1 Introduction
Oracle Health Sciences Translational Research Center (TRC) comprises of two products - Oracle Health Sciences Cohort Explorer (OHSCE) and Oracle Health Sciences Omics Data Bank (ODB). Through a user-friendly interface, TRC enables posing biologically meaningful questions by combining both clinical and cross-platform omics data. It also enables visualizing clinical records and omics features using both in-house business intelligence tools and omics viewers developed by the research community. This guide describes various security guidelines for the TRC installation.

1.1 General Security Principles
The following principles are fundamental to using any application securely.

1.1.1 Keep Software Up To Date
One of the principles of good security practice is to keep all software versions and patches up to date.

1.1.2 Keep Up To Date on Latest Security Information Critical Patch Updates
Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October. We highly recommend customers apply these patches as soon as they are released.

1.1.3 Configuring Strong Passwords on the Database
Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, refer to the Oracle® Database Security Guide specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
Passwords for the database application-specific schema accounts, such as HDM.

Password for the database listener. You should not configure a password for the database listener as that will enable remote administration. For more information, refer to the Removing the Listener Password section of Oracle® Database Net Services Reference 11g Release 2 (11.2)

1.4 Following the Principle of Least Privilege
The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants — especially early on in an organization’s life cycle when people are few and work needs to be done quickly — often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Before executing the DDL scripts to create Healthcare Data Warehouse Foundation (HDWF), the database user should be created with the specified limited set of privileges. DBA access should not be given to the user.

2 Security Guidelines for Database Objects and Database Options
This section describes security guidelines for TRC database objects and database options.

2.1 Translational Research Center Objects
TRC contains database objects. You can use DDL scripts and PL/SQL procedures and functions to create database objects and DML scripts to create seed data. These files are part of the media pack.

The guidelines for installing and configuring Oracle Database Server are available here http://docs.oracle.com/cd/E11882_01/network.112/e16543/toc.htm.

2.2 Oracle Database Options
The Oracle Database has options that provide additional security features. TRC may include data that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. These features can help you comply with those guidelines.

Database Vault
TRC includes data that may fall under HIPAA or other regulations outside the United States. These data are highly sensitive and only those with a need to know should have access to it. To prevent DBAs and others from seeing the data, it is recommended that Oracle Database Vault be used to limit access to the TRC schema to the TRC user to prevent DBAs and other superuser accounts from accessing the data.

Note: Database Vault requires a separate license.

Oracle Audit Vault
Oracle Audit Vault automates the audit collection, monitoring, and reporting process, turning audit data into a key security resource for detecting unauthorized activity.
Consider using this feature to satisfy compliance regulations such as SOX, PCI, and HIPAA, and to mitigate security risks. Note that Oracle Audit Vault requires a separate license. TRC sets the client identifier in the database session to allow identification of the end user.

**Transparent Data Encryption**

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. If you employ Transparent Data Encryption, applications do not have to be modified and continue to work seamlessly as before. Data is automatically encrypted when it is written to disk and automatically decrypted when accessed by the application. Key management is built in, eliminating the complex task of creating, managing and securing encryption keys. Note that the Advanced Security Option is licensed separately from the database.

**Tablespace Encryption**

Tablespace Encryption is another component of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. Tablespace encryption facilitates encryption of the entire tablespace contents, rather than having to configure encryption on a column-by-column basis. It encrypts data at the datafile level to keep users from viewing the oracle datafiles directly. Oracle recommends that you perform tablespace encryption for maximum protection.

**User Management**

WebLogic Server supports several authentication security providers, for example, LDAP. For more information, see http://docs.oracle.com/cd/E29542_01/web.1111/e13707/atn.htm. TRC supports any authentication security providers supported by WebLogic Server.

**Virtual Private Database**

TRC now uses Row Level Security (also referred to as Virtual Private Database or VPD) to store identifiable attributes. The policies created on the tables containing identifiable attributes are always controlled by policies to prevent any user from being able to query this information. The Row Level Security option used will return null values for any column value that a user does not have permission to view. TRC now has views on all of these patient tables to use a NVL function on each identifiable attribute to show an obfuscated value instead of the real value. If a user has permission to see the real value, then the real value will be returned in the view. Earlier versions of TRC only showed obfuscated values and never stored real identifiable attributes.

There is an optional configuration to hide the rows of data that any user does not have permissions to view. By default this option is not enabled, meaning that users can query the data and see obfuscated values for all protected attributes. There is a default configuration that allows access to all identifiable data. Specific users that have proper credentials can be assigned access to this configuration. All control to the assignments of users is allowed to only users that have the VPD_ADMIN role assigned, and all calls use the CDM.VPD_UTIL package. For more information, see the Oracle® Health Sciences Translational Center Administrator’s Guide.
3 Revoking Unnecessary Grants
For security purposes, you must revoke all unnecessary grants on the schema (grants that are needed during installation and are not required during runtime). You need DBA privileges to perform this action.

1. Revoke unnecessary grants from Omics Data Bank Schema.
   Execute odb_revoke_grants.sql to remove unnecessary grants from Omics Data Model Schema. This script should be executed by a user with DBA privileges.

2. Revoke unnecessary grants from Cohort Data Model Schema.
   Execute cohort_revoke_grants.sql to remove unnecessary grants from Cohort Data Model Schema. This script should be executed by a user with DBA privileges.

4 Disabling Unnecessary Operating System Level Services
This section suggests various unused operating system level services that you can disable to improve security.

4.1 Disabling the Telnet Service
Oracle Health Sciences Cohort Explorer does not use the Telnet service.

Telnet listens on port 23 by default. If the Telnet service is available on any computer, Oracle recommends that you disable Telnet in favor of Secure Shell (SSH). Telnet, which sends clear-text passwords and user names through a log-in, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

4.2 Disabling Other Unused Services
Oracle Health Sciences Cohort Explorer does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of Oracle Health Sciences Cohort Explorer. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.
5 Designing Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers, for example, only allowing communication to the database tier on the port used for SQL*NET communications, (1521 by default).
- Placing firewalls between servers so that only expected traffic can move between servers.

6 Security Guidelines for Oracle Data Integrator

While installing and configuring the Oracle Data Integrator (ODI) Server, follow the guidelines documented in section Managing Security in Oracle Data Integrator in the document Oracle® Fusion Middleware Developer’s Guide for Oracle Data Integrator 11g Release 1 (11.1.1).

7 Security Guidelines for the Middle Tier

This section describes the security guidelines for the TRC middle tier.

7.1 Removing Unused Applications from WebLogic

Currently, the WebLogic Server installation includes the entire JDK and some additional WebLogic Server development utilities (for example, wlsvc). These development programs are not needed at runtime and can be safely removed. The following are recommendations for making a WebLogic Server installation more secure:

- Do not install the WebLogic Server sample applications.
- Delete development tools, such as the Configuration Wizard and the jCOM tools.
- Delete the Derby database, which is bundled with WebLogic Server for use by the sample applications and code examples as a demonstration database.

For more details, refer to the Determining Your Security Needs section in Oracle® Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 12c Release 1 (12.1.1).

7.2 Enabling SSL

Due to the complexity in setting up SSL it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL.

It is optional to enable SSL, but Oracle recommends SSL for a production environment.

To enable SSL:

1. Log into WebLogic Server Administration Console.
2. Click the Environment node in the Domain Structure pane and click Servers in Environment table.
3. Click the server where you deployed TrcApp.ear.
4. Click the Configuration tab.
5. Click the General tab.
6. If Save is disabled, click Lock & Edit in the Change Center pane.
7. Select the SSL Listen Port Enabled check box and enter a port number.
8. To disable non-SSL port, deselect the Listen Port Enabled check box.
9. Click Save.
10. Click Activate Changes in the Change Center pane, if it is enabled.
11. Click the Control tab.
12. Click the Start/Stop tab.
13. Click Restart SSL
14. Click Yes.

The “SSL channels have been successfully restarted.” message appears.

You must also configure SSL, identity, and trust. For more information, refer to Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.5).

7.3 Configuring SSL

To set up SSL, perform the following steps:
1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server. Use the digital certificates, private keys, and trusted CA certificates provided by WebLogic Server, the CertGen utility, the keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.
2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in keystores.
3. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.
4. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console. Optionally, set configuration options that require the presentation of client certificates (for two-way SSL).

For more details, refer to Configuring SSL section in Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c Release 1 (12.1.1).

7.4 Disabling Other Unused Services

Oracle Health Sciences Cohort Explorer does not use the following services or information for any functionality:
- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of Oracle Health Sciences Cohort Explorer. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

### 7.5 Protecting User Accounts

WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. You can use the Administration Console to modify these options on the **Configuration > User Lockout** page.

As a system administrator, you have the option of turning off all the configuration options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks. For more details, refer to Configuring Security for a WebLogic Domain section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c Release 1 (12.1.1)*.

### 8 Protecting Data

Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it.

### 9 Setting Up Fine Grain Audit Policy

The TRC application has 3 different schemas:

- Schema for Cohort Data Mart (CDM)
- Schema for Omics Data Bank (ODB)
- Application schema used by the TRC application user interface

Oracle recommends that only the CDM and ODB schemas have audit policies. There is no need to log unwarranted access to the application schema. The package used to create each policy is the DBMS_FGA package. This package lets you create specific policies for each table. Oracle recommends that the policy names match each table name that is to be audited. This allows for simple identification of audit policies for each table. The audit policies must be defined for INSERT, DELETE, or UPDATE operations. If you plan to move PHI data in OHSCE Schema, then Oracle recommends that you have auditing enabled for **Select** operations. Also, the columns that are audited must be left **NULL** to audit all columns that are accessed. The default value for any column change must be left as is. The mode used to record information must be set to DB + extended or XML extended in order to log the exact SQL statement and bind variables. This is important to detect which data may is affected. Refer to the Oracle database documentation, for a detailed description of the DBMS_FGA package.

There are initialization parameters to specify where the audit logs are stored. Oracle recommends that the audit logs be stored in a separate tablespace and preferably on a
different disk so as to not interfere with other database operations which may need high throughput of the disks with real data. Information about parameters for audit log storage can also be found in the Oracle database documentation.

Oracle recommends that a general audit mode be set to audit each logon to the database as the actual DBA password could be compromised and you may want to disable audit policies. Setting up an audit policy to log all logon operations to the database is always a very good idea in production databases.

There is a list of tables in the ODB schema that do not need any audit policy. These tables are used as staging tables in order to move data to the final tables. All of these tables have _STG in the end of the name. No need to audit any of these tables.

Here is an example of the SQL to set up an audit policy:

```sql
begin
  DBMS_FGA.ADD_POLICY(
    object_schema=>'ODB',
    object_name=>'W_EHA_GENE',
    policy_name=>'W_EHA_GENE',
    enable=>true,
    statement_types=>'INSERT,UPDATE,DELETE'
  );
end;
```

For more information on setting up the audit policy, refer to Oracle data documentation at [http://www.oracle.com/pls/db112/homepage](http://www.oracle.com/pls/db112/homepage).

### 10 Documentation Accessibility


#### Access to Oracle Support
