Oracle® Life Sciences InForm

Security Guide

Release 7.0.1

F56801-01

August 2024

Oracle Life Sciences InForm Security Guide, Release 7.0.1

F56801-01

Contents

Preface

1 Security overview

2 Secure installation and configuration

3 Security features

4 Developement security overview

5 Top ten security risks

Preface

This preface contains the following sections:

- Documentation accessibility
- Diversity and Inclusion
- Related resources
- Access to Oracle Support
- Additional copyright information

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related resources

All documentation and other supporting materials are available on the Oracle Help Center.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through Oracle Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface Customer Support Portal (https://hsgbu.custhelp.com/)
- Japanese interface Customer Support Portal (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit https://www.oracle.com/life-sciences/support/ or visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab if you are hearing impaired.

Additional copyright information

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

1

Security overview

In this chapter:

Application security overview

To ensure security in the Oracle InForm application, carefully configure all system components, including the following third-party components:

- Web browsers
- Firewalls
- Load balancers
- Virtual Private Networks (VPNs)

General security principles

In this section:

Keep software up to date

Keep all software versions and patches up to date.

Keep up to date on the latest 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 the following months:

- January

- April
- July
- October

Oracle highly recommends that customers apply these patches as soon as they are released.

Follow 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. Oracle recommends reviewing user privileges periodically to determine relevance to current job responsibilities.

Before executing data definition language (DDL) scripts, create a database user with the specified limited set of privileges. Do not provide users with DBA access.

Require secure session practices

Users must observe the following rules:

- Run the Oracle InForm application in a single browser session.
- Run the Oracle InForm application in a single browser window.
- Log out of the Oracle InForm application and close the browser completely.

Scan files for viruses prior to uploading them to Oracle InForm

Make sure you have properly scanned all files for viruses prior to uploding them to Oracle InForm or its related applications. To that end, Oracle recommends the following process:

1. Train a limited number of users to perform a virus scan on all relevant files.
2. Grant upload permission to those users for a limited time.
3. Once the files have been uploaded, revoke the upload permission to those users.

Lock computers to protect data

Encourage users to lock computers that are left unattended. For more information, see Login security.

Provide only the necessary rights to perform an operation

Assign users to user types, assign rights to rights groups, and assign users to rights groups and groups so that they can perform only the tasks necessary for their jobs.

For more information, see:

- Users assigned to user types.
- Rights assigned to rights groups.
- Users assigned to rights groups.
- Users assigned to groups.

Design multiple layers of protection

When designing a secure deployment, design multiple layers of protection. For example, if someone were to gain unexpected access to a layer, such as the application server, the person should not automatically have access to other layers, such as the database server.

Providing multiple layers of protection might include the following activities:

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

web.config settings to secure Oracle InForm .NET projects

To prevent sensitive information from being released, customErrors in the web.config file must be turned off. This ensures that the stack trace of an error is not shown publicly.

```
<customErrors mode="On" />
```

The setting is RemoteOnly by default. If you customize web.config files, verify that the value is set to On or RemoteOnly before deploying it to production.

You can find the web.config file in <InForm_install_directory>/bin/aspmvc project.

Password security principles

In this section:

- Configure strong passwords on the database
- Require complex and secure passwords
- Keep passwords private and secure
- Configure your browser so that it doesn't remember or automatically fill passwords
- Change passwords periodically
- Configure updated database user passwords in Oracle InForm

Configure strong passwords on the database

Make sure all your passwords are strong passwords. Oracle recommends that you use a mix of uppercase and lowercase letters, numbers, and symbols.

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, see the *Oracle Database Security Guide* specific to the database release you are using.

You must modify the following passwords so that they comply with your password policies, such as a minimum length or character requirements:

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

Additionally, you should not configure a password for the database listener because a configured password enables remote administration. For more information, see Removing the Listener Password in the documentation for Oracle® Database Net Services Reference 12c Release.

For more information about configuring strong passwords, see the *Security Guide* for Oracle Database 12c Release.

Require complex and secure passwords

Each password should meet the following requirements:

- Contains a minimum of eight characters.
- Contains at least one upper case character, and at least one number or special character.
- Does not contain a common word, name, or any part of the user name.

For more information, see Configure strong user passwords.

Keep passwords private and secure

All users should change their passwords when they log in for the first time.

Tell users never to share passwords, write down passwords, or store passwords in files on their computers. For more information, see Passwords for new users.

Configure your browser so that it doesn't remember or automatically fill passwords

Make sure to configure the following settings for the browser you're using to access Oracle InForm.

Browser	Where to find the setting	Setting names	Set to
Chrome	1. Click **Settings**, and at the bottom of the page, click **Advanced**. 2. In the **Passwords and forms** section, click **Autofill settings**.	• Autofill settings—Enable Autofill to fill out forms in a single click • Manage passwords—Offer to save your web passwords	Off
Firefox	1. Click **Options**, then click **Security**.	Remember logins for sites	Disabled
Edge	1. Click **Settings**, and at the bottom of the page, click **Advanced**. 2. In the **Passwords and forms** section, click **Autofill settings**.	• Autofill settings—Enable Autofill to fill out forms in a single click • Manage passwords—Offer to save your web passwords	Off

Browser	Where to find the setting	Setting names	Set to
Safari	1. Click **File**, and select **Preferences**. 2. Select the **AutoFill** tab.	User names and passwords	Deselected

Change passwords periodically

It is good practice to change both system account passwords and user passwords periodically.

Follow your organization's operating procedures for the frequency of making changes.

Configure updated database user passwords in Oracle InForm

When database user passwords are soon to expire, they have to be changed and InForm needs to be updated with the new password information for each user. This section covers which Oracle InForm database users need to be configured and how to update their new password information.

> **Note:**
>
> The default expiration period for database user passwords is 180 days. This value can be changed through the INFORMPROFILE in the database by the database administrator.

For more information on how to change the database user passords, see the *Oracle InForm Installation Guide*.

- PFDBAdmin (sysdba)
- Oracle InForm admin DSN
- Trial schema
- Customer Defined Database (CDD)
- Randomization Database (RND)
- Oracle InForm Publisher Grantor
- Oracle InForm Adapter user

PFDBAdmin (sysdba)

1. Open a Command Prompt window.
2. To get the username for the PFDBADMIN (sysdba) user, run the follwing command:

```
REG QUERY HKLM\SOFTWARE\ORACLEHS\INFORM -v PFDBAUID
```

3. To update InForm with the new PFDBADMIN password, run the PFADMIN command:

   ```
   PFADMIN CONFIG SERVICE /SYSDBA
   ```

4. Enter the existing username and new password when prompted.

Oracle InForm admin DSN

1. Open a Command Prompt window.
2. To get the DSN, run the follwing command:

   ```
   REG QUERY HKLM\SOFTWARE\ORACLEHS\INFORM -V DSN
   ```

3. To tet the admin schema username, run the following command:

   ```
   REG QUERY HKLM\SOFTWARE\ORACLEHS\INFORM -V UID
   ```

4. To update InForm with a new admin DSN password, run the PFADMIN command:

   ```
   PFADMIN CONFIG SERVICE /ADMINDSN <admindsn>
   ```

5. Enter the existing username and new password when prompted.

Trial schema

1. Open a Command Prompt window.
2. To get the trial schema's username and DSN, run the follwing command:

   ```
   PFADMIN VIEW TRIAL <trialname>
   ```

   The **Trial UID:** value is the trial schema's username.

   The **Trial DSN:** value is the trials DSN.
3. To update Oracle InForm with a new trial schema password, run the PFADMIN command:

   ```
   PFADMIN CONFIG TRIAL <trialname> /TRIDSN <trial dsn>
   ```

4. Enter the existing username and new password when prompted.

> **Note:**
>
> To update Oracle InForm Adapter with the new trial schema password, re-register the trial with Oracle InForm Adapter. For more information, see the *Oracle InForm Installation Guide*.

Customer Defined Database (CDD)

1. Open a Command Prompt window.

2. To update Oracle InForm with a new CDD schema password, run the PFADMIN command:

   ```
   PFADMIN CONFIG CDD <trialname> <cdd-dsn>
   ```

3. Enter the existing username and new password when prompted.

Randomization Database (RND)

1. Open a Command Prompt window.
2. To determine the Randomization Database DSN (rnddsn) and username, run the PFADMIN command:

   ```
   PFADMIN VIEW TRIAL <trialname>
   ```

   The **Rnd DSN:** value is the Randomization Databases DSN.

   The **Rnd UID:** value is the Randomization Databases Username.
3. To update Oracle InForm with a new Randomization Database schema password, run the PFADMIN command:

   ```
   PFADMIN CONFIG TRIAL <trialname> /RNDDSN <rnddsn>
   ```

4. Enter the existing username and new password when prompted.

Oracle InForm Publisher Grantor

1. Open a Command Prompt window.
2. To determine the Oracle InForm Publisher Queue Grantor Username (grantoruser), run the PUBLISHERADMIN command:

   ```
   \ORACLEHS\INFORMPUBLISHER\BIN\PUBLISHERADMIN GRANTOR SHOW <tnsname>
   ```

   This will show the name of the queue grantor user that is set, if one is configured for the Oracle InForm installation.
3. To update Oracle InForm with a new Publisher Queue Grantor User password, run the PUBLISHERADMIN command:

   ```
   \ORACLEHS\INFORMPUBLISHER\BIN\PUBLISHERADMIN GRANTOR UPDATE <tnsname>
   <grantoruser>
   ```

4. Enter the existing username and new password when prompted.

Oracle InForm Adapter user

To update Oracle InForm with a new Oracle InForm Adapter schema user, re-run the Oracle InForm Adapter Service Configuration. For more information, see the *Oracle InForm Installation Guide*.

2 Secure installation and configuration

In this chapter:

- Installation overview
- Post-installation configuration

Installation overview

Use the information in this chapter to ensure the Oracle InForm application is installed and configured securely. For information about installing and configuring the Oracle InForm application, see the *Installation Guide*.

- Transport Layer Security (TLS)
- Secure cookies
- Add HTTP Strict-Transport-Security (HSTS) headers
- Signing authorizations
- Install only the Oracle InForm features needed
- About entering passwords
- Configure strong administrator passwords
- Close all unused ports
- Disable all unused services
- Disable unnecessary services provided by the operating system for Oracle InForm Publisher
- Revoke unnecessary grants for Oracle InForm Publisher
- Restrict network access to critical services for Oracle InForm Adapter
- Secure Socket Layer (SSL) for Oracle InForm Adapter
- Installation username and password for Oracle InForm Adapter
- Close all unused ports and open necessary ports for Oracle InForm Adapter
- Disable all unused Windows services for Oracle InForm Adapter
- Restrict access to the Register Trial tool for Oracle InForm Adapter

Transport Layer Security (TLS)

Configure your environment so that the Oracle InForm application servers are hosted behind a firewall and all communication through the firewall is over HTTPS.

TLS version 1.2 or higher is required, as versions 1.1 and below have been found to be vulnerable.

Secure cookies

If HTTPS is enabled for communication between the Oracle InForm and Cognos Analytics 11 Reporting applications, for additional security, Oracle recommends that you secure Cognos cookies.

For more information, see the Cognos documentation.

If you are using a TLS termination device between the Oracle InForm clients and the Oracle InForm application server, set up rules on the TLS termination device to add the secure flag for the necessary cookies.

Add HTTP Strict-Transport-Security (HSTS) headers

The HTTP Strict-Transport-Security response header (HSTS) is a security configuration that notifies web browsers that the site should only be accessed using HTTPS. Also, any future attempts to access said site using HTTP is automatically converted to HTTPS.

To add HTTP HSTS headers:

1. Open a command prompt.
2. Run the following command:

   ```
   appcmd.exe set config /section:httpProtocol
         /+customHeaders.["name='Strict-Transport-Security',value='max-
   age=2592000; includeSubDomains'
         "] /commit:apphost
   ```

3. Perform IIS reset.

Signing authorizations

Signing web service authorizations and deployment packages is required for integration with the Central Designer application. You must install the certificates used for signing on all application servers before you deploy a Central Designer deployment package.

For instructions for installing the certificate used for signing, see the *Installation Guide*.

- Use digital certificates issued by Certificate Authorities

Use digital certificates issued by Certificate Authorities

A Certificate Authority (CA) assures users that the server information has been verified by a trusted source.

Oracle recommends that you use digital certificates that are issued by a Certificate Authority, and that do the following:

- Verify the server and domain.
- Use 256-bit encryption.
- Include a $1 million per year warranty.

Install only the Oracle InForm features needed

To enhance security, the Oracle InForm installer allows you to select the features to install.

- Complete—Recommended option. This option installs:
  - Oracle InForm core, including the Oracle InForm Adapter, Oracle InForm Publisher, and Oracle InForm Portal features, as well as Reporting Configuration.
  - Required utilities.
  - All Oracle InForm utilities.
  - Documentation.
    For the Complete option, all the utilities are installed. You cannot select specific utilities to install.
  - Custom—Installs Oracle InForm with all of its components, required utilities, and documentation, but allows you to opt out of installing Reporting Configuration.

> **Note:**
>
> Oracle recommends locking down any Oracle InForm utilities and restrict access to the server hosting them.

About entering passwords

The Oracle InForm software and installation scripts do not contain default or hard-coded passwords. You must supply passwords for predefined users, such as the Windows OS user and Oracle database users.

Installation scripts prompt for passwords on the command line or allow a file containing the passwords to be passed in as parameters. For more information, see the *Installation Guide*.

> **Note:**
>
> If you use password parameter files, delete the files after installation.

Configure strong administrator passwords

When you install the Oracle InForm application, the following database administrator users are created:

- **Oracle InForm Admin**—PFADMIN.
- **Streams Admin**—strmadmin.
- **Reporting Admin**—rptinstall.
- **PFCapAdmin**—Unique name set by the customer.
- **Content Store**—Unique name set by the customer.

When you configure the Oracle Directory Server for the Reporting and Analysis module, you create the Cognos System Admin user.

Ensure that all passwords for these users are strong passwords.

Close all unused ports

Keep only the minimum number of ports open. Close all ports not in use.

The Oracle InForm application defaults to the following ports, but can be configured to use non-standard ports.

- **Port 1521**—Default connection to the Oracle Database.
- **Port 80**—For the client connection (HTTP).
- **Port 443**—For the client connection (HTTPS).
- **Port 389**—For connection to the Oracle Directory Server for reporting.

The Oracle InForm application does not require both Port 80 and Port 443. However, you must configure the Oracle InForm application to use either HTTP or HTTPS.

The ports used by the following web services should also be kept open at all times:

- AuthService
- ODMSubmitService
- DeploymentService

These port numbers are configurable and have no default values.

Disable all unused services

Disable all unused services. The Oracle InForm application uses the following services:

- Oracle InForm Service.
- IBM Cognos Analytics.
- COM+ System Application.
- Distributed Transaction Coordinator.
- DNS Client.
- IIS Admin Service.
- Oracle MTS Recovery Service.
- World Wide Web Publishing Service.

Disable unnecessary services provided by the operating system for Oracle InForm Publisher

The Oracle InForm Publisher feature does not use the following services:

- 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.

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, upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

Revoke unnecessary grants for Oracle InForm Publisher

For security purposes, you must revoke all unnecessary grants on the schema. You must have DBA privileges to perform this action.

Restrict network access to critical services for Oracle InForm Adapter

Set up a firewall between the internet and an isolated server, and between the isolated server and the intranet. This configuration creates a demilitarized zone (DMZ), which blocks any illegal traffic and contains intrusions.

Keep the Oracle InForm Adapter server behind a firewall to provide assurance that access is restricted to a known network route that can be monitored and restricted, if necessary. As an alternative, a firewall router can substitute for multiple, independent firewalls.

Secure Socket Layer (SSL) for Oracle InForm Adapter

Configure your environment so that the Oracle InForm Adapter feature server is hosted behind a firewall with an appliance such as an F5 load balancer for handling HTTPS and converting to HTTP.

The Oracle InForm web services allow for SSL setup so data that is transported between the client and web services is encrypted (if the Oracle InForm Adapter feature server is not behind an F5 and is accessed directly).

Clients calling the Oracle InForm web service should be configured to send data over SSL using TLS 1.2.

Depending on the client applications you are running, secure the corresponding web services as follows:

- If you are using CIS, secure the Transaction Adapter and Central Admin web services by running WebConfigFileSelector F5Cert. For this, you must upload an X.509 digital certificate from the CIS system to the personal certificate store on the Oracle InForm Adapter machine.
- If you are using Central Coding, secure the Adapter Admin WCF web service by running WebConfigFileSelector F5Cert. For this, you must upload an X.509 digital certificate from the Central Coding system to the personal certificate store on the Oracle InForm Adapter machine.
  You can also secure the Coding and Enhanced Discrepancy web services using digital certificates as described above or you can configure them to use username/password authentication over HTTPS by running WebConfigFileSelector F5. For this, the authentication user account must be active in the Oracle InForm study and the username and password must be stored in the Central Coding system. Change passwords on a regular basis to ensure security.
- If you are using ODM, secure the ODM web service by running WebConfigFileSelector F5Cert. For this, you must upload an X509 digital certificate from your ODM client application to the personal certificate store on the Oracle InForm Adapter application server.

Follow the best practices for configuring IIS. For more information, see the documentation available on the Microsoft TechNet website.

Installation username and password for Oracle InForm Adapter

During configuration of the Oracle InForm Adapter feature, you are prompted for a database username and password. Make sure the username and password that you provide follow these guidelines:

- Contain a minimum of eight characters.
- Include at least one number.
- Contain a combination of upper and lowercase characters.
- Do not contain repeating words or characters.

Close all unused ports and open necessary ports for Oracle InForm Adapter

Keep open only the minimum number of ports needed. Close all ports not in use. Follow best practices for unused and necessary ports.

Disable all unused Windows services for Oracle InForm Adapter

Disable all unused Windows services.

Restrict access to the Register Trial tool for Oracle InForm Adapter

The Register Trial Tool is a command line tool that you use to register a study, register a server adapter, decommission a study in the Oracle InForm Adapter feature, and view lists of existing studies, server adapters, and decommissioned studies.

This tool is provided with the <if> installation. Restrict access to only those individuals who need to use this tool.

Post-installation configuration

In this section:

- Restrict access to Oracle InForm server machines
- Restrict access control for Oracle InForm Adapter
- Restrict access to the file server for Oracle InForm Publisher
- Configure strong user passwords
- Configure rights and rights groups
- Review administrative configurations periodically
- Configure the pfreportinguser account
- Change the pfuser password as required
- Change the PFCapAdmin password as required

Restrict access to Oracle InForm server machines

Allow only administrator and system accounts access to the Oracle InForm server machine.

Limit the number of users with access to the server machine. Disable or delete any unnecessary users.

Restrict access control for Oracle InForm Adapter

Limit the number of users who have access to the following items, which contain critical information:

- Configuration files.
- Application paths and directories.
- Assembly files (DLLs).
- The registry.

These items should have the most restrictive access control possible.

The Oracle InForm Adapter feature does not write any temporary files during Oracle InForm installation. Therefore, after installation is complete the directories can be made read-only.

Restrict access to the file server for Oracle InForm Publisher

The Oracle InForm Publisher feature can be configured to write files to a remote file server using secure file transfer protocol. Allow only administrator and system accounts access to the file server.

Limit the number of users with access to the server machine. Disable or delete any unnecessary users.

Configure strong user passwords

Configure password options to require a secure level of complexity. For example, a minimum required password length of eight characters requires users to create more secure and complex passwords than a minimum required password length of six characters.

For more information, see Password configuration for user security.

Configure rights and rights groups

Assign users to user types, assign rights to rights groups, and assign users to rights groups and groups, so that users can perform only the tasks necessary for their jobs.

For more information, see:

- Users assigned to user types.
- Rights assigned to rights groups.
- Users assigned to rights groups.
- Users assigned to groups.

Review administrative configurations periodically

Periodically review administrative configurations and implement best practices for two sets of eyes when making any administrative configuration updates.

Due to its high risk nature, the administrative role may cause risky transactions for all customers and should be validated by a second set of eyes and verified after implementing or making updates.

Configure the pfreportinguser account

The Oracle InForm application includes a user named pfreportinguser, which is used to perform certain functions for the Reporting and Analysis module, including running pfrinit and the model updater service. If the password for this user expires, clinical data in the Reporting and Analysis module is not updated and becomes out of date.

To ensure that the data in the Reporting and Analysis module remains current, a user with administrative rights must do the following:

1. Reset the password for the pfreportinguser account before it expires.

   > **Note:**
   >
   > The amount of time before a password expires is configured in the Password Expiration Period field on the System Configuration page in the Oracle InForm Admin user interface. The recommended setting is 90 days.

2. Run the following pfadmin command to propagate the password change to the Reporting and Analysis database:

   ```
   PFADMIN SETSERVER PFREPORTINGUSERPW <studyname>
   ```

   You supply the new password in a parameter file or in response to a command line prompt.

For more information, see the *Installation Guide*.

Change the pfuser password as required

pfuser is a local user created during installation to run the Oracle InForm service and all Oracle InForm processes. This user account can be assigned any name; by default, it is pfuser_<machine name>.

Change the pfuser password as required by your operating procedures. To change the password:

- Run pfadmin
- Update IIS with the new pfuser password
- Update COM+ applications with the new password

Run pfadmin

The following pfadmin command resets the pfuser account password in the Oracle InForm registry and the Windows account:

```
PFADMIN CONFIG SERVICE /PFUSER
```

You supply the new password in a parameter file or in response to a command line prompt.

> **Note:**
>
> You must use the same password when you update IIS. For more information, see Update IIS with the new pfuser password.

Update IIS with the new pfuser password

When you change the pfuser password, you must manually update the value in IIS.

1. Select **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand the tree until you see the children of Default Web Site.
3. Select a study listed under Default Web Site.
4. Double-click **Authentication** in the center panel, select **Anonymous Authentication**, and then click **Edit** in the Actions panel on the right.
5. Copy the user name in the **Specific user** field, and then click **Set**.

   The Set Credentials dialog box appears.
6. Paste the user name you copied into the User name field, and enter the new password in the password fields.

   > **Note:**
   >
   > The new password should be the same as the password that was entered when pfadmin config service/pfuser was run. For more information, see Run pfadmin.
7. Expand the study tree of the study that you selected in step 3.
8. For each child node listed under the study, repeat steps 4 to 6 to update the password.
9. Repeat steps 3 to 8 for:
   - Each study listed under Default Web Site.
   - The Schema virtual directory listed under Default Web Site.
   - The System virtual directory listed under Default Web Site.

Update COM+ applications with the new password

When you change the pfuser password, you must manually update the value in all the COM+ applications for the study.

1. Select **Start** > **Administrative Tools** > **Component Services**.
2. Expand **Component Services** > **Computers** > **My Computer**.
3. Select **COM+ Applications**.
4. In the middle panel, right-click any COM+ application, and then select **View** > **Details**.

   The middle panel changes to a detailed display.
5. Right-click **InFormDisp**, and select **Properties**.
6. Select the **Identity** tab.

7. Enter the new password in the password fields.
8. Click **Apply**, and then click **OK**.
9. Repeat steps 5 to 8 for each additional COM+ application.

Change the PFCapAdmin password as required

Change the PFCapAdmin password as required by your operating procedures. You change the password by updating the MotioCAP_informcap.properties file. For more information, see the *Installation Guide*.

3

Security features

In this chapter:

In this chapter

In this section:

Password configuration for user security

An administrator can define the following formatting, entry, and reuse requirements for passwords directly in theOracle InForm application on the System Configuration page. For the recommended settings, see General security principles and the *User Guide for Administrators*.

- Minimum length of the password. Recommended setting is 8 characters.
- Whether the password must include a number. Recommended setting is Yes.
- Whether the password must include an upper-case letter. Recommended setting is Yes.
- Whether the password must include a nonalphanumeric character. Recommended setting is Yes.
  Valid non-alphanumeric characters correspond to ASCII codes in the following ranges:
  - 33-47
  - 58-64
  - 91-96
  - 123-126
- Whether the password can be reused. Recommended setting is No.

- Number of consecutive failed login attempts allowed. Recommended setting is 3.
- Whether password recovery is enabled. Recommended setting is Yes.
- Number of days before the password expires. Recommended setting is 90 days.

Passwords for new users

When you create a new user, you supply a user name and password. Users must change their passwords the first time they log in.

Login security

Oracle InForm requires users to authenticate by logging in with a unique user name and password. You can use the following authentication methods:

- **Local**—User information stored in the Oracle InForm application is used for authentication.
- **Single Sign-On (SSO)**—For studies hosted by Oracle, user information stored in Oracle® Identity and Access Management Services (IAMS) is used for authentication.

Users must enter their user names and passwords to log in. The application does not allow duplicate user names.

If either a user name or password is incorrect, an error message appears, but does not tell the user which value is incorrect. Therefore, if someone else is using the account to attempt to log in, the message does not confirm either a user name or password.

No data loss after a session transaction

Studies are configured to require users to re-enter their user names and passwords after a defined period of inactivity. The user can log in and continue working on a form without losing data.

This security feature is controlled by the following settings on the System Configuration page:

- **Re-authentication inactivity period**—Number of minutes of inactivity that can pass before the Oracle InForm application requires a user to log in again.
- **Re-identification period**—Number of minutes that a session can be active before the Oracle InForm application requires a user to log in again.

Select values for these settings that work with your study protocol.

Automatically inactivated user accounts

Studies are configured to allow a defined number of attempts to log in correctly. When a user exceeds the number of allowed login attempts, which is defined on the System Configuration page, the user account is inactivated and the user cannot log in.

Only a user with the appropriate rights can activate an automatically inactivated account. Relevant rights include:

- Activate Site User
- Deactivate Site User
- Activate Sponsor User
- Deactivate Sponsor User

Restricted access to the application

You can restrict access to the application in the following ways:

- Terminate a user.
  Typically, you terminate users who leave the organization. Terminated users cannot log in. All users, including terminated users, remain in the study for audit purposes. Terminated users can be reinstated and then activated.
- Inactivate a user.
  Typically, a user is automatically inactivated when the user fails to log in after the number of attempts set on the System Configuration page. After the user account is inactivated, only an administrator can manually reactivate the user. The user must be reactivated before the user can work in the application.

Application security features

In this section:

Users assigned to user types

You can assign users to user types. The following user types are available:

- **Site user (default)**—User who performs site functions, such as data entry.
- **Sponsor user**—User who performs study functions, such as reviewing and verifying clinical data.

Rights assigned to rights groups

A right is the permission to perform a specific activity. A rights group is a collection of rights.

Rights grant access to different parts of the application. Entire parts of the application are hidden when users do not have the rights to work in those areas.

When a new user is created in the Oracle InForm application, an administrator with the right to modify user information assigns the user to a rights group, providing the user permissions to perform specific study activities.

For example, a user can be assigned to a rights group with the appropriate rights to screen and enroll subjects. The individual Enroll Subjects right is static, but the group of rights assigned to the rights group is configurable.

A user can be a member of only one rights group.

For more information, see the *User Guide for Administrators*.

Users assigned to rights groups

The following predefined rights groups are provided with the Oracle InForm software. The rights groups contain the default set of rights that are normally associated with that rights group, but they do not contain any users.

- AutoQuery RG
- Deployment RG
- Oracle InForm Server Group
- Integration RG
- PFArchUser Rights Group
- Reports Only Rights Group
- System Creator Group
- User Activator RG
- User Manager RG

After you review the rights that are assigned to rights groups and make any necessary changes, you can assign users to rights groups. A user assigned to a rights group has the rights that are granted to that rights group. Changes to a rights group are immediately applied to all users assigned to the rights group.

Users assigned to groups

Groups allow you to associate users who have similar roles in a study and to allow them access to specific areas ofOracle InForm functionality. Groups provide an advanced level of authorization. In order to perform certain activities, a user must have rights to perform the activities and also be in a group for which the activities are authorized.

The Oracle InForm application allows you to define and maintain different types of groups. Users can sign forms, enter queries, and access the Reporting and Analysis module if they are assigned to the corresponding groups and have the appropriate rights. For more information, see the *User Guide for Administrators*.

Users assigned to sites

Users can view subject and visit information only for the sites to which they are assigned. Users must also be assigned to rights groups that grant them access to this information.

Display overrides

Display overrides allow you to refine user access to individual data items on forms. For a particular rights group, you can specify whether the group of items that make up an item group is Hidden, Editable, or Read-Only. This designation overrides the rights conveyed by membership in the rights group and also overrides the display properties of the items in the group. This additional level of security allows you to give users with the same set of rights different access to specific items.

For more information, see the *User Guide for Administrators*.

To create item definition display overrides, use the Oracle Central Designer application.

Changed Cognos user groups

The rights for the following Cognos user groups have been changed to limit the ability of users to create user-defined HTML and user-defined SQL:

- Directory Administrators group:
  - Can view Groups and Roles, but cannot view the Capabilities.
    The ability to make any changes to Cognos Capabilities and Cognos Groups and Roles have been removed from this group.
  - Can accept only Oracle InForm Support user types.
    Sponsor or Site users can no longer be added to this group.
- Server Administrators group:
  - Can accept only Oracle InForm Support user types.
    Sponsor or Site users can no longer be added to this group.
- Authors group:
  - In Report Studio—Authors can create, edit, or run reports that use clinical or operational model packages.
    Authors cannot create, edit, or run reports that contain custom HTML and/or custom SQL.
  - In Cognos Connection—Authors can run reports that use clinical or operational model packages.
    Authors cannot run reports that contain custom HTML and/or custom SQL.

For more information, see the *Installation Guide*.

Data security features

In this section:

Restricted viewing of Protected Health Information

You can configure the Oracle InForm Publisher feature to write clinical data that might contain protected health information (PHI) to a local directory or remote file server. For example, ODM extract files might contain PHI. You must restrict access to these locations to an administrator or system users.

Audit trails for data security

Audit trails record updates to the following information:

- Subject information
- Data on forms
- Queries

- Signatures

Audit trails are comprehensive records that include the person who made the change, the date and time of the change, the change itself, as well as additional details. You cannot modify data in an audit trail.

For more information, see the *User Guide for Site Users*.

Freezing and locking data

You can freeze or unfreeze data on the subject, visit, and form levels. Freezing prevents changes in data—either temporarily during a study, or permanently at the end of a study.

- Freezing a subject freezes all visits, forms, and items for that subject.
- Freezing a visit freezes all forms and items within the visit.

After a subject, visit, or form is frozen, you cannot update the data, but you can issue manual queries for items. If a repeating form is frozen, no new instances of the repeating form can be added to a visit.

> **Note:**
>
> If an update is made to a frozen item when someone responds to a manual query, the item maintains its frozen status to prevent additional updates to the item aside from query generation.

To prevent any further modification to data, you can also lock a subject, visit, or form.

Considerations for using email

In this section

- Considerations for configuring email notifications
- Considerations for using automated emails for gathering subject data
- Considerations for sending reports by email from the Cognos software

Considerations for configuring email notifications

Although the Oracle InForm application can be configured to send emails from the trial server, the emails are not able to be encrypted. Customers must consider this fact when designing email notifications, and should not include any data in an email that is required to be encrypted.

Considerations for using automated emails for gathering subject data

Automated emails should not be the sole method of gathering important subject information. Proactive monitoring of subject information is required.

Considerations for sending reports by email from the Cognos software

The send report by email feature available in Cognos Analytics 11 for self-hosted Oracle InForm studies offers the option to attach copies of reports to emails. If you configure your

Cognos environment to send emails, users must be instructed to never select the option to attach reports to emails.

web.config settings to secure Oracle InForm .NET projects

To prevent sensitive information from being released, customErrors in the web.config file must be turned off. This ensures that the stack trace of an error is not shown publicly.

```
<customErrors mode="On" />
```

The setting is RemoteOnly by default. If you customize web.config files, verify that the value is set to On or RemoteOnly before deploying it to production.

You can find the web.config file in <InForm_install_directory>/bin/aspmvc project.

web.config settings that secure the Oracle InForm Adapter web services

Settings in the web.config file control various aspects of the use of Oracle InForm Adapter interfaces. These settings are determined by the behavior you want to control.

By default, these settings are off (disabled). When developing your client, you might want to enable certain settings for testing purposes. However, before deploying your client to production, be sure to disable the settings to ensure web services are secure.

Settings in the web.config file affect the following:

- Access to metadata.
  Metadata that is output by Oracle InForm Adapter interfaces can be used as input to client programs that you build. Settings in the web.config file control whether metadata is output by an interface, and whether client programs have access to this metadata.
- The amount of detail provided in exceptions.
  For more information, see WCF—Turn off includeExceptionsDetailsInFaults attribute.
- User authentication against the Oracle InForm release.
- WCF—Enabling and disabling metadata
- WCF—Turn off includeExceptionsDetailsInFaults attribute

WCF—Enabling and disabling metadata

By default WCF services do not publish the metadata. If you want the configuration to allow access to the metadata through the use of import tools such as **svcUtil.exe** to generate the client code, you must explicitly set the following in the web.config file:

```
<serviceBehaviors>
                 <behavior name="DiscrepancyServiceBehavior">
                           <serviceMetadata httpGetEnabled="true" />
                           <serviceDebug
includeExceptionDetailInFaults="true" />
                 </behavior>
```

After successfully developing and deploying the client, set the values to false, which prevents unwanted clients from generating proxy files or looking at potentially sensitive information.

```
<serviceBehaviors>
                  <behavior name="DiscrepancyServiceBehavior">
                            <serviceMetadata httpGetEnabled="false" />
                            <serviceDebug
includeExceptionDetailInFaults="false" />
                  </behavior>
```

If you do not need to publish metadata, leave the setting turned off.

WCF—Turn off includeExceptionsDetailsInFaults attribute

Make sure that the includeExceptionsDetailsInFaults attribute is turned off (set to False) for all the behaviors. This attribute should be turned on (set to True) for debugging purposes only.

```
<serviceDebug includeExceptionDetailInFaults="False" />
```

Configure user authentication for applicable web services

For WCF interfaces, run WebConfigFileSelector.cmd to enable user authentication.

For more information, see the *Installation Guide*.

Restricted viewing of Protected Health Information

You can configure the Oracle InForm Publisher feature to write clinical data that might contain protected health information (PHI) to a local directory or remote file server. For example, ODM extract files might contain PHI. You must restrict access to these locations to an administrator or system users.

4

Developement security overview

In this chapter:

OWASP top ten security vulnerabilities 2021

To guide developers for what they need to protect against, the Open Web Application Security Project publishes an annual document that lists the ten most critical security vulnerabilities identified for a year. Addressing the ten security vulnerabilities does not provide for total security, but is a good start in raising awareness to the current major security threats. This document explains how the Clinical Data API and API developers should address security vulnerabilities and risks documented by OWASP for 2021.

This document identifies the controls within the Clinical Data API that are used or may be used to address the associated risks. In some cases, the controls are baked into the product and proper use of the controls by the clients must be used to validate the integrity of the controls.

Security awareness and education

The best application security money can buy is education. Developers and project leads need to be mindful of security issues and have an understanding of secure coding practices. Training must include an in depth explanation of the potential risks as well as features of the development and deployment platforms that help mitigate exploits.

The most important design principle for application security is to implement security by design and default. Secure coding guidelines should be made available, adhered to, and enforced in all development organizations, irrespective of the tools and platforms being used.

A good example for security by default is the expectation that we all have for how elevators behave in case of a power outage. Instead of releasing the breaks, we expect elevators to apply the breaks for the safety of passengers in the cabin. But how would the elevator know that it should apply the brakes if no one defined this as the default behavior? So before thinking about how to prevent external attacks, it makes sense to identify secure defaults for an application to protect it from the inside. This however does not work well without training and awareness.

The risk associated with build your own

It is not always that developers immediately find the security they need for an application within the security toolset provided by a platform or built into a framework. As a result, *build your own* *security* is not uncommon among development projects. This is especially true if the application is a replacement of an existing system that uses a specific non-standard security infrastructure. An example for this is database-table-based authentication and authorization in combination with user provisioning and resource granting at runtime.

The risk associated with building your own security is that you are also on your own when it comes to quality assurance of the security layer, application security propagation, and single sign on, and you are responsible for bug fixing and maintenance of the security layer.

Not all developers are security experts, but experts are what it takes to build a custom security layer.

Time spent investigating existing, well-vetted security solutions is probably time well spent. Existing solutions can be applied to custom applications more easily and more cost effectively than creating an error-prone, self-written mechanism.

Other aspects of security

Application security is useless if the application itself runs in an insecure environment. Perimeter security describes the levels of protection that are added on servers, the network, and other data access channels outside of the API domain. As can be seen in this document, not all of the OWASP top ten security vulnerabilities documented for 2021 are relevant for application developers for specific implementations.

Disclaimer

This guide discusses the security options and features available in the Oracle InForm Clinical Data API that help mitigate security risks published in the OWASP Top 10 list of security vulnerabilities for the year 2021.

The set of recommendations in this guide is not exhaustive and no guarantee is given that implementing all the suggestions in this guide provides sufficient protection for all security threats listed in the OWASP Top 10. The reason for this disclaimer is that you cannot delegate responsibility for secure application development to a 3rd party or a single document. This guide is to help developers that know security to identify tools and features in the Oracle InForm Clinical Data API that they can use to implement application security. This guide does not replace a formal code review process and secure development practice.

Secure development for the Oracle InForm Adapter

In this section:

- Overview of Oracle InForm Adapter secure development
- Transport layer protection
- Web service authentication
- SQL injection
- XML injection
- Secure misconfiguration

Overview of Oracle InForm Adapter secure development

The *Secure Development Guide* provides an overview of the security options provided with the Oracle InForm Adapter feature that help mitigate some of the common security risks. The recommendations in this document are not exhaustive and there is no guarantee that implementing all the suggestions provides sufficient protection for all security threats, as you cannot delegate responsibility for secure application development to a third party or a single document. This document is to help developers who know the security tools and features that they can use to implement application security. This document does not replace a formal code review process.

The Oracle InForm Adapter feature provides the following web services that can be called by client applications:

- ODM interface
- Discrepancy interface

Transport layer protection

If your client is calling Oracle InForm Adapter web services that are hosted by Oracle, you must use Transport Layer Security (TLS) 1.1 or above to avoid man-in-the-middle attacks. In general, it is more secure to use TLS 1.2 for any client calling the Oracle InForm Adapter web services. Web client developers should enforce encrypted data transport when the application transports sensitive data and should validate that all certificates are legitimate and signed by public authorities.

Ciphers should be restricted to modern implementations.

Web service authentication

To address web service client authentication attacks, the Oracle InForm Adapter software supports username token and X.509 client certificate authentication. To ensure the integrity of web client authentication, the proper handling of the authentication artifacts should be followed.

The ODM and Discrepancy interfaces support username token authentication. Refer to the *Interfaces Guide* for information on how to invoke the ODM and Discrepancy web services using username token authentication. Make sure you refer to the correct section for the interface you are calling from your client.

To ensure that the web client authentication is secure, the password for the username token should be treated with the utmost care, as password exposure can compromise the authentication mechanisms. The Oracle InForm Adapter software does not store the password in clear-text on the file system and does not log the password. As such, the client web service password should be protected in the same fashion. The password should always be stored in an encrypted form. To reduce password exposure during password exchange, do not transfer the password through unencrypted side channels between web service endpoint parties. The authentication of each side channel endpoint is also a concern during the password exchange and is open to social engineering attacks if not done properly.

The Discrepancy and ODM Export interfaces also support X.509 certificate authentication. The client application must sign the message with the X.509 private certificate and the public X.509 certificate must be installed on the Oracle InForm Adapter application server. The X.509 Certificate Authentication is based on the signature generated from SHA256 signature algorithm. For the X.509 certificate authentication, a trusted public certification authority (CA) should be used to validate the legitimacy of the organization controlling the web service client endpoint. The use of a trusted public CA reduces the chances of social engineering attacks based on username token password handling. Public CAs provide different levels of organization checks, depending on the costs of their services. More organization checks ensure fewer chances of a social engineering attack.

For examples on how to sign the message with an X.509 certificate, see the ODM Sampler's source code: SignXml method in \certificate\MyClientMessageInspector.cs.

SQL injection

SQL injection issues occur when an SQL query is built using input from an untrusted source. This could allow an attacker to modify an SQL statement or to execute dangerous SQL commands.

The Oracle InForm Adapter interface web service uses bind variables and does not dynamically generate SQL, which makes SQL injection impossible.

XML injection

XML injection issues occur when the data used to construct XML code, which may contain XML metacharacters, is not encoded properly. The Oracle InForm Adapter software handles this by using standard XML processing components that construct the XML documents. It is recommended that the client code also uses standard XML processing components to ensure that data is properly encoded. If XML is constructed manually, the developer should ensure that any untrusted data is properly encoded to prevent XML injection.

Secure misconfiguration

Ensure the product API is locked down appropriately.

5

Top ten security risks

In this chapter:

- Overview of the OWASP top ten list

Overview of the OWASP top ten list

The list of the top OWASP ten web application security issues reflects a global consensus among many security experts. These security risks are likely the most serious ones that developers of applications need to be aware of and guard against. The OWASP most critical security weaknesses for 2021 are highlighted in this section.

For more information, see the following:

- OWASP home page: https://www.owasp.org/
- General descriptions for the OWASP top ten list of security risks for 2021: https://owasp.org/Top10/A00_2021_Introduction/
- The OWASP Top Ten Proactive Controls describes the most important control and control categories: https://www.owasp.org/www-project-proactive-controls/
- #1 - Broken access control
- #2 - Cryptographic failures
- #3 - Injection
- #4 - Insecure design
- #5 - Security misconfiguration
- #6 - Vulnerable and Outdated Components
- #7 - Identification and authentication failures
- #8 - Software and data integrity failures
- #9 - Security Logging and Monitoring Failures
- #10 - Server-Side Request Forgery (SSRF)

#1 - Broken access control

When a developer exposes a reference to an object without proper access or other protection, then this reference becomes a source of attack. The objects defined in the Clinical Data API have been tested to validate proper authorization constructs within the functions of the defined service. When developing code and sending data to and from the API, ensure that the authorization model of the API interface is consistent to guard against insecure direction object references.

The defense in depth design pattern specifies that multiple layers of security must be implemented in an application. This also means that application functionality that executes methods and operations should be guarded by authorization checks even if the underlying data object is protected through entity security. When the client application calls out to the Clinical Data API to submit the data, such calls should be protected with the level of the access control. As a best practice, never assume that a specific method will only be called within the context that it was initially designed for. All access to functionality that manipulates data must be protected either by access control on the entity or by guarding the invocation of methods with the appropriate permission checks. The credential of the identity associated with the access control in the client application must be encrypted and stored in the secured identity management system as the API does.

#2 - Cryptographic failures

Not all data is public and caution should be used to hide sensitive information from unauthorized users. Failure in security configuration and the selection of insecure defaults may pose a of risk data leakage.

Developers should use TLS 1.2 or above to consume the Clinical Data API to ensure the protection of the sensitive data and address Man-in-the-Middle attacks. Web client developers should enforce encrypted data transport when the application transports sensitive data and should validate that all certificates are legitimate and signed by public authorities. Ciphers should be restricted to modern implementations.

#3 - Injection

Injection vulnerabilities occur when data is sent into an interpreter via an interface specification and the party submitting the data does not perform checks on the data to ensure only the expected actions are performed by the interpreter on the data. SQL, Code, Command, Log, Path Transversal (XML) are all possible types of injection based upon the interpreter used in the container.

- Valid content types
- SQL injection
- XML injection

Valid content types

The Clinical Data API is a web service based on SOAP over HTTP. Developers must use *application/soap+xml* as MIME types in the Content-Type HTTP headers. Otherwise, the API rejects the requests.

SQL injection

SQL injection issues occur when an SQL query is built using input from an untrusted source. This could allow an attacker to modify an SQL statement or to execute dangerous SQL commands.

The Oracle InForm Adapter interface web service uses bind variables and does not dynamically generate SQL, which makes SQL injection impossible.

XML injection

XML injection issues occur when the data used to construct XML code, which may contain XML metacharacters, is not encoded properly. The Oracle InForm Adapter software handles this by using standard XML processing components that construct the XML documents. It is recommended that the client code also uses standard XML processing components to ensure that data is properly encoded. If XML is constructed manually, the developer should ensure that any untrusted data is properly encoded to prevent XML injection.

#4 - Insecure design

A perfect implementation cannot solve an insecure design; instead, effective security controls are required to protect against certain threats. In order to prevent known attack methods, developers must routinely assess threats and make sure that code is robustly designed and tested. Utilize threat modeling for crucial key flows, access control, business logic, and authentication. Establish and use Architecture Risk Assessment protocols to help evaluate and design security and privacy-related controls.

#5 - Security misconfiguration

To securely allow subject data to be submitted, the Clinical Data API requires authentication information from two users:

- An InForm Integration user with the ODM Submit right.
- An InForm Site or Sponsor user with the Enter CRF data right.
- XML External Entities (XXE)

XML External Entities (XXE)

The format for API is based on the Operational Data Model (ODM), which is a representation of clinical data created by the Clinical Data Interchange Standards Consortium (CDISC). The XML format that the Oracle InForm application accepts is called Oracle InForm ODM because it has Oracle InForm-specific extensions to the base ODM XML schema.

Clinical Data API have been tested to verify that XML upload functionality validates incoming XML using XSD validation that can be submitted to the Oracle InForm application.

#6 - Vulnerable and Outdated Components

The Clinical Data API stack is constantly updated with the latest security fixes and patches. Oracle recommends that developers using the API do the same.

#7 - Identification and authentication failures

Risks associated with broken authentication and session management are often due to these functions not being implemented properly. As previously stated, custom authentication mechanisms should not be implemented and have not been implemented. To address web service client authentication attacks, the Clinical Data API supports username token authentication. To ensure the integrity of web client authentication, the proper handling of the authentication artifacts should be followed.

To ensure the web client authentication is secure, the password for the username token should be treated with the utmost care since exposure of the password could compromise the authentication mechanisms systems. The Clinical Data API does not store the password in clear-text on the file system and does not log the password. As such, the client password should be protected in the same way. The password should always be stored in an encrypted fashion. Do not transfer the password through un-encrypted side channels between web service endpoint parties when exchanging the password to reduce exposure. The authentication of each side channel endpoint is also a concern during the exchanging of the password and is open to social engineering attacks if not done properly. To access the web service interfaces and to use the Clinical Data API, you must be an InForm Integration user with the ODM Submit right. For more information, see the *Clinical Data API Guide*.

The Clinical Data API is stateless and does not maintain the session. The API is re-entrant and the same credentials may be used for the calls. Considerations with the number of the concurrent calls should be designed not to exhaust the resources of the systems.

#8 - Software and data integrity failures

If APIs deserialize hostile or tampered objects supplied by an attacker, they will become vulnerable. The Clinical Data API should not accept serialized objects from untrusted sources or use serialization mediums that only permit primitive data types.

#9 - Security Logging and Monitoring Failures

Developers should establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion. Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts. Ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions.

#10 - Server-Side Request Forgery (SSRF)

Server Side Request Forgery, also known as SSRF, is a security vulnerability that allows a malicious threat actor to induce the server side of a web application or API to perform unauthorized actions. The Clinical Data API's objects have undergone testing to ensure that suitable permission structures are used within the scope of the service's functions. To prevent common SSRF attacks, make sure the authorization model of the API interface is consistent while writing code and delivering data to and from the API.