpi/ohmpi-ihe.properties
   ```

   WebLogic example:

   ```
   <weblogic_install_dir>/user_projects/domains/<domain_
   name>/config/ohmpi/ohmpi-ihe.properties
   ```

3. Ensure that the "aa/oid" value that you enter here matches with the one that is configured in the Secure Health Email Server and the OHIG Gateway. To do this:
   a. If the Secure Health Email Server is not yet configured, look at the property "james_init.assigningAuthorityOid" in the `<install_dir>/addons/direct/config/config.properties` file as this is used during the initial configuration set up. However, if it is already configured, look at the property "james_init.assigningAuthorityOid" in `<james_install_dir>/bin/config.properties` file.
   b. Also look at the corresponding OHIG Gateway property which is "assigningAuthorityId" in `<config_nhin_dir>/adapter.properties` file.

Table 2–1 List of Properties in the ohmpi-ihe.properties File

Property Name	Description	Example
enable_patient_feed	"true" enables sending Assigning Authority patient feed to OHRL, "false" disables it. In order for Secure Health Email to work, feed must be enabled.	`true`
enable_euid_query	“true” to return Global or EUID domain patient ID references also known as Affinity Domain Patient ID with PIX and PDQ queries. This must be “true” for OHIG Secure Health Mail Server to get Affinity Domain Patient IDs.	true
registry/endpoint	The URL of OHRL or XDS.b Doc Registry Web service endpoint URL.	`http://<oracle_registry_host_ip>:8080/hrl/regsvc`
aa/oid	The Assigning Authority OID that OHMPI uses while sending a patient feed to OHRL.	1.3.6.1.4.1.21367.2010.1.2.300
aa/namespace	The Assigning Authority Name.	OHMPI Assigning Auth
pisv3/device/oid	Patient Identity Source v3 (Sender) Device Universal ID.	1.3.6.1.4.1.21367.13.10.380
pisv3/device/namespace	Patient Identity Source v3 (Sender) Device Namespace ID.	PIX_X_REF_MGR_ORACLE
pisv3/device/org/oid	Patient Identity Source v3 (Sender) Device Organization Universal ID.	1.3.6.1.4.1.21367.13.50.5380
pisv3/device/org/namespace	Patient Identity Source v3 (Sender) Device Organization Namespace ID.	Oracle
registry/device/oid	Registry (Receiver) Device Universal ID	0.0.0.0.0.0.0.0.0.0
registry/device/namespace	Registry (Receiver) Device Namespace ID	Registry_Device

Table 2–1 (Cont.) List of Properties in the ohmpi-ihe.properties File

Property Name	Description	Example
registry/device/org/oid	Registry (Receiver) Device Organization Universal ID	0.0.0.0.0.0.0.0.1
registry/device/org/namespace	Registry (Receiver) Device Organization Namespace ID	Registry_Device_Organization

2.6.3.3 Adding Unknown Document Type's Coding Scheme to Oracle Health Sciences Information Manager Health Record Locator

The server uses the following "unknown" properties when it is not able to infer the coding scheme and codes, for Healthcare Facility Type or Practice Setting classifications, from the XDM metadata and CDA and/or CCD documents.

> **Note:** See also Table F–1, " Advanced Secure Health Email Properties" on page F-1.

-- IHE specified class Scheme value for Healthcare Facility classification is `urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1`.

- `unknownFacilityCodingScheme`
- `unknownFacilityCode`

-- IHE specified class Scheme value for Practice Setting classification is `urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead`.

- `unknownPracticeSettingCodingScheme`
- `unknownPracticeSettingCode`

By default, the server will use `1.3.6.1.4.1.21367.3100.1.2` as the coding scheme and `Unspecified` as the code.

To add these coding schemes and codes to the OHIM Health Record Locator, perform the following steps:

1. Log into the OHIM Health Record Locator.
2. Edit the file `<config_hrl_dir>/codes.xml`.

   GlassFish example:

   `<glassfish_install_dir>/domains/<domain_name>/config/hrl/codes/codes.xml`

   WebLogic example:

   `<weblogic_install_dir>/user_projects/domains/<domain_name>/config/hrl/codes/codes.xml`

3. Add the configured unknown document type's coding schemes to the HRL `codes.xml` file.

   For example,

```
<CodeType name="healthcareFacilityTypeCode"
classScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1">
 ...
    <Code code="Unspecified" codingScheme="1.3.6.1.4.1.21367.3100.1.2"
display="Unspecified"/>
</CodeType>
```

```
<CodeType name="practiceSettingCode"
classScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead">
...
    <Code code="Unspecified" codingScheme="1.3.6.1.4.1.21367.3100.1.2"
display="Unspecified"/>
</CodeType>
```

2.7 Testing Secure Health Email

Inbound and Outbound Examples

```
> cd <install_dir>/addons/direct/config/examples
```

Follow the instructions in the `README.txt` file.

A

Running the Oracle Health Sciences Information Gateway Secure Health Email Installer

This appendix describes how to run the OHIG Secure Health Email installer. It contains the following topics:

A.1 Running the Secure Health Email Installer

```
$ cd <install_dir>
$ java -jar ohig_direct_installer.jar
Oracle HIG Direct Installer 2.0.1.0
-- Command
Choose option install_command (usage, version, install)
> install
Starting init install
-- James install directory
Enter james_install_dir [#null]
> james
```

B

Oracle Health Sciences Information Gateway Secure Health Email Configuration Tool

This appendix provides a description and examples of the OHIG Secure Health Email script.

B.1 Using the Secure Health Email Configuration Tool

This section provides a description of the OHIG Secure Health Email Script, and then provides command line tool examples.

B.1.1 Oracle Health Sciences Information Gateway Secure Health Email Script

`usage: ant <command> -D<option>*`

Use the above script to configure the OHIG Secure Health Email environment.

B.1.1.1 Commands

- `direct-add-address`

  Associate an address with an OHIG Secure Health Email server domain, mapping an internal secure email address to an internal corporate email address

  – **Options**

    * `domain_name=<HOSTNAME>`

      The OHIG Secure Health Email server domain name

    * `display_name=<STRING>`

      The display name for the internal secure email user

    * `email_address=<EMAIL>`

      An internal secure email address

    * `type=<TYPE>`

      The type of the endpoint (XD, SMTP)

    * `endpoint=<EMAIL>`

      An internal corporate email address

- `direct-add-anchor`

  Add a certificate to the list of trusted anchor certificates

  - **Options**
    - `domain_name=<HOSTNAME>`

      The direct email server domain name
    - `cert_file=<FILE>`

      A public certificate in `.der` format
- `direct-add-domain`

  The OHIG Secure Health Email server domain name

  - **Options**
    - `domain_name=<HOSTNAME>`

      The OHIG Secure Health Email server domain name
- `direct-add-public-cert`

  Associate a public certificate with an external trusted email address

  - **Options**
    - `email_address=<EMAIL>`

      An external trusted email address
    - `cert_file=<FILE>`

      A public certificate in `.der` format
- `direct-add-private-cert`

  Associate a public or private certificate pair with an internal secure email address

  - **Options**
    - `email_address=<EMAIL>`

      An internal secure email address
    - `cert_file=<FILE>`

      A public certificate in `.der` format
    - `key_file=<FILE>`

      A private certificate in `.der` format
- `direct-add-setting`

  Set a configuration setting

  - **Options**
    - `name=<STRING>`

      The setting name
    - `value=<STRING>`

      The setting value
- `direct-add-user`

  Add a user to james email server

- **Options**
  - name=<*STRING*>

    The user name
  - pass=<*STRING*>

    The user pass

B.1.2 Example of Secure Health Email Commands

- direct-add-address

  > ant direct-add-address *-Ddomain_name=<HOSTNAME> -Ddisplay_name=<STRING> -Demail_address=<EMAIL> -Dtype=<TYPE> -Dendpoint=<EMAIL>*

- direct-add-user

  > ant direct-add-user -Duser=<*USERNAME*> -Dpass=<*PASSWORD*>

C

Oracle Health Sciences Information Gateway Secure Health Email Tables

This appendix provides six OHIG Secure Health Email tables that list column names and their data type.

This appendix includes the following section:

C.1 Using the Secure Health Email Tables

This appendix includes the following OHIG Secure Health Email tables:

Table C–1 ADDRESS

COLUMN_NAME	DATA_TYPE	COMMENTS
ID	NUMBER(19,0)	Primary key
CREATETIME	TIMESTAMP(6)	Create time
DISPLAYNAME	VARCHAR2(255 BYTE)	Display name
DOMAINID	NUMBER(19,0)	Foreign key to address's DOMAIN
EMAILADDRESS	VARCHAR2(255BYTE)	Internal secure email address
ENDPOINT	VARCHAR2(255 BYTE)	Internal corporate email address
STATUS	NUMBER(10,0)	Object status (0=NEW, 1=ENABLED, 2=DISABLED)
TYPE	VARCHAR2(64 BYTE)	Type of address (XD or SMTP)

Table C–1 (Cont.) ADDRESS

COLUMN_NAME	DATA_TYPE	COMMENTS
UPDATETIME	TIMESTAMP(6)	Update time

Table C–2 ANCHOR[1]

COLUMN_NAME	DATA_TYPE	COMMENTS
ID	NUMBER(19,0)	Primary key
CERTIFICATEDATA	BLOB	Anchor binary data
CERTIFICATEID	NUMBER(19,0)	<deprecated>
CREATETIME	TIMESTAMP(6)	Create time
FORINCOMING	NUMBER(1,0)	Use anchor for incoming messages (0=NO, 1=YES)
FOROUTGOING	NUMBER(1,0)	Use anchor for outgoing messages (0=NO, 1=YES)
OWNER	VARCHAR2(255 BYTE)	Domain hostname (see DOMAIN) or User name
STATUS	NUMBER(10,0)	Object status (0=NEW, 1=ENABLED, 2=DISABLED)
THUMBPRINT	VARCHAR2(255 BYTE)	Anchor thumbprint
VALIDENDDATE	TIMESTAMP(6)	Anchor expiration date
VALIDSTARTDATE	TIMESTAMP(6)	Anchor start date

[1] Changes to the ANCHOR table require a restart of the application.

Table C–3 CERTIFICATE

COLUMN_NAME	DATA_TYPE	COMMENTS
ID	NUMBER(19,0)	Primary key
CERTIFICATEDATA	BLOB	Certificate binary data
CREATETIME	TIMESTAMP(6)	Create time
OWNER	VARCHAR2(255 BYTE)	Certificate associated email address
PRIVATEKEY	NUMBER(1,0)	Holds public and private key (0=NO public only, 1=YES)
STATUS	NUMBER(10,0)	Object status (0=NEW, 1=ENABLED, 2=DISABLED)
THUMBPRINT	VARCHAR2(255 BYTE)	Certificate thumbprint

Table C–3 (Cont.) CERTIFICATE

COLUMN_NAME	DATA_TYPE	COMMENTS
VALIDENDDATE	TIMESTAMP(6)	Certificate expiration date
VALIDSTARTDATE	TIMESTAMP(6)	Certificate start date

Table C–4 DOMAIN[1]

COLUMN_NAME	DATA_TYPE	COMMENTS
ID	NUMBER(19,0)	Primary key
CREATETIME	TIMESTAMP(6)	Create time
DOMAINNAME	VARCHAR2(255 BYTE)	Domain hostname
POSTMASTERADDRESSID	NUMBER(19,0)	Foreign key to domain's postmaster ADDRESS
STATUS	NUMBER(10,0)	Object status (0=NEW, 1=ENABLED, 2=DISABLED)
UPDATETIME	TIMESTAMP(6)	Update time

[1] Changes to the DOMAIN table require a restart of the application.

Table C–5 SEQUENCE

COLUMN_NAME	DATA_TYPE	COMMENTS
SEQ_COUNT	NUMBER(38,0)	Sequence count
SEQ_NAME	VARCHAR2(50 BYTE)	Sequence name

Table C–6 SETTING[1]

COLUMN_NAME	DATA_TYPE	COMMENTS
ID	NUMBER(19,0)	Primary key
CREATETIME	TIMESTAMP(6)	Create time
NAME	VARCHAR2(255 BYTE)	Setting name
STATUS	NUMBER(10,0)	Object status (0=NEW, 1=ENABLED, 2=DISABLED)
UPDATETIME	TIMESTAMP(6)	Update time
VALUE	VARCHAR2(1024 BYTE)	Setting value

[1] Changes to the SETTING table require a restart of the application.

Required and Optional SETTINGs

Table C–7 Required Settings

NAME	DEFAULT	VALUE	COMMENT
AnchorStoreType	n/a	WS	Required to be WS

Table C–7 (Cont.) Required Settings

NAME	DEFAULT	VALUE	COMMENT
PublicStoreType	n/a	WS	Required to be WS
PrivateStoreType	n/a	WS	Required to be WS

Table C–8 Optional Settings

NAME	DEFAULT	VALUE	COMMENT
AnchorResolverType	uniform	uniform, multidomain	uniform ■ `FORINCOMING` anchors, are used for both incoming and outgoing messages multidomain ■ `FORINCOMING` anchors, are used for incoming messages ■ `FORINCOMING` anchors, are used for outgoing messages
BadMessageSaveFolder	null	<directory name>	Test directory for logging bad messages
IncomingMessageSaveFolder	null	<directory name>	Test directory for logging incoming messages
OutgoingMessageSaveFolder	null	<directory name>	Test directory for logging outgoing messages
RawMessageSaveFolder	null	<directory name>	Test directory for logging raw messages

D

System Email Template Reference

This appendix provides the System Email Template properties and comments on them. It includes the following section

D.1 System Email Template Table

The following table provides the name, file name, property, and comments about the System Email template:

```
> cd <james_install_dir>/bin/templates
```

Table D–1 System Email Template

NAME	FILENAME	PROPERTY	COMMENT
Header	Header.txt	**now**	The day and time of notification generation in ISO 8601 format.
		hostname	The host name of this system.
		hostaddr	The IP address of this system. (IPv4 or IPv6).
Footer	Footer.txt	**now**	The day and time of notification generation in ISO 8601 format.
		hostname	The host name of this system.
		hostaddr	The IP address of this system. (IPv4 or IPv6).
Error Notification (ERROR)	ErrMessage.txt	**now**	The day and time of notification generation in ISO 8601 format.
		hostname	The host name of this system.
		hostaddr	The IP address of this system. (IPv4 or IPv6).
		subject	The subject of the original message.
		sender	The sender of the received message.
		timeDone	The time of receipt.
		recipients	The recipients for this message.
		recipCount	The number of recipients for this message.

Table D–1 (Cont.) System Email Template

NAME	FILENAME	PROPERTY	COMMENT
Message Disposition Notification-Message (MDN)	MdnMessage.txt	**now**	The day and time of notification generation in ISO 8601 format.
		hostname	The host name of this system.
		hostaddr	The IP address of this system. (IPv4 or IPv6).
		subject	The subject of the original message.
		sender	The sender of the received message.
		timeDone	The time of receipt.
		recipients	The recipients for this message.
		recipCount	The number of recipients for this message.
		action	'processed' or 'error'
Message Disposition Notification-Report	MdnReport.txt	**hostname**	The host name of this system.
		recipients	The recipients of this message.
		messageId	The message ID of the original message.
		system	The system address.
		action	'processed' or 'error'
Notification of Document Availability (NAV)	NavMessage.txt	**now**	The day and time of notification generation in ISO 8601 format.
		hostname	The host name of this system.
		hostaddr	The IP address of this system. (IPv4 or IPv6).
		subject	The subject of the original message.
		sender	The sender of the received message.
		timeDone	The time of receipt.
		recipients	The recipients for this message.
		recipCount	The number of recipients for this message.
		action	'processed' or 'error'
System Notification Message (SYS)	SysMessage.txt	**now**	The day and time of notification generation in ISO 8601 format.
		hostname	The host name of this system.
		hostaddr	The IP address of this system. (IPv4 or IPv6).
		subject	The subject of the original message.
		sender	The sender of the received message.
		timeDone	The time of receipt.
		recipCount	The number of recipients for this message.
		action	'processed' or 'error'

E

Inbound and Outbound Email Matrix

This appendix provides an inbound and outbound matrix for OHIG Secure Health Email.

This appendix includes the following section:

E.1 Inbound and Outbound Email

See the following tables for inbound and outbound email requests.

Table E–1 Inbound

Accepted Email Types	Required Content-Type	Outcome
S/MIME Email + one or more CCD Attachments	multipart/mixed "text/xml"	When trusted ■ On processing success: Sender receives "processed" MDN If `ADDRESS.TYPE == XD` Recipients receive NAV If `ADDRESS.TYPE == SMTP` Recipients receive SYS ■ On processing failure: Sender receives "error" MDN Manual handler receives ERROR When Untrusted ■ Email is dropped
S/MIME Email + single XDM Attachment	multipart/mixed "*.zip"	

Table E–2 Outbound

Accepted Email Types	Required Content-Type	Outcome
Email + single XDS Registry Request[1] Attachment	multipart/mixed "text/xml"	When trusted ■ On processing success: Sender receives "processed" MDN Recipients receive XDM ■ On processing failure: Sender receives "error" MDN Manual handler receives ERROR When untrusted ■ Email is dropped
Email + single XDM Attachment	multipart/mixed "*.zip"	

[1] See Appendix G, "XDS Registry Request XML Schema Reference."

F

Advanced Oracle Health Sciences Information Gateway Secure Health Email Property Reference

This appendix provides the Advanced OHIG Secure Health Email properties and comments on them.

This appendix includes the following section:

F.1 Advanced Secure Health Email Properties

The following table provides the property, default value, and comments about the Advanced Secure Health Email properties:

1. `> cd <james_install_dir>/app/james/SAR-INF`

   Edit the `config.xml` file.

2. Search for "InitMailet".

Table F–1 Advanced Secure Health Email Properties

PROPERTY	DEFAULT	COMMENTS
certStoreCachePolicyMaxItems	1000	Maximum certificate cache size
certStoreCachePolicyTtlSecs	86400 (3600*24=one day)	Time-to-live in seconds for certificates in cache
errSubjectLine	Error Notification	Error notification email subject line
mdnSubjectLine	Message Disposition Notification	Message disposition notification email subject line
navSubjectLine	Document Availability Notification	Document availability notification email subject line
sysSubjectLine	System Notification	System notification email subject line
xdmSubjectLine	XDM/1.0/DDM	Cross-enterprise document media interchange email subject line

Table F–1 (Cont.) Advanced Secure Health Email Properties

PROPERTY	DEFAULT	COMMENTS
unknownDocClassCodeCodingScheme	1.3.6.1.4.1.21367.3100.1.2	Unknown document type's coding scheme
unknownDocClassCodeCode	Clinical Data	Unknown document type's code
unknownDocClassCodeCodeDisplayName	Unspecified clinical data transferred via OHIG Secure Health Email	Unknown document type's display name
unknownFacilityCodingScheme	1.3.6.1.4.1.21367.3100.1.2	Unknown healthcare facility type's coding scheme
unknownFacilityCode	Unspecified	Unknown healthcare facility type's code
unknownFacilityCodeDisplayName	Unspecified clinical data transferred via OHIG Secure Health Email	Unknown healthcare facility type's display name
unknownPracticeSettingCodingScheme	1.3.6.1.4.1.21367.3100.1.2	Unknown practice setting type's coding scheme
unknownPracticeSettingCode	Unspecified	Unknown practice setting type's code
unknownPracticeSettingCodeDisplayName	Unspecified clinical data transferred via OHIG Secure Health Email	Unknown practice setting type's display name
unknownConfCodeCodingScheme	Connect-a-thon confidentialityCodes	Unknown confedentiality code's coding scheme
unknownConfCodeCode	N	Unknown confedentiality code
unknownConfCodeCodeDisplayName	Normal	Unknown confedentiality code's display name

G

XDS Registry Request XML Schema Reference

This appendix provides a reference to the XDS Registry Request XML Schema and an example of an XDS registry request.

This appendix includes the following section:

G.1 XDS Registry Request XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://hsgbu.oracle.com/direct/XdsRegistry/1"
xmlns:tns="http://hsgbu.oracle.com/direct/XdsRegistry/1"
elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:element name="XdsRegistryRequest">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="XdsSubmissionSets" type="tns:XdsSubmissionSetsType"
maxOccurs="1" />
   </xs:sequence>
  </xs:complexType>
 </xs:element>

 <xs:complexType name="XdsSubmissionSetsType">
  <xs:sequence>
   <xs:element name="XdsSubmissionSet" type="tns:XdsSubmissionSetType"
maxOccurs="unbounded" />
  </xs:sequence>
 </xs:complexType>

 <xs:complexType name="XdsSubmissionSetType">
  <xs:sequence>
   <xs:element name="XdsDocumentEntry" type="tns:XdsDocumentEntryType"
minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attribute name="id" type="tns:OID" use="required" />
  <xs:attribute name="recommendedRegistry" type="xs:string" use="optional" />
 </xs:complexType>

 <xs:complexType name="XdsDocumentEntryType">
  <xs:attribute name="id" type="tns:OID" use="required" />
 </xs:complexType>
```

```
 <xs:simpleType name="OID">
  <xs:restriction base="xs:string">
   <xs:whiteSpace value="collapse"/>
  </xs:restriction>
 </xs:simpleType>
</xs:schema>
```

Example of XDS Registry Request

```
<?xml version="1.0" encoding="UTF-8"?>
<XdsRegistryRequest xmlns="http://hsgbu.oracle.com/direct/XdsRegistry/1">
 <XdsSubmissionSets>
  <XdsSubmissionSet id="1.3.6.1.4.1.21367.2100.1.2.3.1305228382703.7569" />
 </XdsSubmissionSets>
</XdsRegistryRequest>
```

H

Password Encoding

This appendix contains the following topics:

H.1 Editing cipher.properties

```
Default base64
cipher_algorithm=b64
```

For example, hex

```
cipher_algorithm=hex
```

For example, des

```
cipher_algorithm=des
cipher_passphrase=hiapassphrase123
cipher_salthex=0102030405060F0F
cipher_iterations=19
```

For example, desede

```
cipher_algorithm=desede
cipher_passphrase=hiapassphrase123
cipher_salthex=0001020304050F0F
cipher_iterations=19
```

For example, aes

```
cipher_algorithm=aes
cipher_passphrase=hiapassphrase123
cipher_salthex=001020304050F0F
cipher_ivhex=0001020304050F0F08090A0B0C0D0E0F
cipher_iterations=19
```

For example, rsa

```
cipher_algorithm=rsa
cipher_privatekeyfile=private.key
```

```
cipher_publickeyfile=public.key
```

H.2 Editing config.properties

- To edit a password in a properties file, execute the following command:

  ```
  > ant update-config-properties-file-password
  ```

- To edit a property in a properties file, execute the following command:

  ```
  > ant update-config-properties-file-property
  ```

H.3 config.xml and beans.xml

For the files config.xml and beans.xml:

- Variables and/or xml attributes starting and ending with `${}` will be retrieved from the config.properties file accounting for encoding and decoding. Use this in conjunction with `> ant update-config-properties-file-password`.

Acronyms

This section provides a list of commonly used acronyms.

I.1 Acronyms

CCD
Continuity of Care Document

CDA
Clinical Document Architecture

DER
Distinguished Encoding Rules

HIE
Health Information Exchange

HIO
Health Information Organization

HL7
Health Level 7

IHE
Integrating the Healthcare Enterprise

NAV
Notification Of Document Availability

NHIE
Nationwide Health Information Exchange

NHIN
Nationwide Health Information Network

NHIO
Nationwide Health Information Organization

OHIG
Oracle Health Sciences Information Gateway

OHIM
Oracle Health Sciences Information Manager

SAML
Security Assertion Markup Language

VM
Oracle Virtual Machine

WSDL
Web-Service Definition Language

XDM
Cross-Enterprise Document Media Interchange

J

High-level Network Diagram

This appendix provides a high level diagram of the OHIG Secure Health Email network.

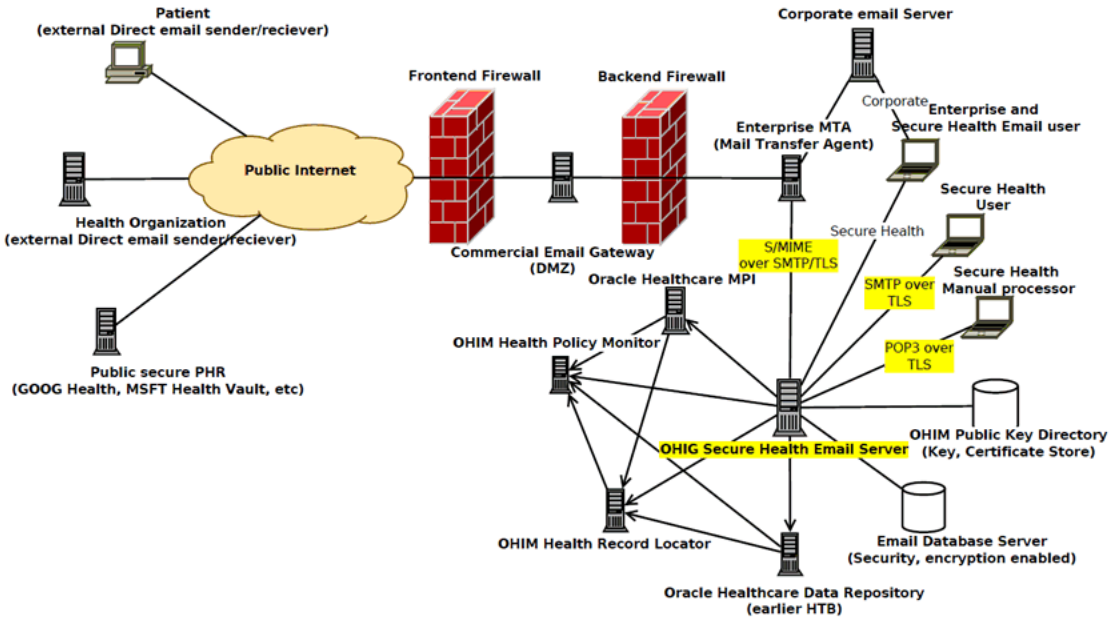
This appendix includes the following section:

- OHIG Secure Health Email Network

J.1 OHIG Secure Health Email Network

The below figure presents a high-level diagram of the OHIG Secure Health Email network.

Figure J–1 High-level View of the OHIG Secure Health Email Network



K

References

This section provides links to supporting documentation and resources.

K.1 Apache James Mail Server

Please visit the following links for more information about the Apache James Email Server and documentation:

James 2.3.2 Documentation

http://james.apache.org/server/2/index.html

Using TLS

http://james.apache.org/server/2/usingTLS.html

Glossary

This section provides definitions of commonly used words.

Clinical Document Architecture (CDA)

Clinical Document Architecture (CDA) is a flexible XML-based clinical document architecture that uses the HL7 document markup standard that specifies the structure and semantics for the purpose of exchanging these documents. CDA documents use HL7 v3 Data Types and obtain their machine processable meaning from the HL7 Reference Information Model (RIM). Although the CDA is not a specific document, it can be used to express many types of documents.

CCD, Lab Report (HITSPC37), XDS-MS Discharge Summary (HITSP C48), and History and Physical (HITSP C84) are some of the types of CDA documents. CDA document data sections can be few or numerous and contain narrative text or structured data elements with text or code.

CONNECT

Is a software solution that supports health information exchange that implements Nationwide Health Information Network (NHIN) standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country. It enables public and private organizations to participate in the NHIN by leveraging their existing health information systems.

CONNECT Adapter

The portion of the CONNECT architecture that encapsulates the components most likely to be customized or replaced by an organization implementing CONNECT.

CONNECT Gateway

The portion of the CONNECT architecture that encapsulates the components most likely to be use as-is by an organization without modification. These components are primarily responsible for orchestrating information exchange with the NHIN.

Continuity of Care Document (CCD)

The Continuity of Care Document (CCD), in accordance with the ASTM E2369-05 Standard Specification for Continuity of Care Record (CCR), describes constraints on the HL7 Clinical Document Architecture, Release 2 (CDA) specification, and is intended as an alternate for the institutions or organizations committed to implementation of the HL7 Clinical Document Architecture specified in the ASTM ADJE2369 implementation. The CCD is just one of numerous types of CDA documents that can contain some of the same CCD sections, but can also contain different sections.

The Continuity of Care Record (CCR) shows one or more patient healthcare encounters, and is the core data set of the most relevant information facts in the patient's health records. It is used to support the patient's continuity of care, and provides a means for a healthcare practitioner, system, or setting to gather together a collection of all of the patient's pertinent data forward it to another practitioner, system, or setting.

Cross-Enterprise Document Media Interchange (XDM)

XDM uses a common file and directory structure over standard media to provide a document interchange that allows patients to carry medical documents using physical media. It also allows person-to-person email for the transfer of medical documents.

Health Information Exchange

Health Information Exchange is an entity that enables the movement of health-related data among entities within a state, a region, or a non-jurisdictional participant group, which might include "classic" regional health information organizations at regional and state levels, Health Information Organization integrated delivery systems and health plans, or health data banks that support health information exchange.

Health Information Organization

Health Information Organization is an organization that enables the movement of health-related data among entities, evolving as a replacement term for health information exchange or HIE. Healthcare Information Technology Standards Panel Or simply HITSP, a cooperative partnership between the public and private sectors formed and supported by ONC for the purpose of harmonizing and integrating standards that will meet clinical and business needs established by AHIC use cases for sharing information among organizations and systems.

Integrating the Healthcare Enterprise

Integrating the Healthcare Enterprise is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information, promoting and coordinating the use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care. The Nationwide Health Information Network is being developed by ONC to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare.

Nationwide Health Information Network

Nationwide Health Information Network is a set of standards, services and policies that enable secure health information exchange over the Internet. The network will provide a foundation for the exchange of health information across diverse entities, within communities and across the country, helping to achieve the goals of the HITECH Act. This critical part of the national health IT agenda will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care so as to improve population health.

Nationwide Health Information Network Gateway

Within the CONNECT solution, the implementation of the core NHIN services and service interface specifications, comprising the CONNECT gateway and CONNECT adapter. The NHIN health information exchange or NHIE, a health information exchange that implements the NHIN architecture, processes, and procedures, is accredited as a participant of the NHIN.

Oracle Virtual Machine

Oracle Virtual Machine is a platform that provides a fully equipped environment for better leveraging the benefits of virtualization technology. Oracle VM enables you to deploy operating systems and application software within a supported virtualization environment.

Oracle Virtual Machine Manager

Oracle Virtual Machine Manager provides the user interface, which is a standard ADF (Application Development Framework) web application, to manage Oracle VM Servers. It manages virtual machine lifecycle, including creating virtual machines from installation media or from a virtual machine template, deleting, powering off, uploading, deployment and live migration of virtual machines. It manages resources, including ISO files, virtual machine templates, and sharable hard disks.

Oracle Virtual Machine Server

Oracle Virtual Machine Server allows a self-contained virtualization environment designed to provide a lightweight, secure, server-based platform for running virtual machines. Oracle VM Server is based upon an updated version of the underlying Xen hypervisor technology, and includes Oracle VM Agent.

Oracle Virtual Machine Template

Oracle Virtual Machine Template provides an innovative approach to deploying a fully configured software stack by offering pre-installed and pre-configured software images. Use of Oracle VM templates eliminates the installation and configuration costs, and reduces the ongoing maintenance costs helping organizations achieve faster time to market and lower cost of operations.

Security Assertion Markup Language

Security Assertion Markup Language is an XML-based standard for exchanging authentication and authorization data between security domains.

Web Services Description Language

Web Services Description Language is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.

XML Schema

XML Schema is a means for defining the structure, content, and semantics of XML documents.

Index