

# Secure Configuration Guide

Oracle<sup>®</sup> Health Sciences InForm 6.0



**ORACLE**

Part Number: E37408-01

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software -- Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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.

# Contents

<b>About this guide</b>	<b>v</b>
Overview of this guide.....	vi
Audience .....	vi
Related information.....	vii
Documentation.....	vii
If you need assistance.....	x
<b>Chapter 1 Security overview</b>	<b>1</b>
Application security overview.....	2
General security principles .....	3
Require complex and secure passwords.....	3
Change passwords periodically .....	3
Keep passwords private and secure .....	3
Lock computers to protect data.....	3
Provide only the necessary rights to perform an operation.....	3
<b>Chapter 2 Secure installation and configuration</b>	<b>5</b>
Installation overview .....	6
Secure Sockets Layer (SSL).....	6
Install only the InForm features needed .....	6
About entering passwords .....	7
Configure strong administrator passwords.....	7
Close all unused ports.....	8
Disable all unused services.....	8
Terminate unneeded user accounts.....	9
Post-installation configuration .....	10
Restrict access to InForm server machines .....	10
Configure strong user passwords .....	10
Configure rights and rights groups.....	10
Configure the pfreportinguser account .....	11
Change the pfuser password as required.....	11
Change the PFCapAdmin password as required .....	13
<b>Chapter 3 Security features</b>	<b>15</b>
User security features .....	16
Password configuration for user security.....	16
Passwords for new users .....	16
Login security.....	16
Security questions .....	17
No data loss after a session transaction.....	17
Automatically inactivated user accounts.....	17
Restricted access to the application.....	18
Application security features.....	19
Users assigned to user types .....	19
Rights assigned to rights groups .....	19
Users assigned to rights groups.....	20
Users assigned to groups.....	20
Users assigned to sites .....	20
Display overrides.....	21

Data security features.....	22
Restricted viewing of Protected Health Information.....	22
Audit trails for data security .....	22
Freezing and locking data .....	22

# About this guide

## In this preface

Overview of this guide.....	vi
Related information.....	vii
If you need assistance.....	x

## Overview of this guide

The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences InForm application, including details about the general principles of application security, and how to install, configure, and use the InForm application securely.

## Audience

This guide is for users who install and configure the InForm application.

## Related information

### Documentation

All documentation is available from the Oracle Software Delivery Cloud (<https://edelivery.oracle.com>) and the Download Center (<https://extranet.phaseforward.com>).

Document	Description
<i>Release Notes</i>	The <i>Release Notes</i> document describes enhancements introduced and problems fixed in the current release, upgrade considerations, release history, and other late-breaking information.
<i>Known Issues</i>	The <i>Known Issues</i> document provides detailed information about the known issues in this release, along with workarounds, if available.  <b>Note:</b> The most current list of known issues is available on the Extranet. To sign in to the Extranet, go to <a href="https://extranet.phaseforward.com">https://extranet.phaseforward.com</a> .
<i>Upgrade and Migration Guide</i>	The <i>Upgrade and Migration Guide</i> provides instructions for upgrading and migrating the InForm software and InForm Portal software to the current InForm release, and for upgrading the Cognos 8 Business Intelligence software for use with the Reporting and Analysis module. The guide also describes any changes and additions made to the database schema, MedML, and resource files.
<i>Secure Configuration Guide</i>	The <i>Secure Configuration Guide</i> provides an overview of the security features provided with the Oracle® Health Sciences InForm application, including details about the general principles of application security, and how to install, configure, and use the InForm application securely.
<i>Installation Guide</i>	The <i>Installation Guide</i> describes how to install the software and configure the environment for the InForm application and Cognos 8 Business Intelligence software.
<i>Study and Reporting Setup Guide</i>	The <i>Study and Reporting Setup Guide</i> describes how to perform the tasks that are required to set up an InForm study and configure the Reporting and Analysis module for the study.
<i>User Guide</i>	The <i>User Guide</i> provides an overview of the InForm application including details on multilingual studies, how to navigate through the user interface, and how to use the application to accomplish typical tasks you perform while running a clinical study.  This document is also available from the Documentation CD and the InForm user interface.

Document	Description
<i>Reporting and Analysis Guide</i>	<p>The <i>Reporting and Analysis Guide</i> provides an overview of the Reporting and Analysis module. It includes a brief overview of the Reporting and Analysis interface, illustrates how to access the Ad Hoc Reporting feature, and describes the study management and clinical data packages available for Reporting and Analysis. It also provides detailed descriptions of each standard report that is included with your installation.</p> <p>This document is also available from the Documentation CD.</p>
<i>Reporting Database Schema Guide</i>	<p>The <i>Reporting Database Schema Guide</i> describes the Reporting and Analysis database schema, and provides information on creating Reporting Database Extracts (RDEs).</p>
<i>Portal Administration Guide</i>	<p>The <i>Portal Administration Guide</i> provides step-by-step instructions for setting up the InForm Portal software, and configuring and managing the InForm Portal application.</p> <p>This document is also available from the Documentation CD.</p>
<i>Utilities Guide</i>	<p>The <i>Utilities Guide</i> provides information about and step-by-step instructions for using the following utilities:</p> <ul style="list-style-type: none"> <li>• PFConsole utility</li> <li>• MedML Installer utility</li> <li>• InForm Data Import utility</li> <li>• InForm Data Export utility</li> <li>• InForm Performance Monitor utility</li> <li>• InForm Report Folder Maintenance utility</li> </ul> <p>This guide also provides reference information for the MedML elements and scripting objects that are used to import and export data to and from the InForm application, as well as sample data import XML.</p> <p>This document is also available from the Documentation CD.</p>
MedML Installer utility online Help	<p>The MedML Installer utility online Help provides information about, and step-by-step instructions for using, the MedML Installer utility, which is used to load XML that defines study components into the InForm database.</p> <p>This guide also provides reference information for the MedML elements and scripting objects that are used to import and export data to and from the InForm application, as well as sample data import XML.</p> <p>This document is also available from the user interface.</p>

---

Document	Description
InForm Data Export utility online Help	<p>The InForm Data Export utility online Help provides information about and step-by-step instructions for using the InForm Data Export utility, which is used to export data from the InForm application to the following output formats:</p> <ul style="list-style-type: none"><li>• Customer-defined database (CDD).</li><li>• Name value pairs.</li></ul> <p>This document is also available from the user interface.</p>
InForm Data Import utility online Help	<p>The InForm Data Import utility online Help provides information about and step-by-step instructions for using the InForm Data Import utility, which is used to import data into the InForm application.</p> <p>This document is also available from the user interface.</p>

---

## If you need assistance

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

# CHAPTER 1

## Security overview

### In this chapter

Application security overview .....	2
General security principles .....	3

## Application security overview

To ensure security in the 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

## 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* (on page 10).

## 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.

## 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* (on page 16).

Encourage users to choose password-reset questions and answers that are easy for them to remember, but difficult for someone else to guess. For more information, see *Security questions* (on page 17).

## Lock computers to protect data

Encourage users to lock computers that are left unattended. For more information, see *Login security* (on page 16).

## 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* (on page 19).
- *Rights assigned to rights groups* (on page 19).
- *Users assigned to rights groups* (on page 20).
- *Users assigned to groups* (on page 20).



## CHAPTER 2

# Secure installation and configuration

### In this chapter

Installation overview .....	6
Post installation configuration .....	10

## Installation overview

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

### Secure Sockets Layer (SSL)

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

### Install only the InForm features needed

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

- Minimal—Default option. This option installs:
  - InForm core software
  - Required utilities
  - Documentation

If you plan to use the Reporting and Analysis module, do not select the Minimal option. It does not install the reporting utilities.

- Complete—Recommended option. This option installs:
  - InForm core software
  - Required utilities
  - Sample study
  - InForm Portal
  - All InForm utilities
  - Documentation

For the Complete option, all the utilities are installed. You cannot select specific utilities to install.

- Custom—Installs the InForm core software and required utilities and the following options, if they are selected:
  - Documentation
  - Sample study
  - InForm Portal
  - InForm utilities

For Custom installations, all the utilities are selected by default to be installed. You can choose whether to install each of the following utilities:

- InForm Data Import
- InForm Data Export
- InForm Performance Monitor
- InForm Reporting

If you plan to use the Reporting and Analysis module, the InForm Reporting utility must be selected.

**Note:** If you are using the Reporting and Analysis module, you must install the Cognos software, and run the Reporting installers and the reporting utilities that are installed by the InForm application.

## About entering passwords

The 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 InForm application, the following database administrator users are created.

- **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 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.

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

## Disable all unused services

Disable all unused services.

The InForm application uses the following services:

- InForm Service
- IBM Cognos 8
- COM+ System Application
- Distributed Transaction Coordinator
- DNS Client
- IIS Admin Service
- Oracle MTS Recovery Service
- World Wide Web Publishing Service

## Terminate unneeded user accounts

The InForm application creates a number of user accounts for studies.

Certain user accounts that were created in InForm releases prior to release 6.0 are not required by the InForm 6.0 application and can be terminated.

- When studies are migrated to the InForm 6.0 release, these accounts are terminated automatically.

It is possible, though unlikely, that a study design has a dependency on an account that is not required by the InForm application. Before terminating these accounts for active studies, ensure that no dependency exists. If necessary, change the study to remove the dependency before terminating the account.

- The InForm 6.0 application does not create non-critical accounts by default.
- Some user accounts are required by the InForm application and cannot be terminated. Do not terminate or deactivate these user accounts.

The following table summarizes how user accounts are handled in the InForm 6.0 release.

Account name	After migration	In InForm 6.0
UM	Terminated	Not created
UA	Terminated	Not created
InfAdmin	Terminated	Not created
InFusionAdmin	Terminated	Not created
InFormUser	Terminated	Not created
Pfreportuser	Terminated	Not created
Sysadmin	Terminated	Not created
system	Terminated	Terminated
Pfreportinguser	Not terminated	Not terminated
autoquery	Terminated	Terminated
pfarchuser	Terminated	Not created
ctcoding	Terminated	Terminated
ctvalidation	Terminated	Terminated
IVRS	Terminated	Not created

## Post-installation configuration

### Restrict access to InForm server machines

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

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* (on page 16).

### 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* (on page 19).
- *Rights assigned to rights groups* (on page 19).
- *Users assigned to rights groups* (on page 20).
- *Users assigned to groups* (on page 20).

## Configure the pfreportinguser account

The 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 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 about the pfreportinguser user, and resetting the pfreportinguser account password, see the *Installation Guide*.

## Change the pfuser password as required

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

- 1 *Run pfadmin* (on page 11).
- 2 *Update IIS with the new pfuser password* (on page 12).
- 3 *Update COM+ applications with the new password* (on page 12).

### Run pfadmin

The following pfadmin command resets the pfuser account password in the 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* (on page 12).

## 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 username in the **Specific user** field, and then click **Set**.

The Set Credentials dialog box appears.

- 6 Paste the username 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* (on page 11).

- 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 COM+ application that has a listed account of `PfUSR_<machine name>`.

## 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*.



# CHAPTER 3

## Security features

### In this chapter

User security features .....	16
Application security features .....	19
Data security features .....	22

# User security features

## Password configuration for user security

An administrator can define the following formatting, entry, and reuse requirements for passwords directly in the InForm application on the System Configuration page. For the recommended settings see, *General security principles* (on page 3) and the *User Guide*.

- 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.
- Whether the password can be reused. Recommended setting is No.
- Number of 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. At the initial login, users set their security questions and answers, and provide their email address.

## Login security

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 the value that 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.

Users who forget their passwords must answer their security questions correctly in order to have a new, temporary password sent to their email address. After entering the temporary password, the user must reset the password and the security questions.

## Security questions

Users who exceed the number of allowed login attempts, resulting in a locked user account, can answer their security questions to reset the password and unlock the account. Password questions and answers are available in the application to control access to some studies.

- At the initial login, each user:
  - Selects two security questions and provides answers to be used when the user forgets the password.
  - Sets the password.
- To reset a password in the application, the user must provide the correct answers to the security questions.

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

## 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. Queries in the Candidate state are not visible to Site users. This user is not allowed to see certain information, for example Candidate queries.
- **Sponsor User**—User who performs sponsor functions such as monitoring and data management. Queries in the Candidate state are visible to sponsor users.

## 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 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*.

## Users assigned to rights groups

The following pre-defined rights groups are provided with the 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.

- PFReportUser
- User Manager
- User Activator
- InForm Server Group
- PFArchUser
- SysAdmin
- Admin
- Principal Investigator
- CRC
- CRA
- CDM
- Project Manager

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 of 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 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*.

## 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*.

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

# Data security features

## Restricted viewing of Protected Health Information

You can use user types, rights, groups, and display overrides to restrict the users that can view Protected Health Information, which appears in subject profiles.

Access to confidential subject information is also restricted. Therefore, your study is set up so that only specific users, such as clinical research coordinators, can enter subject data.

## 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*.

## Freezing and locking data

You can freeze or unfreeze data on the subject, visit, form, and item 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, form, or item 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, form, or item.