

Integrated Assessment Record (IAR)

IAR PRIVACY OFFICER MANUAL

NOVEMBER 2016

Legal Notice

These educational materials may be copied or distributed without permission solely for educational and implementation purposes, provided that (i) this notice is reproduced on all copies, and (ii) these materials are not modified in any way, neither provided nor distributed alone or in conjunction with any other materials, for money or other consideration.

These educational materials are provided by the Community Care Information Management – Integrated Assessment Record (CCIM – IAR) and are designed for use with the education and implementation support program provided by the CCIM – IAR Project Team. These materials alone are not sufficient for a successful and complete IAR implementation.

This education material and the information contained herein are proprietary to Community Care Information Management. The recipient of this information, by its retention and use, agrees to protect it from any loss, theft or compromise.

Contents

Introduction	5
Purpose	5
Getting Started	6
Logging in to the IAR	6
Logging out of the IAR	7
Forgotten Password	7
Automatic Logout	7
Homepage	8
Left Menu	8
Top Menu Icons	10
Shortcut Keys	10
My Details	11
Change Password	11
Set Security Question	11
Inactivity Logout	12
Time Zone	12
Important Message Notification	12
Groups I Belong To	12
Roles I Belong To	12
Users and IAR Common Details	12
Person Search	13
Person Search Criteria	13
Person Search Results	14
Summary View	15
Person Demographics	15
Assessment Information	15
Person Context Bar	16
Worklists	17
Add Person Records to a Worklist	17
Add Person Names from a Person Search	17
Add Person Names from the Context Bar	18
Customize Worklists	18
Rename a Worklist	18
Edit the Columns that Appear on a Worklist	19
Remove a Person from a Worklist	19
Privacy and Consent Directives	20
Monitoring	21
Privacy Log	21
Clinical Log	22
Current Activity Log	25
System Log	27

Printing or Downloading the Search Results	28
Operational Reports	29
OP1 – IAR Users	29
OP2A – IAR Locations.....	31
OP2B – List of IAR Organizations	32
Privacy Reports	33
PS1 – IAR User Activity Report	34
PS2 – IAR Event Type Report.....	35
PS3 – IAR Consent Directives History Report.....	36
PS4 – IAR Current Consent Directive Report.....	37
PS5 – IAR User PHI Access Report.....	38
PS6 – IAR PHI Disclosure Report	39
PS7 – Assessment Disclosure Report.....	40
PS8 – Inactive User Report.....	41
Messaging.....	42
Received Messages	42
New Messages.....	44
Sent Messages.....	45
Deleting a Message.....	45
Appendix A: Audit Log Event Types	46
Different Event Types in the Clinical Log.....	46

Introduction

The Integrated Assessment Record (IAR) is a framework that provides security, user account management, a seamless view of a person's details and assessment information and monitoring capabilities.

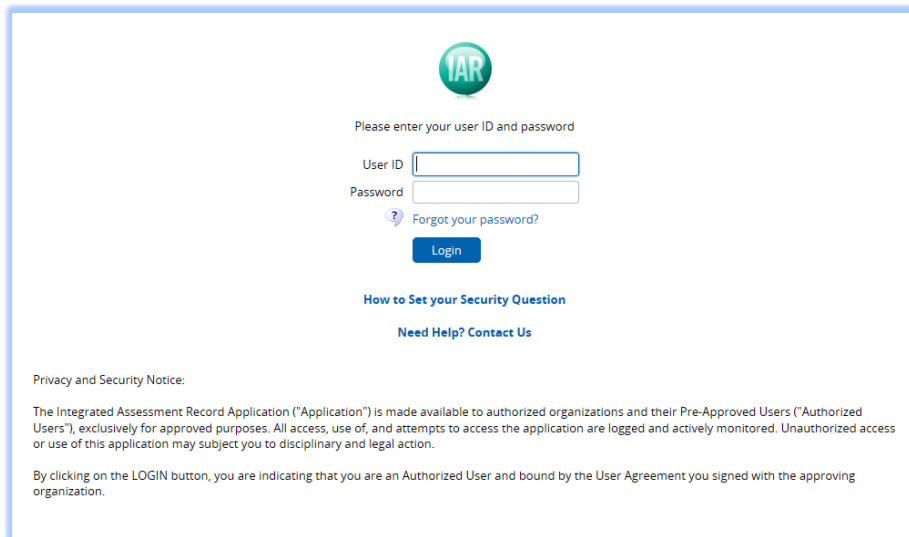
Purpose

This document identifies the key concepts that will allow the **Privacy Officer** role to effectively use the application. Examples include selecting and viewing person records, monitoring users associated with their organization(s), and exchanging messages with other users.

Getting Started

Logging in to the IAR

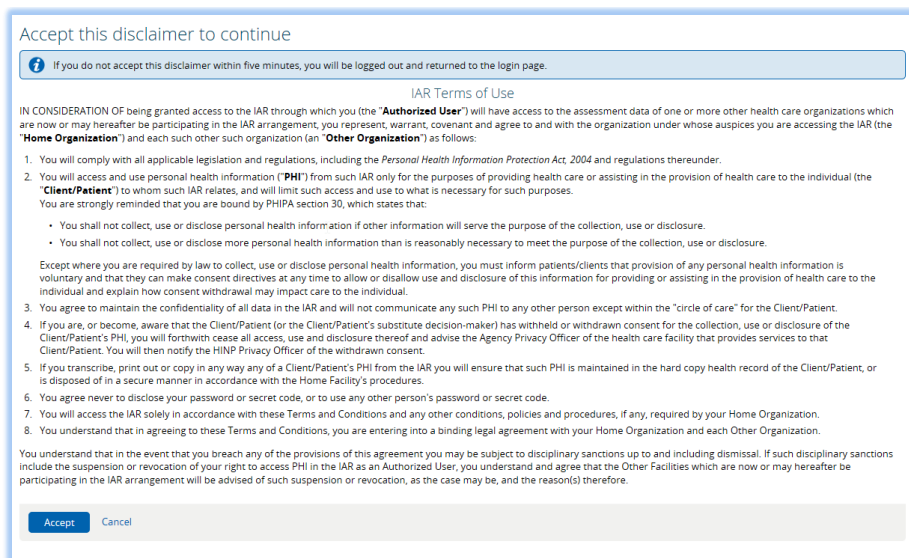
The IAR login screen is shown below. A user ID and password are required to gain access to the application. A default password will be assigned when the account is first set up. Once the user has entered the user ID and default password the system will prompt the user to change the password. **Note:** While the user ID is not case-sensitive, the password is and must be at least 8 characters in length. Passwords will expire after 90 days and must be reset at that time.



The IAR login screen features a green circular logo with 'IAR' in white. Below the logo, the text 'Please enter your user ID and password' is displayed. There are two input fields: 'User ID' and 'Password'. A link for 'Forgot your password?' is located below the password field. A blue 'Login' button is positioned below the input fields. Below the login button, there are two links: 'How to Set your Security Question' and 'Need Help? Contact Us'. At the bottom, a 'Privacy and Security Notice' section contains text about the application's use and a statement that clicking the LOGIN button indicates the user is an Authorized User bound by the User Agreement.

IAR LOGIN SCREEN

When an individual assigned to the **Privacy Officer** role logs in to the IAR, a **disclaimer** screen will appear as displayed below:




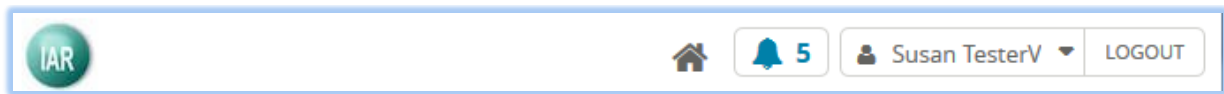
The disclaimer screen has a title 'Accept this disclaimer to continue'. A blue box with an information icon contains the text: 'If you do not accept this disclaimer within five minutes, you will be logged out and returned to the login page.' Below this is the 'IAR Terms of Use' section. It begins with 'IN CONSIDERATION OF being granted access to the IAR through which you (the "Authorized User") will have access to the assessment data of one or more other health care organizations which are now or may hereafter be participating in the IAR arrangement, you represent, warrant, covenant and agree to and with the organization under whose auspices you are accessing the IAR (the "Home Organization") and each such other such organization (an "Other Organization") as follows:'. It then lists eight numbered points regarding data confidentiality, PHI use, consent, and legal agreement. At the bottom, there are two buttons: 'Accept' (highlighted in blue) and 'Cancel'.

IAR LOGIN DISCLAIMER SCREEN


The user must select the **Accept** button within 5 minutes to proceed with logging in to the IAR. If you do not accept the terms of use click on the **Cancel** link to return to the login screen.

Logging out of the IAR

The **Logout**  button is used to exit the IAR. It is located in the top menu (upper right portion of any screen).

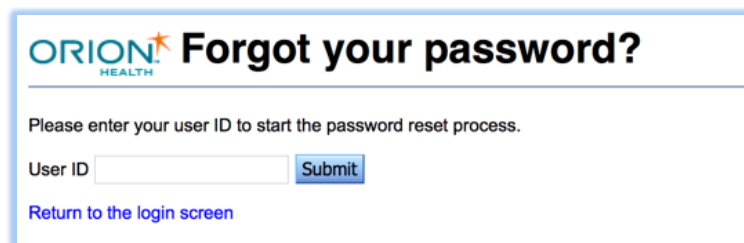


LOGOUT BUTTON


It is important to use the **Logout** button as opposed to clicking on the red X button  located in the upper right hand corner of the browser. The **Logout** button will log the user out of the system. If it is not used, the session will remain active for a pre-defined period of time before the auto-logout feature is activated.

Forgotten Password

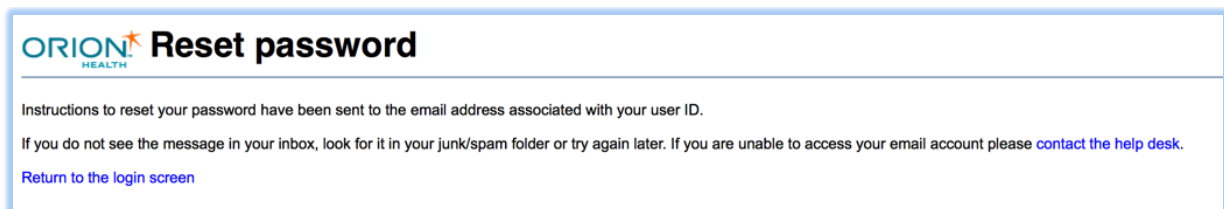
Note: If a user has three (3) invalid login attempts within a 30 minute period, he or she will be locked out of the IAR for 24 hours. Therefore, if a user forgets his or her password, he or she may select the '**Forgot Your Password?**' link on the log in screen. The user will be asked to submit his or her user ID as displayed in the screen below:



FORGOTTEN PASSWORD SCREEN

Select the **Submit**  button to send an email to the administrator.

If the user has set up his or security question and email the system will prompt the user to answer this security question. The user will then be requested to select a new password and verify it.

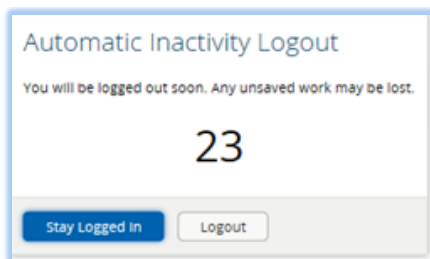


RESET PASSWORD MESSAGE

Automatic Logout

The inactivity logout feature in the IAR ensures robust security by logging out the user if he or she has been inactive for a pre-defined set of time. The inactivity logout period currently set by the administrator is 30 minutes. A user may change his or her inactivity logout setting to a time less than 30 minutes on the **My Details** screen. See **The My Details** section of this document for more information.

The screen below provides an example of the warning a user will see if the user has been inactive for a set period of time.

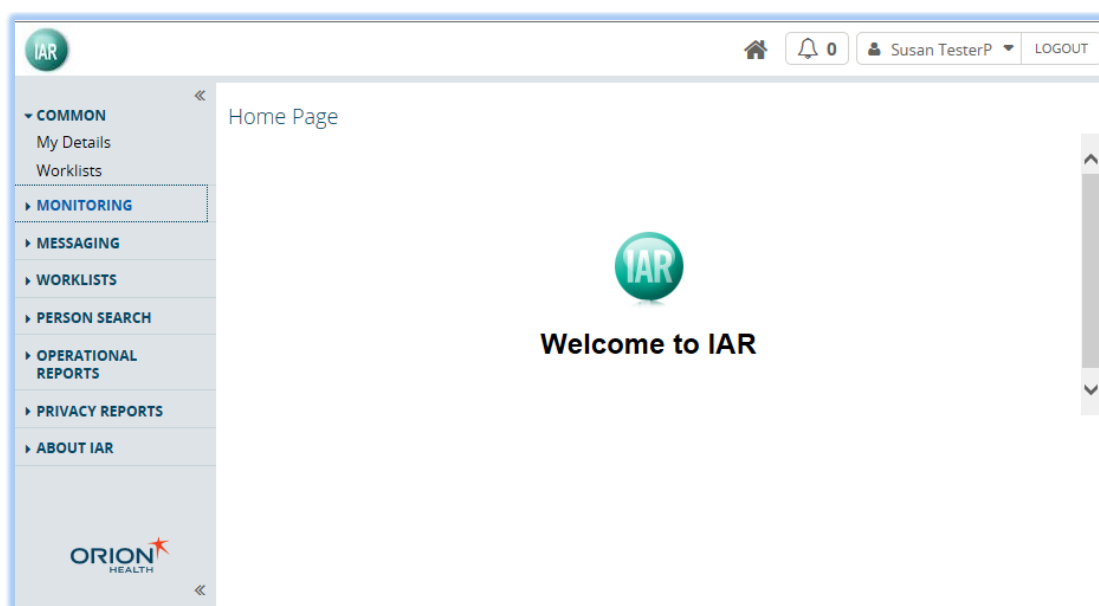


AUTOMATIC LOGOUT

Clicking the **Stay Logged In** button will allow you to remain active.

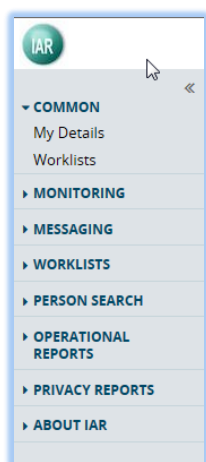
Homepage

The following **Homepage** automatically appears when a **Privacy Officer** user logs in to the IAR:



PRIVACY OFFICER HOMEPAGE

Left Menu



Found on the left hand side of the IAR window, the **Left Menu** is the primary navigation method. Each left menu option contains one or more items which are links to various functions for the Privacy Officer. Access to menus and items within it are dependent on access privileges granted to the user.

If more items are available than can be displayed, **Up** and **Down** scroll arrows will become available.




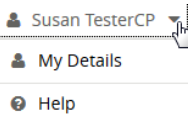

Click the  icon to hide or the  icon to show the left menu.

The following menus are available for the **Privacy Officer** role:

Menu	Description	Entry Point
COMMON	Maintain personal details	<ul style="list-style-type: none"> • My Details • Worklists
MONITORING	Monitor the audit logs for all users associated with his or her organization (or organizations)	<ul style="list-style-type: none"> • Clinical Log • Current Activity Log • Privacy Log • System Log
MESSAGING	Compose, receive and send messages to other IAR users	<ul style="list-style-type: none"> • New Message • Received Messages • Sent Messages
WORKLISTS	Maintain links to the personal worklists	<ul style="list-style-type: none"> • Red • Blue • Yellow • Green • Orange • Purple
PERSON SEARCH	Locate a person to view assessment forms	<ul style="list-style-type: none"> • Person Search
OPERATIONAL REPORTS	View, print or save reports related to IAR users, organizations, uploads, and assessment statistics	<ul style="list-style-type: none"> • OP1 – IAR Users • OP2A – IAR Locations • OP2B – IAR Organizations
PRIVACY REPORTS	View, print or save reports related to privacy, including consent directives and user access of personal health information	<ul style="list-style-type: none"> • PS1 – IAR User Activity Report • PS2 – IAR Event Type Report • PS3 – IAR Consent Directives History Report • PS4 – IAR Current Consent Directive Report • PS5 – IAR User PHI Access Report • PS6 – IAR PHI Disclosure Report • PS7 – Assessment Disclosure Report • PS8 – IAR Inactive User Accounts Report
ABOUT IAR	View details about this release of the IAR	<ul style="list-style-type: none"> • About

Top Menu Icons

The top menu is displayed at the top right of any screen, and allows you to do the following:

Icon	Function	Description
	Home	Clicking the home icon will display your Homepage
	Messages	Displays the number of unread messages; the  symbol and red colour indicates one or more of these messages are important - clicking the icon will display your list of received messages
	Username	Displays your IAR user name – clicking on your name will provide you with the option to navigate to the My Details screen or access details to contact the IAR Support Centre (Help)
	Logout	Ends the current IAR session

Shortcut Keys

The following shortcut keys are available:

Keys	Description
F11	Toggles between a full screen and a standard Windows display (feature not available on Mac OS machines)
F5	Refreshes the screen display
Tab	Moves to the next field on a screen
Shift+Tab	Moves to the previous field on a screen
Enter	Activates the current selected button or option

My Details

My Details is located in the **Common** tab of the left menu bar. It allows individuals assigned to the **Privacy Officer** role to change their passwords, set a security question in case they forget their password, set inactivity logout, customize time zone settings, set the time that important message notification messages will display, view roles and groups and view their organization and email.

MY DETAILS SCREEN

The following fields are available on the **My Details** page:

Change Password

Click the **Change Password** button to change the password.

PASSWORD CHANGE POP UP SCREEN

Set Security Question

Select the **Set Security Question** link to create a security question and answer which can be used to authenticate the user in the event that a user has forgotten his/her password and cannot log into the IAR. The user will also be required to provide a password for verification. Once you have set your security question and answer, use this function to **Change** your security question and answer in future, if required.

SECURITY QUESTION SCREEN

Inactivity Logout

In order to provide a secure environment, the IAR allows a user to set up an inactivity logout period. This setting ensures that the user will be logged out of the IAR if he/she does not use his/her computer for the number of minutes equal to the inactivity logout value.

- The logout on this screen may only be set to a time that is less than 30 minutes.
- The IAR counts mouse movement as activity. As such, if a user is viewing a document and the mouse pointer does not move, a logout may be triggered.

Time Zone

Select the time zone to display if it is different than the default setting of the Canada/Eastern Standard Time zone.

Important Message Notification

An important message is one that has been tagged important by the user who sent it. The IAR user who receives the message will see an alert at the bottom of the screen. The message that displays is based on the alert selected on the **My Details** screen. The following options are available:

- **Show alert until dismissed:** If selected, displays the message until the alert is closed by the user
- **Show alert for <n> seconds:** If selected, displays the message for the set number of seconds
- **Do not show alert:** If selected, the important message alert will never be displayed

An example of the message notification is provided below:



IMPORTANT MESSAGE NOTIFICATION

Groups I Belong To

This section lists the user's group membership which determines access to the different IAR screens and functions. It is important to provide this information to the support desk if you are having any difficulties with the IAR.

Roles I Belong To

This section lists the user's typical function within the organization; in this case; the **Privacy Officer** role. It is important to provide this information to the support desk if you are having any difficulties with the IAR.

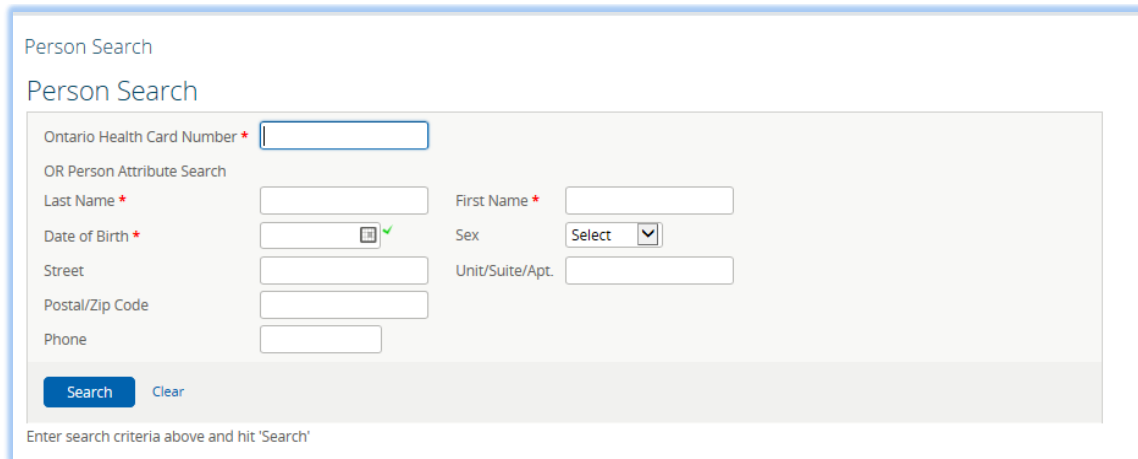
Users and IAR Common Details

This section provides the user with the ability to enter or update his/her email. It also displays the organization(s) associated with the user's IAR account.

Person Search

The person search allows the **Privacy Officer** role to find a person using a variety of different search criteria. Once the person is found, the user may easily access the person record. The **Person Search** can be found by selecting **Person Search** from the **Person Search** option in the left menu.

Person Search Criteria




PERSON SEARCH CRITERIA

The person search allows a user to search for a person using one or more of the following search criteria:

- The person's **Ontario Health Card Number** (OHIP Number): The identification must be an exact match. If entered as a part of the search criteria, it will take precedence over all other search criteria. Do not enter a version code.

OR

- The person's **last name**: The person's full family name (e.g., Phillips). The full first name and date of birth must also be entered.
- The person's **first name**: The person's first name (e.g., Jim). Partial information may be entered; **Note**: A full last name and date of birth must also be entered.
- The person's **date of birth**. Click on the **Calendar**  icon and select a date from the resulting screen to ensure the correct format is used (DD-MM-YYYY). **Note**: The last name and first name must also be entered.

Additional demographic information can help narrow down a search. Please note that last name, first name and date of birth must also be entered.

- The person's **sex or gender**. Female, Male or Unknown.
- The person's **street** address.
- The person's **unit/suite/apartment** number if applicable.
- The person's residential **postal code**.
- The person's **phone number**.

Person Search Results

<input type="checkbox"/>	Score	Last Name	First Name	Alias	Sex	Date of Birth	City	Phone
<input type="checkbox"/>	4.4	Linson	Ashley		Female	20-Jun-1978	Toronto	416-111-2233
Add checked results to worklist <input type="button" value="v"/> Replace worklist with checked results <input type="button" value="v"/>								
Results 1-1								

PERSON SEARCH RESULTS

Up to 15 person names may be returned by a Person Search. The results are sorted by the last name. The following results are displayed:


- **Score:** reflects the algorithm based on the amount and quality of information entered.
- Last name
- First name
- **Alias:** The most recent alias will display if there is more than one alias for this person
- Sex
- Date of Birth
- **City:** The most current city will display if there is more than one city identified as contact information
- **Phone:** The most current phone number will display if there is more than one contact number

The person search allows users to navigate through person records, and add a person to a worklist. See the **Worklists** section of this document for more information.

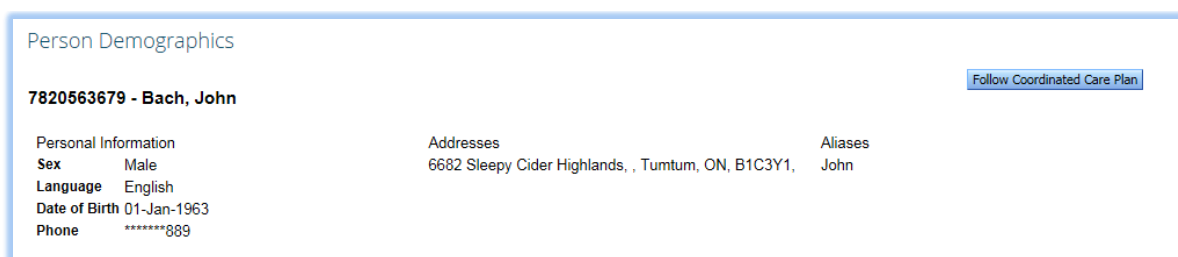
Summary View

The **Summary View** is displayed when a **Privacy Officer** selects a person from the person search results or a worklist. The **Privacy Officer** has privileges to see the **Person Demographics**. He or she does not have privileges to view the assessment windowlet.

If the person summary is not currently on the screen, it can be displayed by clicking the **Assessment Listing**

 **Assessment Listing** icon at the top of the Document Tree.

Person Demographics



The screenshot shows a windowlet titled "Person Demographics". At the top left, it displays "7820563679 - Bach, John". At the top right, there is a button labeled "Follow Coordinated Care Plan". Below this, the information is organized into three columns: "Personal Information", "Addresses", and "Aliases". Under "Personal Information", it lists Sex: Male, Language: English, Date of Birth: 01-Jan-1963, and Phone: *****889. Under "Addresses", it lists 6682 Sleepy Cider Highlands, , Tumtum, ON, B1C3Y1. Under "Aliases", it lists John.

THE PERSON DEMOGRAPHICS WINDOWLET

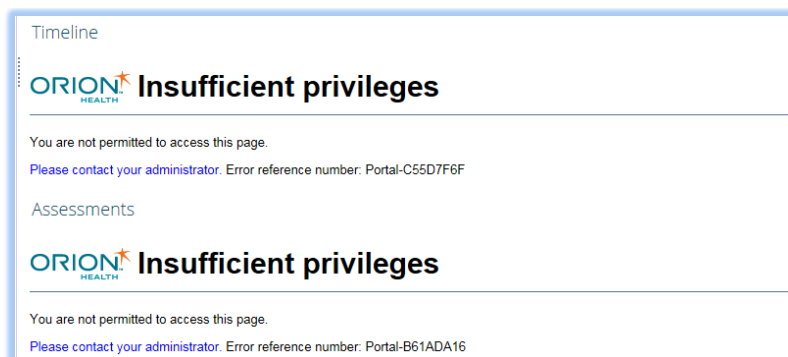
The **Person Demographics** windowlet displays the person's personal and contact details, and can be used to check that the intended person has been selected. It includes the following information:

- The person's **name**
- The Ontario **Health Card Number** (if available)
- **Personal information** such as sex, language, date of birth and phone number
- **Address** details (if the person has multiple addresses, the last five addresses will be displayed)
- **Aliases** (if the person has multiple aliases, the last five names will be displayed)

Note: If additional address information or alias information is available, the user may select the **Show Additional...** buttons to view the additional details.

Assessment Information

The **Privacy Officer** does not have privileges to view the assessment information. Therefore, the following screenshot will appear:

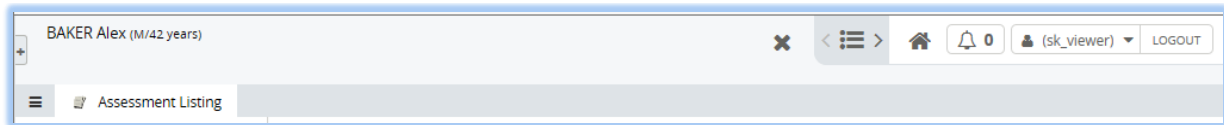


The screenshot shows two messages in a list. The first message is titled "Timeline" and contains the ORION HEALTH logo followed by "Insufficient privileges". Below this, it says "You are not permitted to access this page." and "Please contact your administrator. Error reference number: Portal-C55D7F6F". The second message is titled "Assessments" and also contains the ORION HEALTH logo followed by "Insufficient privileges". Below this, it says "You are not permitted to access this page." and "Please contact your administrator. Error reference number: Portal-B61ADA16".

TIMELINE AND ASSESSMENTS MESSAGES

Person Context Bar

The **Person Context Bar** is visible once a person record has been selected (placed in context). It displays the person's basic identification details, the worklist flag, and other navigation tools. Refer to the table below for more details.



PERSON CONTEXT BAR

Icon	Function	Description
	Person Information	This area will display the person details, including: <ul style="list-style-type: none"> Last name [caps] Suffix, First Name Middle name (Sex/Age years). Note: The years field may display as days, weeks, or months
	Worklists	This will allow you to add or remove a person from a worklist
	Show / Hide Menu	This will allow you to show or hide the left menu
	Assessment Listing	This icon will take you back to the list of that person's assessments
	Close page	This will close the page and return you to your Homepage
	Previous / Next	This will take you back to the previous or next person in context

Worklists

Worklists allow users to quickly access and manage records that may be of special interest. Up to six worklists are available to each user within the IAR. Users cannot see the names of persons on another user's worklist, nor can they see the name that other users have given their worklists.

Up to 100 person names can be added to each worklist. If a user adds more than 100 persons, the user is prompted to choose which persons to remove from the worklist.

The screenshot shows a worklist interface for a user named 'Blue'. At the top, there is a message: 'This worklist is full. To add to this worklist please remove at least 14.' Below this is a table with columns: Name, Sex, Age, and a settings icon. The table contains 10 rows of records, all with the name 'ABBOTT, Addie'. Below the table, there is a 'Show More' link and a 'Remove' button with the text 'None selected'. At the bottom, it says 'Showing 10 of 113'.

	Name	Sex	Age	
<input type="checkbox"/>	ABBOTT, Addie	M	56 years	-
<input type="checkbox"/>	ABBOTT, Addie	M	60 years	-
<input type="checkbox"/>	ABBOTT, Addie	F	64 years	-
<input type="checkbox"/>	ABBOTT, Addie	F	56 years	-
<input type="checkbox"/>	ABBOTT, Addie	M	54 years	-
<input type="checkbox"/>	ABBOTT, Addie	M	77 years	-
<input type="checkbox"/>	ABBOTT, Addie	M	96 years	-
<input type="checkbox"/>	ABBOTT, Addie	M	83 years	-
<input type="checkbox"/>	ABBOTT, Addie	M	59 years	-
<input type="checkbox"/>	ABBOTT, Addie	F	68 years	-

FULL WORKLIST MESSAGE

The following default worklists and their default display names are available:

Green	Blue	Orange
Red	Yellow	Purple

A person's record is added to the worklist either one at a time or in a group selected from the results of a search. Once on a worklist, a person's record can be selected and viewed by clicking on the person's name. A user may also change the display name of the worklist by selecting the corresponding **rename** link at the top of the worklist.

Add Person Records to a Worklist

Add Person Names from a Person Search

Users can add person names to a worklist from the results of a person search by selecting the checkbox to the left of the person's identifier. To add the person, the user then selects the worklist option from either of the drop-down lists at the bottom of the screen.

The screenshot shows a table with columns: Score, Last Name, First Name, Alias, Sex, Date of Birth, City, and Phone. Two rows are visible, both with checkboxes in the first column. Below the table, there is a dropdown menu with the text 'Add checked results to worklist' and a list of worklist options: Red, Blue, Yellow, Green, Orange, and Purple. To the right of the dropdown, there is a button that says 'Replace worklist with checked results'.

	Score	Last Name	First Name	Alias	Sex	Date of Birth	City	Phone
<input checked="" type="checkbox"/>	4.4	Bruce	Wayne	Batman	Male	22-Aug-1949	Merrickville	*****234
<input checked="" type="checkbox"/>	4.2	Wayne	Bruce		Male	12-Oct-1968	Toronto	*****254

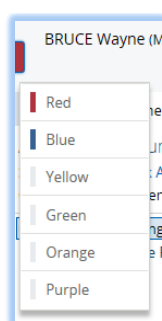
ADDING A PERSON TO A WORKLIST FROM A PERSON SEARCH

- **Add checked results to worklist:** Add the selected person names to the top of the worklist without affecting the names which are already on the list. If the results of this action increase the list past the maximum number of 100, the user will be prompted to select persons to remove from the worklist.
- **Replace worklist with checked results:** Replaces all person names in the worklist with the names selected from the person search.

Add Person Names from the Context Bar

The **Person Context Bar** is visible once a person record has been selected (placed in context). It displays the person's basic identification details, the worklist flag, and other navigation tools. Please see the **Person Context Bar** section for more information.

The **Context Bar** displayed for a selected person includes a **Flag** icon which can be used to manage the user's worklist memberships. If the person is currently on a worklist, the flag icon's background colour will change to match the colour of the flag associated with that worklist, even if you have changed the name of the worklist. If the person is on two or more worklists, the background colour will match the first worklist the person has been added to based on the order displayed in the drop down list (red, blue, yellow, green, orange and finally purple).

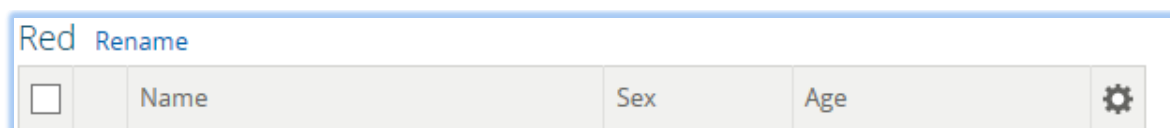


ADDING A PERSON FROM THE CONTEXT BAR

Customize Worklists

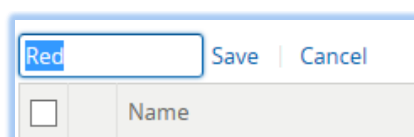
Rename a Worklist

A user can rename a worklist to make it more specific to his or her needs. To rename a worklist, select a specific worklist (e.g., Blue) from the **Worklists** menu. Alternatively, select **Worklists** from the **Common** menu. Click the **Rename** link, beside the worklist name, as shown below:



RENAMING A WORKLIST


The following screen will appear:

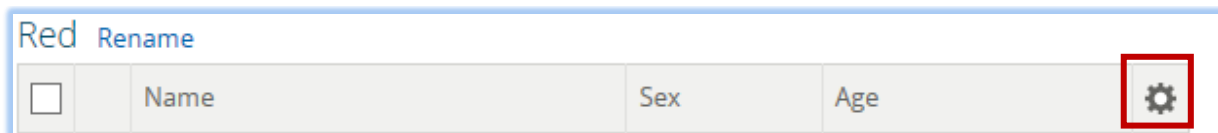


RENAMING A WORKLIST

Type in the new name of the worklist and select the **Save** link. This will change the name of the user's worklist in all that user's locations of the IAR.

Edit the Columns that Appear on a Worklist

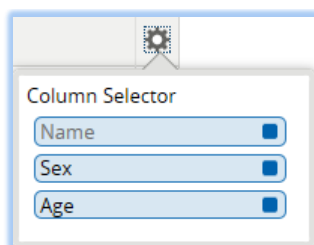
Select the **Settings**  icon on the far right, as shown in the following diagram, to edit which columns appear in that particular worklist.



The screenshot shows the top of a worklist interface. At the top left, there is a text input field containing 'Red' and a 'Rename' link. Below this is a table header with four columns: 'Name', 'Sex', and 'Age'. To the right of the 'Age' column is a gear icon, which is highlighted with a red rectangular box.

EDITING THE COLUMNS

The following screen will appear:




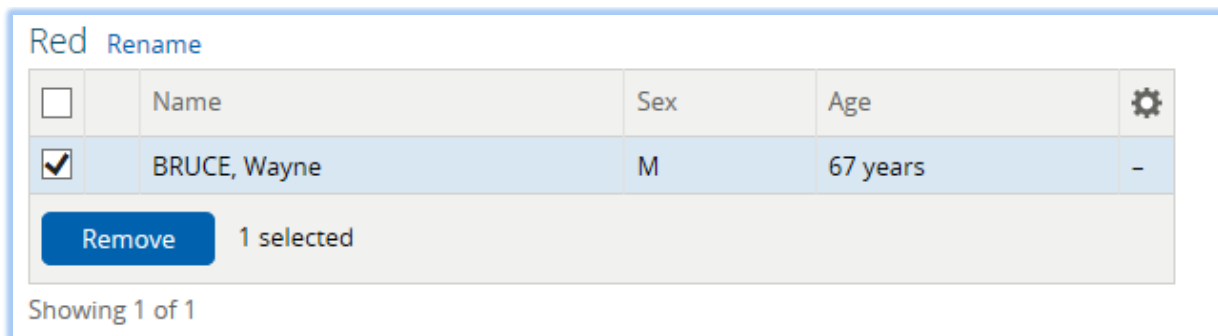
The screenshot shows a 'Column Selector' dialog box. It has a title bar with a close button. Inside, there are three rows, each with a column name and a checkbox: 'Name' with a checked checkbox, 'Sex' with a checked checkbox, and 'Age' with a checked checkbox.

COLUMN SELECTOR

Check or uncheck the sex and/or age column to add or remove these fields from the worklist display.

Remove a Person from a Worklist

Remove one or more persons from a worklist by checking one or more boxes next to the '**Name**' field and clicking the **Remove**  button as displayed in the screenshot below:



The screenshot shows the worklist interface with one data row. The first column has a checkbox that is checked. The 'Name' column contains 'BRUCE, Wayne', the 'Sex' column contains 'M', and the 'Age' column contains '67 years'. To the right of the 'Age' column is a gear icon. Below the table, there is a 'Remove' button and the text '1 selected'. At the bottom, it says 'Showing 1 of 1'.

REMOVE A PERSON FROM A WORKLIST

Privacy and Consent Directives

The IAR solution supports two levels of consent directive: the IAR consent directive and the HSP consent directive.

The **HSP consent directive** is collected by the HSP's staff members from the client/patient when conducting the assessment, and then applied to that assessment. All assessments submitted to the IAR must include a consent flag (i.e., Grant or Deny).

The **IAR consent directive** is obtained directly from the client/patient through the IAR Consent Call Centre, and applied to all assessments relating to an individual client/patient regardless of which HSP uploaded the assessments. An authorized user in the IAR is able to view this client/patient's demographic information, but cannot view any assessment details.

As part of IAR consent directive, the **PI consent directive** is also obtained directly from the client/patient through the IAR Consent Call Centre, and applied to all assessments relating to an individual client/patient regardless of which HSP uploaded the assessments. The IAR would not return any person search results if a user searched for this client/patient.

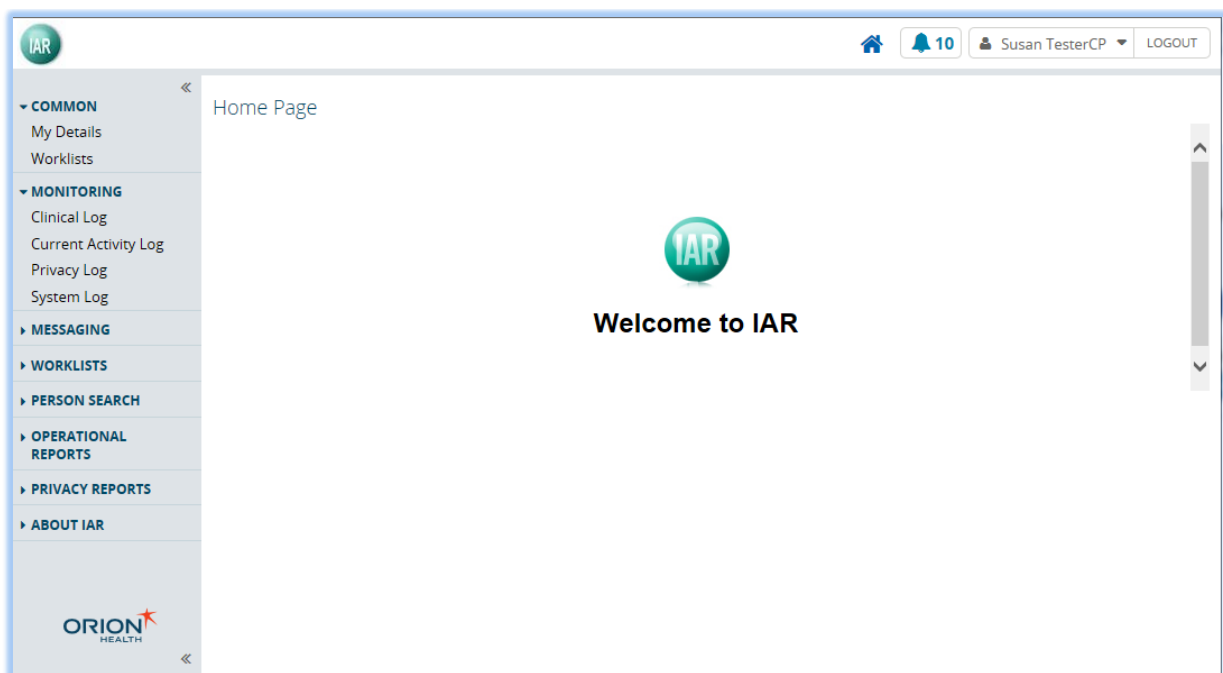
Monitoring

A privacy officer can monitor all user activity associated with his or her organization(s). The following auditing capabilities are available:

- Privacy Log
- Clinical Log
- Current Activity Log
- System Log

The privacy officer can click on one of the logs from the Monitoring menu on the left hand side of the screen.

Privacy Log



The **Privacy Log** captures the consent override events. However, since the consent override is not supported in IAR, the privacy log contains no records at this time.

Clinical Log

Time	User ID	Event Type	Message	Patient ID	Patient Name	Machine IP/ID	Organization	ID Type
19 Oct 2016 13:51:12	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Role Based Clinical Log			10.41.0.98		Patient.Id.MPI
19 Oct 2016 13:51:12	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Clinical Log			10.41.0.98		Patient.Id.MPI
19 Oct 2016 13:49:25	Susan.TesterCPO	Open Application	IAR - User Homepage, Welcome			10.41.0.98		Patient.Id.MPI
19 Oct 2016 13:49:25	Susan.TesterCPO	Open Application	IAR - User Homepage, User Homepage			10.41.0.98		Patient.Id.MPI
19 Oct 2016 13:49:18	Susan.TesterCPO	Search Performed	Integrated Assessment Repository, Privacy Log			10.41.0.98		Patient.Id.MPI
19 Oct 2016 13:49:17	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Role Based Privacy Log			10.41.0.98		Patient.Id.MPI
19 Oct 2016 13:49:17	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Privacy Log			10.41.0.98		Patient.Id.MPI

CLINICAL LOG

The **Clinical Log** entry point under the **Monitoring** menu identifies persons whose data is or has been viewed, and by whom. The list automatically displays all events for the organization(s). A user can choose to filter the list by:

- **User ID:** Enter the ID of the user that performed the event. If this option is specified, the results include all events the user has performed in the system.
- **Patient (person) ID:** Enter the ID associated with the person whose record has been accessed. If this option is specified, the results include all users who have accessed this person's record.
- **Patient (person) Type:** Enter the type of ID associated with the person. For example, the OHIP Number. If this option is specified, the results include all users who have accessed records of persons associated with this type of Patient ID.
- **Patient (person) Name:** Enter the person's name (i.e., Last First).
- **Application:** Select the IAR application accessed by a user. For example, Context Manager. If this option is specified, the results include all users who accessed this application along with the event performed on the application.
- **User Events:** Select the event that the user performed. Hold down the **Ctrl** key to make multiple selections. If this option is specified, the results include all users who performed this event. The events in this list are:
 - **User Authentication:** The user was authenticated to the server
 - **Login:** The user logged on to the server

- **Logout:** The user logged out from the server
- **Account Status Change:** The user changed their account status
- **Password Change:** The user changed their IAR login password
- **Security Change:** The user changed their security preferences
- **Concerto Events:** Select the event that was performed specifically within the IAR. Selecting one or more options identifies all users who have performed the associated action:
 - **Open Application:** The users that opened an application
 - **Open Document:** The users that have opened a document in the document tree
 - **Context Change:** The users that have switched between applications and/or person records
- **Other Events:** Select any other event that the user performed. Hold down the **Ctrl** key to make multiple selections. If this option is specified, the results include all users who performed this event.
- **A Particular Date Range:** If this option is specified, the results include all events that occurred within this date range. Please note that the default date range is the last 30 days, and this log is limited to a maximum search range of 180 days. To query data for more than 180 days, the user will need to run multiple queries with date ranges (up to 180 days each) that cover the period that the user is interested in.
- **A Particular Session:** Enter the Session ID that corresponds to the IAR session in which the event took place.
- **Result:** Select the radio button corresponding with the level of detail to be included in the search results:
 - **All:** If selected, all results obtained by a Clinical Log search are returned, for example all successful and failed user login and/or search attempts
 - **Successful:** If selected, only successful authentications to the IAR and the successful Clinical Log search attempts are listed in search results
 - **Fail:** If selected, only the results of unsuccessful authentications to the IAR are listed in search results
- **Machine IP/ID:** Enter the IP address used by a user to login to the IAR.
- **Organization:** If the privacy officer is associated with more than one organization, he/she can select one or more organizations to filter the list of results.

The Clinical Log displays the following information:

Column Heading	Column Descriptions
Time	The date and time the event occurred
User ID	IAR User ID indicating who performed the activity or event
Event Type	The type of event or activity the user was conducting (e.g., searching for a person, opening an assessment, printing an assessment, changing the password)
Message	Description of the event
Person ID	If the event is related to a client, the client's identifier is displayed as Person ID
Person Name	The client's first and last name
Machine IP/ID	The IP address where the user logged in to the IAR
Organization	The ID and name of the organization the user belongs to
ID Type	The type of Person ID that is displayed in the log

Clicking a record in the results list opens a window listing the Audit Event details associated with this action.

Parameter List			
ID	585347	Start Time	19-Oct-2016 13:49
Type	User Accepted Login Disclaimer	Source	Concerto
Message	Terms of Use		
Result	Success		
Session ID	CC424B34-24E9-4449-A031-88F4C47A18D3	Terminal ID	10.41.0.98
User ID	Susan.TesterCPO	Patient ID Type	Patient.Id.MPI

Audit Event Parameters	
Name	Value
ConcertoAccount	AF9395BA-F5C3-49B1-B7D4-9EF13EF28994
code	48203323-7b83-4865-8184-05ca950187a8
disclaimerName	Terms of Use
lastUpdatedTime	2016-05-04 15:10:12.209
userOrgs	
userOrgsDesc	
userRoles	Central Privacy Officer;
version	5

Close

EXAMPLE OF AN AUDIT EVENT

The screenshot above indicates that the 'Susan.TesterCPO' user accepted the login disclaimer on October 19, 2016 at 13:49.

Please note that while the Clinical Log is an excellent source of detailed information about user activities in IAR, it may be challenging to interpret until the privacy officer becomes accustomed to reviewing it. For more help understanding the Clinical Log, please refer to:

1. The Privacy Reports section of this document, which contains pre-determined privacy reports that provide a clearer picture of certain key privacy related activities
2. The audit log event types in Appendix A: Audit Log Event Types, which describes the meaning of the different even types listed in the clinical log.

Current Activity Log

Current Activity Log

User ID: Application: [Update list](#)

Result: ☐ All ☐ Success ☐ Fail

[Search](#) [Reset](#)

Time	User ID	Event Type	Message	Patient ID	ID Type	Patient Name
19 Oct 14:47:57	Susan.TesterCPO	Open Application	IAR - User Homepage, Welcome		Patient.Id.MPI	
19 Oct 14:47:57	Susan.TesterCPO	Open Application	IAR - User Homepage, User Homepage		Patient.Id.MPI	
19 Oct 14:47:56	Susan.TesterCPO	User Accepted Login Disclaimer	Terms of Use		Patient.Id.MPI	
19 Oct 14:47:53	susan.testercpo	Resolve User ID	Susan.TesterCPO		Patient.Id.MPI	
19 Oct 14:47:53	Concerto#BD9EA9...	Join common context			Patient.Id.MPI	
19 Oct 14:47:53	Susan.TesterCPO	Account Validation	Susan.TesterCPO		Patient.Id.MPI	
19 Oct 14:47:53	Susan.TesterCPO	User Authentication	Susan.TesterCPO		Patient.Id.MPI	
19 Oct 14:47:52	susan.testercpo	Resolve User ID	Susan.TesterCPO		Patient.Id.MPI	
19 Oct 14:47:52	Susan.TesterCPO	User Custom Authentication	Custom authentication step required for user		Patient.Id.MPI	
19 Oct 14:47:52	Susan.TesterCPO	User Authentication	Susan.TesterCPO		Patient.Id.MPI	

[Printer Friendly Version](#) | [Download CSV results](#)

CURRENT ACTIVITY LOG

The **Current Activity Log** available from the **Monitoring** menu identifies those users who are currently logged in to the IAR and what they are viewing. If this includes a person's data, the name of the patient and the assessment being viewed is identified. The list automatically displays all events for the organization but a user can choose to filter the list by:

- **User ID:** Enter the ID of the user that is currently accessing the system. If this option is specified, the results include all users currently accessing the system.
- **Application:** Select the IAR application accessed by a user. For example, Context Manager. If this option is specified, the results include all users who accessed this application along with the event performed on the application.
- **Result:** Select the radio button corresponding with the level of detail to be included in the search results:
 - **All:** If selected, all results obtained by a Current Activity Log search are returned: for example all successful and failed user login and/or search attempts
 - **Successful:** If selected, only successful authentications to the IAR and the successful Current Activity Log search attempts are listed in search results
 - **Fail:** If selected, only the results of unsuccessful authentications to the IAR are listed in search results

The Current Activity Log displays the same information as the Clinical Log:

Column Heading	Column Descriptions
Time	The date and time the event occurred
User ID	IAR User ID indicating who performed the activity or event
Event Type	The type of event or activity the user was conducting (e.g., searching for a person, opening an assessment, printing an assessment, changing the password)
Message	Description of the event
Person ID	If the event is related to a client, the client's identifier is displayed as Person ID
Person Name	The client's first and last name
Machine IP/ID	The IP address where the user logged in to the IAR
Organization	The ID and name of the organization the user belongs to
ID Type	The type of Person ID that is displayed in the log

Clicking a record in the results list opens a window listing the Audit Event details associated with this action.

Parameter List			
ID	583860	Start Time	06-Oct-2016 11:10
Type	Open Document	Source	Concerto
Message	RAI-HC - RAI-HC Assessment		
Result	Success		
Patient ID	4237	Patient Name	Knowles Betty
Session ID	75B5AAEA-4601-43EF-BA8E-7FE19EC430E9	Terminal ID	10.41.0.98
User ID	Susan.TesterViewer	Patient ID Type	Patient.Id.MPI
Audit Event Parameters			
Name	Value		
ConcertoAccount	08692EAD-3579-4B17-9F3E-1F95212FC7D3		
Patient ID	4237		
Patient ID Type	[hl7.org]Patient.Id.[hl7.org]MPI		
Patient.Co.DateOfBirth	19280202000000-0500		
Patient.Co.PatientName	Knowles^Betty^M^A^A^A^A		
Patient.Co.Sex	F		
Patient.Id.MPI	4237		
Patient.Id.MRN	client5455781RAI-MDS_2.0^781;5551RAI-CHA^651;client5005OCAN^396;11001RAI-HC^763;11001RAI-CA^345		
applicationName	IAR - Assessments		
author	CCAC		
category	RAI-HC Assessment		
date	15 Nov 2015 12:00 AM		
documentId	384335		
documentPrintType			
documentRepositoryName	RAI-HC - Assessments		
documentViewName	Assessment Documents		
documentViewType	Summary		
service	RAI-HC Assessment		
status	Final		
subcategory			
title	RAI-HC - RAI-HC Assessment		
url	/concerto/ApplicationRedirector.htm?applicationName=IAR - Assessments&entryPointName=RAI-HC-Form&ID=384335&ViewerConfig=RAI-HC-Assessment&cViewerType=		
userOrgs	345		
userOrgsDesc	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION		
userRoles	Viewer;		
version			

EXAMPLE OF AN AUDIT EVENT

The screenshot above indicates that the **'Susan.TesterViewer'** User ID successfully opened an RAI-HC Assessment for a particular patient on October 6, 2016 at 11:10.

System Log

Time	User ID	Event Type	Message	Session ID	IP Address
19 Oct 15:00:35	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Audit Event Details	2A80388D-966D-4973-AEBA-60A5B2F90101	10.41.0.98
19 Oct 15:00:18	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Audit Event Details	2A80388D-966D-4973-AEBA-60A5B2F90101	10.41.0.98
19 Oct 14:59:55	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Audit Event Details	2A80388D-966D-4973-AEBA-60A5B2F90101	10.41.0.98
19 Oct 14:59:43	Susan.TesterCPO	Search Performed	Integrated Assessment Repository, Clinical Log	2A80388D-966D-4973-AEBA-60A5B2F90101	10.41.0.98
19 Oct 14:59:38	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Clinical Log	2A80388D-966D-4973-AEBA-60A5B2F90101	10.41.0.98
19 Oct 14:59:38	Susan.TesterCPO	Open Application	Integrated Assessment Repository, Role Based Clinical Log	2A80388D-966D-4973-AEBA-60A5B2F90101	10.41.0.98

SYSTEM LOG FILE

The **System Log** available from the **Monitoring** menu displays a list of server and/or database activities, plus all successful and unsuccessful login attempts by users. The following filter criteria are available:

- **User ID:** Enter the ID of the user that performed an event on the server or database.
- **Result:** Select the radio button corresponding with the level of detail to be included in the search results:
 - **All:** If selected, all results obtained by a System Log search are returned: for example all successful and failed user login and/or search attempts
 - **Successful:** If selected, only successful authentications to the IAR and the successful System Log search attempts are listed in search results
 - **Fail:** If selected, only the results of unsuccessful authentications to the IAR are listed in search results
- **A Particular Date Range:** If this option is specified, the results include all events that occurred within this date range.
- **Server Events:** Select the event performed on the server from the following options (hold the **Ctrl** key down for multiple selections):
 - **Start Up:** The IAR session started
 - **Shut Down:** The IAR session was terminated

- **Database Events:** Select the event performed on the database from the following options (hold the **Ctrl** key down for multiple selections):
 - **Database Import:** The user restored the configuration by importing it from a file
 - **Database Export:** The user exported the configuration to a file
 - **Database Merge:** The user merged the configuration with the information in a merge file

The System Log displays the following information:

Column Heading	Column Descriptions
Time	The date and time the event occurred
User ID	IAR User ID indicating who performed the activity or event
Event Type	The type of event or activity the user was conducting (e.g., searching for a person, opening an assessment, printing an assessment, changing the password)
Message	Description of the event/activity
Session ID	The ID of the user session with IAR, which can used to associate all of a user's activities within one login session
IP Address	The IP address where the user logged in to the IAR

Printing or Downloading the Search Results

The results of a particular monitoring log may be printed or saved by selecting the appropriate link (**Printer Friendly Version** or **Download CSV results**) at the bottom of the search results screen.

[Printer Friendly Version](#) | [Download CSV results](#)

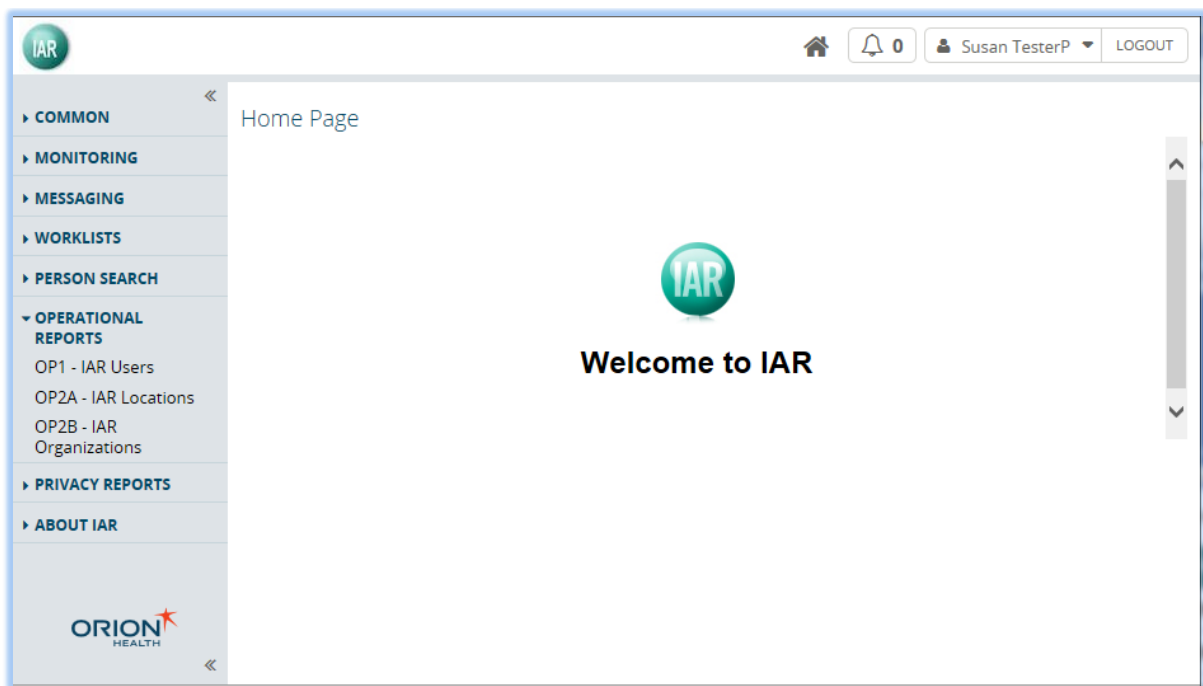
Note: Should a user download a monitoring log (or privacy or operational report) to a CSV file to MS Excel, the user may notice that some French characters are not properly displayed (as the IAR uses UTF-8 for character encoding but MS Excel does not have automatic encoding detection and assumes standard MS Windows encoding). To view properly displayed French characters, complete the following steps:

1. Save the CSV file
2. Open MS Excel
3. Click on **Data** from the menu ribbon at the top of the screen
4. Under the 'Get External Data' options, click on the **From Text** icon
5. Browse to the CSV file you saved in step 1 – make sure you have 'All Files' selected
6. Click the **Import** button
7. Under the 'File origin' drop down, select '65001: Unicode (UTF-8)
8. Click the **Finish** button

Operational Reports

A privacy officer can generate pre-defined operational reports for reviewing users' activities associated with his or her organization(s). IAR provides privacy officers with access to the following Operational Reports:

- OP1 – IAR Users
- OP2A – IAR Locations
- OP2B – IAR Organizations



OP1 – IAR Users

The **OP1 – IAR Users** under the **Operational Report** menu displays a list of users associated with the HSP that the privacy officer belongs to. The privacy officer can select the **Search Button** without entering any search criteria; IAR will return a list of the user accounts associated with the HSP(s) the privacy officer belongs to.

The privacy officer can also enter search criteria to filter the list by User ID, User Status, or login dates.

The privacy officer can only view user accounts inside of his/her HSP. The list of user accounts is sorted first by their roles, and then their User IDs.

OP1 - IAR Users

Organization: ALPHA COURT NON-PROFIT HOUSING CORPORATION (selected) LHIN: [search]

User Status: All (dropdown)

Role: [dropdown]

Last Login Date: From: [calendar] To: [calendar]

☒ Include Users Who Never Logged In

☐ Show Only Users Who Never Logged In (override)

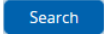
Search Reset

Organization ID	Organization Name	LHIN	Role	User ID	UserName	User Status	Last Successful Login	Email Address	Total Logins	Total Person Searches
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Business Reporting	Susan.TesterBusRep	TesterB, Susan	Enabled	27 Sep 2016 12:53:14		1	0
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Central Privacy Officer	cpo345_MP1-renamed	officer, central privacy	Enabled	16 Mar 2016 13:32:00	manuela.palcu@ccim.on.ca	0	0
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Central Privacy Officer	cpo_DK		Enabled	01 Nov 2013 09:26:23		3	0
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Central Privacy Officer	cuv_JH2	Privacy Officer, Central	Deleted	11 May 2016 22:29:02		1	0

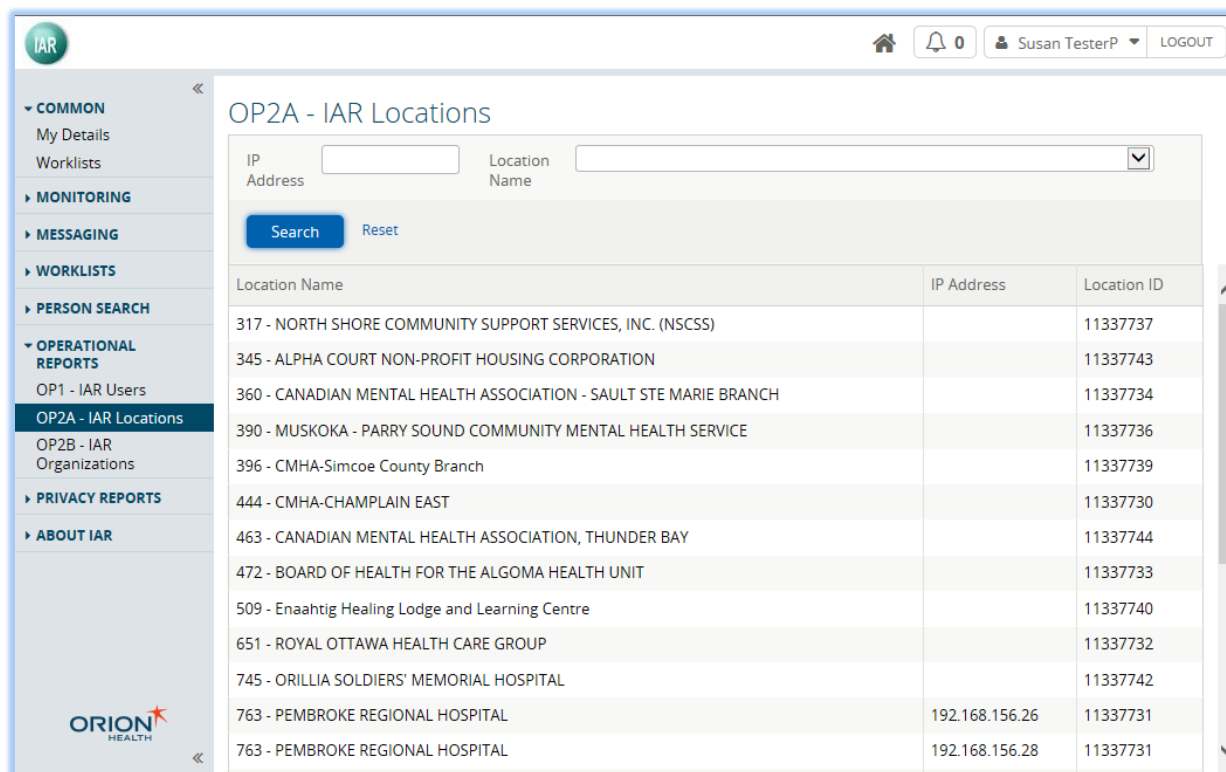
Description of Columns:

Column Heading	Column Descriptions
Organization ID	The ID of the Organization
Organization Name	The Name of Organization the user belongs to
LHIN	The LHIN that the organization belongs to
Role	The role of the user, (e.g. viewer, privacy officer or uploader)
User ID	IAR User ID
User Name	User's first and last name
User Status	User's status details (i.e. enabled or disabled)
Last Successful Login	User's last successful login date and time
Email Address	User's email address
Total Logins	Total number of times the user logged in to IAR over the selected time range
Total Person Searches	Total number of searches for clients over the selected time range

OP2A – IAR Locations

The **OP2A – IAR Locations** under the **Operational Reports** menu displays a list of locations from where the user will access the IAR. The report displays information about each participating organization. By default, the privacy officer can click **Search Button**  and view the information on all participating HSPs.

Alternatively, the privacy officer can also filter the list by entering the IP Address or Location Name as search criteria.





Location Name	IP Address	Location ID
317 - NORTH SHORE COMMUNITY SUPPORT SERVICES, INC. (NSCSS)		11337737
345 - ALPHA COURT NON-PROFIT HOUSING CORPORATION		11337743
360 - CANADIAN MENTAL HEALTH ASSOCIATION - SAULT STE MARIE BRANCH		11337734
390 - MUSKOKA - PARRY SOUND COMMUNITY MENTAL HEALTH SERVICE		11337736
396 - CMHA-Simcoe County Branch		11337739
444 - CMHA-CHAMPLAIN EAST		11337730
463 - CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY		11337744
472 - BOARD OF HEALTH FOR THE ALGOMA HEALTH UNIT		11337733
509 - Enahtig Healing Lodge and Learning Centre		11337740
651 - ROYAL OTTAWA HEALTH CARE GROUP		11337732
745 - ORILLIA SOLDIERS' MEMORIAL HOSPITAL		11337742
763 - PEMBROKE REGIONAL HOSPITAL	192.168.156.26	11337731
763 - PEMBROKE REGIONAL HOSPITAL	192.168.156.28	11337731

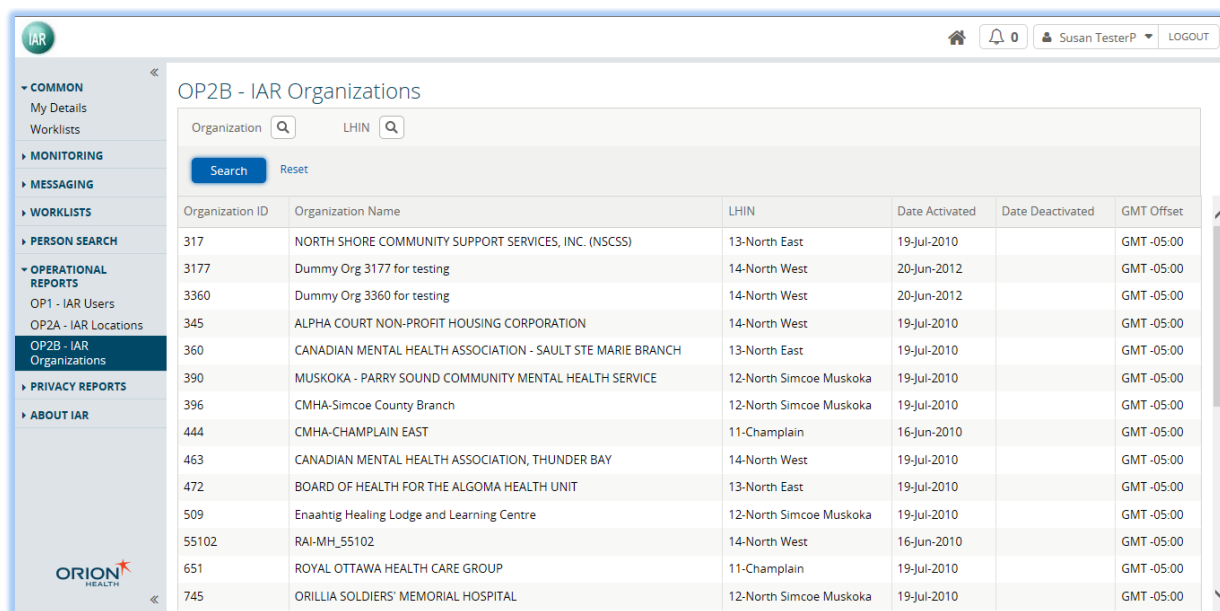
Description of Columns:

Column Heading	Column Descriptions
Location Name	The locations from which user accesses IAR
IP Address	Authorized IP address for the location. IAR will only accept user access from the authorized IP address.
Location ID	The ID of the location

OP2B – List of IAR Organizations

The **OP2B – List of IAR Organizations** under the **Operational Report** menu displays a list of organizations who participate in the IAR. The report displays information about each participating organization. By default, the privacy officer can click the **Search Button**  and view the information on all participating HSPs.

Alternatively, the privacy officer can also filter the list by selecting Organization or LHIN from the **Search Icon**  as search criteria.



Organization ID	Organization Name	LHIN	Date Activated	Date Deactivated	GMT Offset
317	NORTH SHORE COMMUNITY SUPPORT SERVICES, INC. (NSCSS)	13-North East	19-Jul-2010		GMT -05:00
3177	Dummy Org 3177 for testing	14-North West	20-Jun-2012		GMT -05:00
3360	Dummy Org 3360 for testing	14-North West	20-Jun-2012		GMT -05:00
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	19-Jul-2010		GMT -05:00
360	CANADIAN MENTAL HEALTH ASSOCIATION - SAULT STE MARIE BRANCH	13-North East	19-Jul-2010		GMT -05:00
390	MUSKOKA - PARRY SOUND COMMUNITY MENTAL HEALTH SERVICE	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00
444	CMHA-CHAMPLAIN EAST	11-Champlain	16-Jun-2010		GMT -05:00
463	CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY	14-North West	19-Jul-2010		GMT -05:00
472	BOARD OF HEALTH FOR THE ALGOMA HEALTH UNIT	13-North East	19-Jul-2010		GMT -05:00
509	Enaahitig Healing Lodge and Learning Centre	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00
55102	RAI-MH_55102	14-North West	16-Jun-2010		GMT -05:00
651	ROYAL OTTAWA HEALTH CARE GROUP	11-Champlain	19-Jul-2010		GMT -05:00
745	ORILLIA SOLDIERS' MEMORIAL HOSPITAL	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00

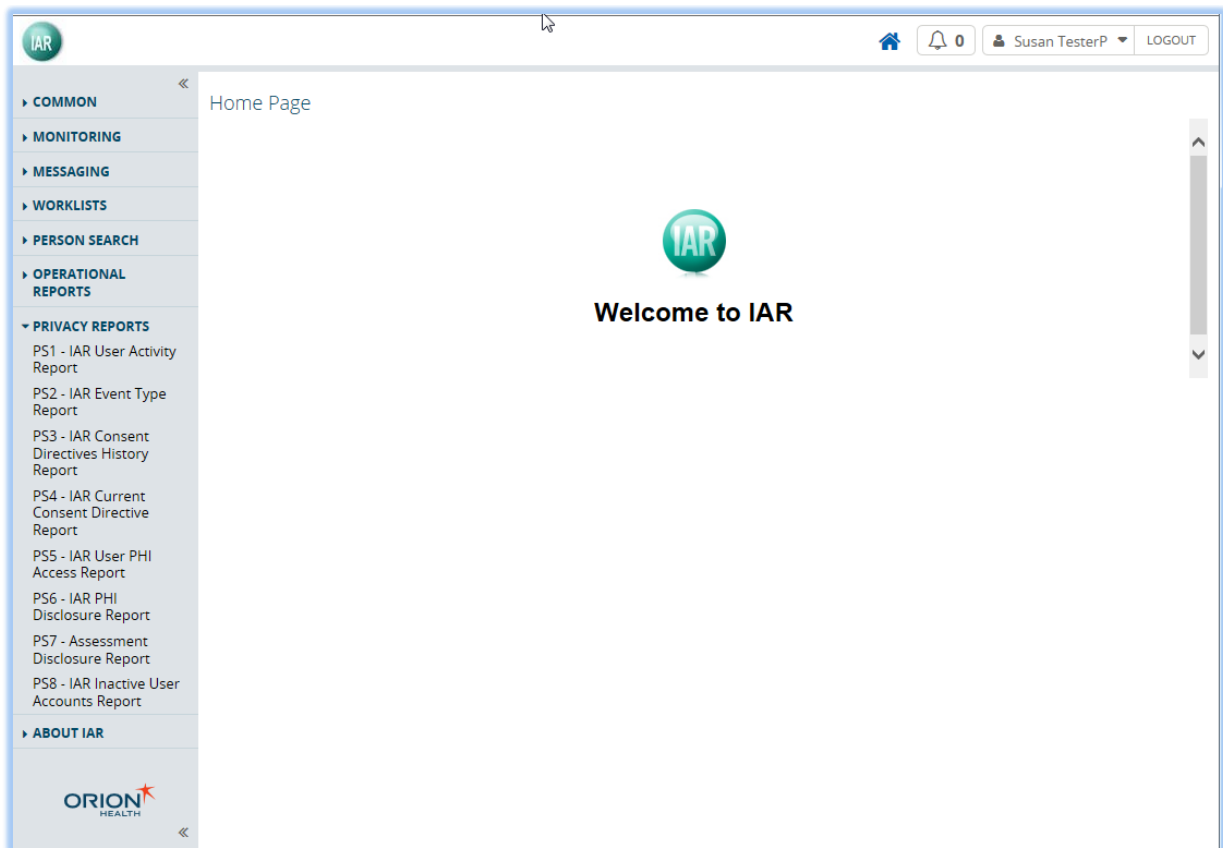
Description of Columns:

Column Heading	Column Descriptions
Organization ID	The ID of the organization
Organization Name	The name of organization
LHIN	The LHIN that the organization belongs to
Date Activated	The date this organization was activated in IAR
Date Deactivated	The date this organization was deactivated from IAR
GMT Offset	Time zone as related to GMT


Privacy Reports

For the privacy officer's convenience, a privacy officer can generate pre-defined privacy reports for auditing all privacy related events associated within his or her organization. Since the Clinical Log may be challenging to review, IAR provides privacy officers access to the following pre-determined Privacy Reports for auditing of key privacy related events:

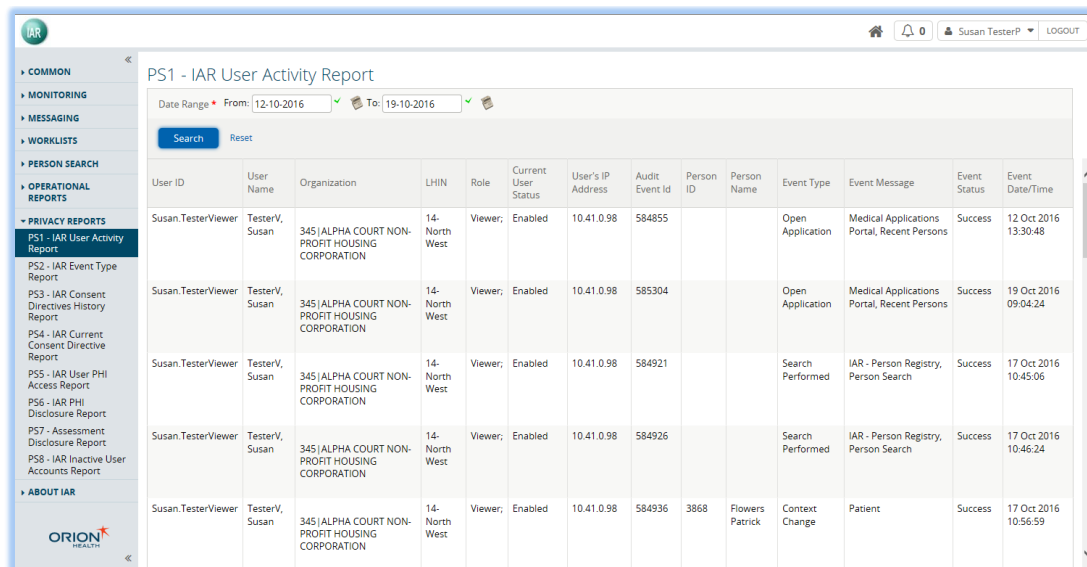
- PS1 – IAR User Activity Report
- PS2 – IAR Event Type Report
- PS3 – IAR Consent Directives History Report
- PS 4 – IAR Current Consent Directive Report
- PS5 – IAR User PHI Access Report
- PS6 – IAR PHI Disclosure Report
- PS7 – Assessment Disclosure Report
- PS8 – IAR Inactive User Accounts Report



PS1 – IAR User Activity Report

The **PS1 – IAR User Activity Report** under the **Privacy Report** menu displays all activities performed by users associated with the privacy officer's HSP(s). The privacy officer can select the **Search Button**  without entering any search criteria, and IAR will return a list of logged audit events on a user-by-user basis. The privacy officer can also provide a different "from" date and "to" date to view the activities in the specified period of time. By default, the date range is the last seven days.

Note: The number of activities (i.e., audit events) could be very large. The privacy officer should always choose reasonable "from" and "to" dates to limit the number of activities displayed in the report.



User ID	User Name	Organization	LHIN	Role	Current User Status	User's IP Address	Audit Event Id	Person ID	Person Name	Event Type	Event Message	Event Status	Event Date/Time
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Viewer	Enabled	10.41.0.98	584855			Open Application	Medical Applications Portal, Recent Persons	Success	12 Oct 2016 13:30:48
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Viewer	Enabled	10.41.0.98	585304			Open Application	Medical Applications Portal, Recent Persons	Success	19 Oct 2016 09:04:24
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Viewer	Enabled	10.41.0.98	584921			Search Performed	IAR - Person Registry, Person Search	Success	17 Oct 2016 10:45:06
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Viewer	Enabled	10.41.0.98	584926			Search Performed	IAR - Person Registry, Person Search	Success	17 Oct 2016 10:46:24
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	Viewer	Enabled	10.41.0.98	584936	3868	Flowers Patrick	Context Change	Patient	Success	17 Oct 2016 10:56:59

Description of Columns:

Column Heading	Column Descriptions
User ID	IAR User ID
User Name	User's first and last name
Organization	The name of the organization the user belongs to
LHIN	The LHIN that the organization belongs to
Role	The role of the user, (e.g. viewer, privacy officer or uploader)
Current User Status	User's current status (i.e. enabled or disabled)
User's IP Address	User's IP address (i.e. which physical computer the user was accessing IAR from)
Audit Event Id	A unique identifier for this audit event record
Person ID	The client's identifier that the user has accessed
Person Name	The client's first and last name
Event Type	The type of event or activity the user was conducting (search for a person, opening an assessment, printing an assessment, changing the password, etc.)
Event Message	Event message from IAR
Event Status	Event status (i.e. successful or failed)
Event Date/Time	The date and time the event occurred

PS2 – IAR Event Type Report

The **PS2 – IAR Event Type Report** under the **Privacy Report** menu displays login events for a specified period of time for all of the HSP's users. The privacy officer can choose three types of login events (All Logins, Failed Logins, and Successful Logins) and a specified period of time by choosing the Date Range and Event Status as search criteria. By default, the date range is the last seven days.

The screenshot shows the 'PS2 - IAR Event Type Report' interface. The sidebar on the left contains navigation links: COMMON, MONITORING, MESSAGING, WORKLISTS, PERSON SEARCH, OPERATIONAL REPORTS, and ABOUT IAR. Under OPERATIONAL REPORTS, there are links for PS1 - IAR User Activity Report, PS2 - IAR Event Type Report (highlighted), PS3 - IAR Consent Directives History Report, PS4 - IAR Current Consent Directive Report, PS5 - IAR User PHI Access Report, PS6 - IAR PHI Disclosure Report, PS7 - Assessment Disclosure Report, and PS8 - IAR Inactive User Accounts Report. The main content area has a title 'PS2 - IAR Event Type Report' and search filters: Date Range (From: 12-10-2016, To: 19-10-2016), Event Status (All Logins), and buttons for Search and Reset. Below the filters is a table with the following data:

User ID	User Name	Organization	LHIN	Role	Status	IP Address	Audit Event Id	Event Type	Event Message	Event Status	Event Date/Time
Susan.TesterPrivacyOfficer	TesterP, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396 CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	585427	User Authentication	Susan.TesterPrivacyOfficer	Success	19 Oct 2016 17:26:54
Susan.TesterPrivacyOfficer	TesterP, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396 CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	585397	User Authentication	Susan.TesterPrivacyOfficer	Success	19 Oct 2016 15:16:51
Susan.TesterPrivacyOfficer	TesterP, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396 CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	585391	User Authentication	Susan.TesterPrivacyOfficer	Invalid login attempt	19 Oct 2016 15:16:28
Susan.TesterPrivacyOfficer	TesterP, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396 CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584862	User Authentication	Susan.TesterPrivacyOfficer	Success	12 Oct 2016 15:16:55

Description of Columns:

Column Heading	Column Descriptions
User ID	IAR User ID
User Name	User's first and last name
Organization	The name of the organization the user belongs to
LHIN	The LHIN that the organization belongs to
Role	The role of the user, (e.g. viewer, privacy officer or uploader)
Status	User's current status (i.e. enabled or disabled)
IP Address	User's IP address (i.e. which physical computer the user was accessing IAR from)
Audit Event Id	An unique identifier for this audit event record
Event Type	The type of event or activity the user was conducting
Event Message	Event message from IAR
Event Status	Event status (i.e. successful or failed)
Event Date/Time	The date and time the event occurred

PS3 – IAR Consent Directives History Report

The **PS3 – IAR Consent Directives History Report** under the **Privacy Report** menu displays a list of both IAR and HSP level consent directives (i.e., Grant or Deny) that happened within a specified period of time. Based on the selected User ID and date/time range, the report shows all consent directives requested by this client. Updates in the IAR during the specified period are also provided.

The Privacy Officer can only generate the report for the client associated with the HSPs the Privacy Officer works for. The Privacy Officer can generate the report by searching for a client and specifying the Date Range as search criteria.

Organization ID	Organization Name	Person ID	Person Name	Alias Name	Consent Directive Type	Assessment ID	Consent Directive	Data Feed Support	Request Date	Effective Date
IAR		4232	Linson, Ashley		IAR		GRANT			04 Oct 2016 14:49:51
IAR		4232	Linson, Ashley		IAR		DENY			04 Oct 2016 14:39:43
IAR		4232	Linson, Ashley		IAR		GRANT			04 Oct 2016 14:39:29
IAR		4232	Linson, Ashley		IAR		GRANT			04 Oct 2016 11:17:28
IAR		4232	Linson, Ashley		IAR		GRANT			04 Oct 2016 11:14:36
IAR		4232	Linson, Ashley		IAR		GRANT			04 Oct 2016 11:14:01
IAR		4232	Linson, Ashley		IAR		DENY			04 Oct 2016 11:13:25
IAR		4232	Linson, Ashley		IAR		GRANT			04 Oct 2016 11:13:05
IAR		4232	Linson, Ashley		IAR		DENY			04 Oct 2016 11:11:25

Description of Columns:

Column Heading	Column Descriptions
Organization ID	The ID of the organization associated with the HSP level consent directive
Organization Name	The name of the organization associated with the HSP level consent directive
Person ID	The client's identifier
Person Name	The client's first and last name
Alias Name	The client's alias, if available
Consent Directive Type	The type of consent directive (i.e., HSP, IAR, PI)
Assessment ID	Client's assessment ID associated with the HSP level consent directive
Consent Directive	The consent directive requested (i.e., Grant or Deny)
Data Feed Support	This field indicates supported or not supported for HSP level consent directives Note: Unsupported consent directives are no longer applicable in the IAR
Request Date	The date and time the HSP consent directive was submitted by the organization
Effective Date	The date and time the consent directive became effective in the IAR

PS4 – IAR Current Consent Directive Report

The **PS4 – IAR Current Consent Directive Report** under the **Privacy Report** menu displays a list of current consent directives (i.e., Granted or Deny) for a specified client. If the client has never requested or changed their consent directive, default consent is 'Grant' and not presented in this report. Therefore, if this report does not display the HSP level consent directive, it indicates that the client has consented to share those assessments in the IAR.

PS4 - IAR Current Consent Directive Report

Person Search

Organization ID	Organization Name	Person ID	Person Name	Alias Name	Consent Directive Type	Assessment ID	Consent Directive	Data Feed Support	Request Date	Effective Date
396	CMHA-Simcoe County Branch	100230CAN	Linson, Ashley		HSP	2255	GRANT	SUPPORTED	06 Dec 2014	06 Dec 2014 09:30:47
IAR		4232	Linson, Ashley		GRANT		IAR			04 Oct 2016 14:49:51

Results 1-2 [Printer Friendly Version](#) [Download CSV results](#)

IAR Audit Reports Disclaimer: This audit report may contain personal information or personal health information and must be protected accordingly. This information may not be used, reproduced, stored, or disclosed to others in any format or by any means without a business need and appropriate authorization based on your organization's policies. The recipient of this information, by its retention and use, agrees to protect this information from any loss, theft, or compromise. This disclaimer must not be removed from the report

Description of Columns:

Column Heading	Column Descriptions
Organization ID	The ID of the organization associated with the HSP level consent directive
Organization Name	The name of the organization associated with the HSP level consent directive
Person ID	The client's identifier
Person Name	The client's first and last name
Alias Name	The client's alias, if available
Consent Directive Type	The type of consent directive (i.e., HSP, IAR, PI)
Assessment ID	Client's assessment ID associated with the HSP level consent directive
Consent Directive	The consent directive requested (i.e., Grant or Deny)
Data Feed Support	This field indicates supported or not supported for HSP level consent directives Note: Unsupported consent directives are no longer applicable in the IAR
Request Date	The date and time the HSP level consent directive was submitted by the organization
Effective Date	The date and time the consent directive became effective in the IAR

PS5 – IAR User PHI Access Report

The **PS5 – IAR User PHI Access Report** under the **Privacy Report** menu displays a list of all Personal Health Information (PHI) accessed by a specified IAR user. Based on the selected User ID and date/time range, the report shows which person or client, as well as which assessments that selected user has reviewed or accessed. This report is focused on access related events; meaning events where either the PHI and/or the assessments were viewed.

For this report, the privacy officer can only select a User ID associated with the privacy officer's HSP(s). The privacy officer can filter the events by selecting the User ID and specifying the Date Range as search Criteria.

User ID	User Name	Role	Current User Status	Organization	LHIN	User's IP Address	Person ID	Person Name	Assessment ID	Audit Event Id	Event Type	Event Message	Event Status	Event Date/Time
Susan.TesterViewer	TesterV, Susan	Viewer	Enabled	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14- North West	10.41.0.98	3868	Flowers Patrick	3371-32	584942	Open Document	Coord. Care Plan	Success	17 Oct 2016 10:57:26
Susan.TesterViewer	TesterV, Susan	Viewer	Enabled	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14- North West	10.41.0.98	3868	Flowers Patrick	3371-32	584975	Open Document	Coord. Care Plan	Success	17 Oct 2016 13:21:07
Susan.TesterViewer	TesterV, Susan	Viewer	Enabled	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14- North West	10.41.0.98	3868	Flowers Patrick	3371-32	585049	Open Document	Coord. Care Plan	Success	17 Oct 2016 15:29:40
Susan.TesterViewer	TesterV, Susan	Viewer	Enabled	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14- North West	10.41.0.98	3868	Flowers Patrick	3371-32	585089	Open Document	Coord. Care Plan	Success	18 Oct 2016 09:51:17
Susan.TesterViewer	TesterV, Susan	Viewer	Enabled	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14- North West	10.41.0.98	3868	Flowers Patrick	3371-32	584936	Context	Patient	Success	17 Oct 2016 10:57:26

Description of Columns:

Column Heading	Column Descriptions
User ID	IAR User ID
User Name	User's first and last name
Role	The role of the user (e.g. viewer, privacy officer or uploader)
Current User Status	User's current status (i.e. enabled or disabled)
Organization	The name of the organization the user belongs to
LHIN	The LHIN that the organization belongs to
User's IP Address	User's IP address (i.e. which physical computer the user was accessing IAR from)
Person ID	The client's identifier that the user has accessed
Assessment ID	Client's assessment ID that the user has accessed
Audit Event Id	A unique identifier for this audit event record
Event Type	The type of event or activity the user was conducting
Event Message	Event message from IAR
Event Status	Event status (i.e. successful or failed)
Event Date/Time	The date and time the event occurred

PS6 – IAR PHI Disclosure Report

The **PS6 – IAR PHI Disclosure Report** under the **Privacy Report** menu displays a list of users who have looked at a given client's assessment. The privacy officer must specify a client by clicking the Search Icon and select the Date Range to generate this report. Based on the selected patient ID and date range, IAR will present which user from which organization has accessed this selected patient's assessment records uploaded by the current organization.

PS6 - IAR PHI Disclosure Report

Person Search: Flowers, Patrick; LadyPatrick Date Range: From: 12-10-2016 To: 19-10-2016

User ID	User Name	Organization	LHIN	User's IP Address	Person ID	Person Name	Assessment ID	Audit Event Id	Event Type	Event Message	Event Status	Event Date/Time
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-31	585502	Open Document	Coord. Care Plan	Success	19 Oct 2016 18:23:53
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-31	585504	Open Document	Coord. Care Plan	Success	19 Oct 2016 18:24:08
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-31	585506	Print Request	Coord. Care Plan	Success	19 Oct 2016 18:24:08
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-32	584942	Open Document	Coord. Care Plan	Success	17 Oct 2016 10:57:26
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-32	584975	Open Document	Coord. Care Plan	Success	17 Oct 2016 13:21:07
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-32	585049	Open Document	Coord. Care Plan	Success	17 Oct 2016 15:29:40
Susan.TesterViewer	TesterV, Susan	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	14-North West	10.41.0.98	3868	Flowers Patrick	3371-32	585089	Open Document	Coord. Care Plan	Success	18 Oct 2016 09:51:17

Results 1-7 Download CSV results

IAR Audit Reports Disclaimer: This audit report may contain personal information or personal health information and must be protected accordingly. This information may not be used, reproduced, stored, or disclosed to others in any format or by any means without a business need and appropriate authorization based on your organization's policies. The recipient of this information, by its retention and use, agrees to protect this information from any loss, theft, or compromise. This disclaimer must not be removed from the report.

Description of Columns:

Column Heading	Column Descriptions
User ID	IAR User ID
User Name	First and last name if the user
Organization	The name of the organization the user belongs to
LHIN	The LHIN that the organization belongs to
User's IP Address	User's IP address (i.e. which physical computer the user was accessing IAR from)
Person ID	The client's identifier that the user has accessed
Person Name	The client's name that the user has accessed
Assessment ID	Client's assessment ID that the user has accessed
Audit Event Id	A unique identifier for this audit event record
Event Type	The type of event or activity the user was conducting
Event Message	Event message from IAR
Event Status	Event status (i.e. successful or failed)
Event Date/Time	The date and time the event occurred

PS7 – Assessment Disclosure Report

The **PS7 – Assessment Disclosure Report** under the **Privacy Report** menu displays disclosures of personal health information. A disclosure is defined as PHI that is viewed by users outside the organization's policies and procedures. PS7 only shows users from outside of the privacy officer's organization who have accessed patient's assessments uploaded from the current organization.

Unlike PS6, this report is generated by date range, or date range and the name of an organization in which the privacy officer is interested if that particular organization has been able to access the assessments they have uploaded.

User ID	User Name	User Organization	LHIN	IP Address	Person ID	Person Name	Assessment ID	Assessment Organization	Event Type	Event Message	Event Status	Event Date/Time
Slava	, Yaroslav	360 CANADIAN MENTAL HEALTH ASSOCIATION - SAULT STE MARIE BRANCH; 463 CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY; 763 PEMBROKE REGIONAL HOSPITAL NewName:Concerto	-	10.21.202.72	1618	Kirillov Kirill	-	-	Context Change	Patient	Success	29 Aug 2016 13:59:44
Slava	, Yaroslav	360 CANADIAN MENTAL HEALTH ASSOCIATION - SAULT STE MARIE BRANCH; 463 CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY; 763 PEMBROKE REGIONAL HOSPITAL NewName:Concerto	-	10.21.202.72	1618	Kirillov Kirill	345HC201114	345-ALPHA COURT NON-PROFIT HOUSING CORPORATION	Open Document	RAI-HC - ER Visits	Success	29 Aug 2016 14:06:45
cuv	uploader/viewer, ccm	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION; 463 CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY; 360 CANADIAN MENTAL HEALTH ASSOCIATION - SAULT STE MARIE BRANCH; 396 CMHA-Simcoe County Branch;	-	10.21.202.72	3916	Graves Shelly	-	-	Context Change	Patient	Success	30 May 2016 11:38:13

Description of Columns:

Column Heading	Column Descriptions
User ID	IAR User ID
User Name	First and last name if the user
User Organization	The name of the organization the user belongs to
LHIN	The LHIN that the organization belongs to
IP Address	User's IP address (i.e. which physical computer the user was accessing IAR from)
Person ID	The client's identifier that the user has accessed
Person Name	The client's name that the user has accessed
Assessment ID	Client's assessment ID that the user has accessed
Assessment Organization	Organization that conducted the assessment
Event Type	The type of event or activity the user was conducting
Event Message	Event message from IAR
Event Status	Event status (i.e. successful or failed)
Event Date/Time	The date and time the event occurred

PS8 – Inactive User Report

The **PS8 – Inactive User Report** under the **Privacy Report** menu displays users who have not logged in for more than 90 days.

The report provides the privacy officer the opportunity to review user's last account login date. If a user has not logged in for more than 90 days, the privacy officer should review it with the user's manager to ensure that the user needs the account in IAR or if the user should be removed from the IAR.


User ID	User Name	User Role	User Account Creation Date	Last Successful Login Date	Days of Inactivity	Is User Account Disabled
AIPrivacyLocal		Privacy Officer	23 Oct 2012 14:38:13	17 Mar 2014 15:19:03	947	No
AIPrivacyLocal		Privacy Officer	23 Oct 2012 14:38:13	17 Mar 2014 15:19:03	947	No
Austin		Viewer	20 Nov 2013 14:59:47		1064	No
Austin		Uploader	20 Nov 2013 14:59:47		1064	No
AustinH		Viewer	25 Nov 2013 15:14:14	26 May 2015 15:43:19	512	No
AustinH		Uploader	25 Nov 2013 15:14:14	26 May 2015 15:43:19	512	No
Oneidqaiar.privacy		Privacy Officer	12 Feb 2014 17:06:55	20 Feb 2014 12:27:25	972	Yes
Oneidqaiar.uploader@oneid.on.ca		Uploader	07 Feb 2014 16:32:02	19 Feb 2014 14:44:06	973	No
Oneidqaiar.viewer		Viewer	12 Feb 2014 17:02:13	24 Feb 2014 11:15:48	968	No
Oneidqaiar.viewer		Uploader	12 Feb 2014 17:02:13	24 Feb 2014 11:15:48	968	No
TestUpload	Test Upload	Uploader	22 Jun 2010 15:30:38		2311	No
TestUpload	Test Upload	Uploader	22 Jun 2010 15:30:38		2311	No
TestUpload	Test Upload	Viewer	22 Jun 2010 15:30:38		2311	No
TestUpload	Test Upload	Viewer	22 Jun 2010 15:30:38		2311	No
TestUpload345		Uploader	28 Jan 2011 09:12:14	28 Jan 2011 15:41:05	2091	Yes

Description of Columns:

Column Heading	Column Descriptions
User ID	IAR User ID
User Name	First and last name if the user
User Role	The role of the user (e.g. viewer, privacy officer or uploader)
User Account Creation Date	The date user account was created in IAR
Last Successful Login Date	The last date on which the user logged in successfully
Days of Inactivity	Number of days since the user's last successful login
Is User Account Disabled	Is the user account active or disabled?

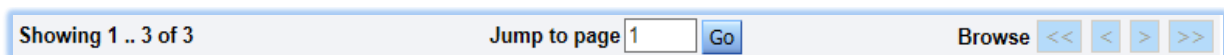
Messaging

The IAR includes a messaging system that allows users to securely exchange information. **Note:** In order to utilize the messaging component of the IAR, the individual must be set up as a user. It is not possible to send or receive messages from individuals who are not users of the IAR.

Received messages may be viewed from the mail icon  6 at the top right of any screen or from the messaging menu.

Received Messages

The navigation bar allows users to browse through pages or jump directly to a specific page.





RECEIVED MESSAGES – NAVIGATION BAR

Received messages may be filtered by selecting one or more of the options from the navigation bar:



RECEIVED MESSAGES – FILTER CRITERIA

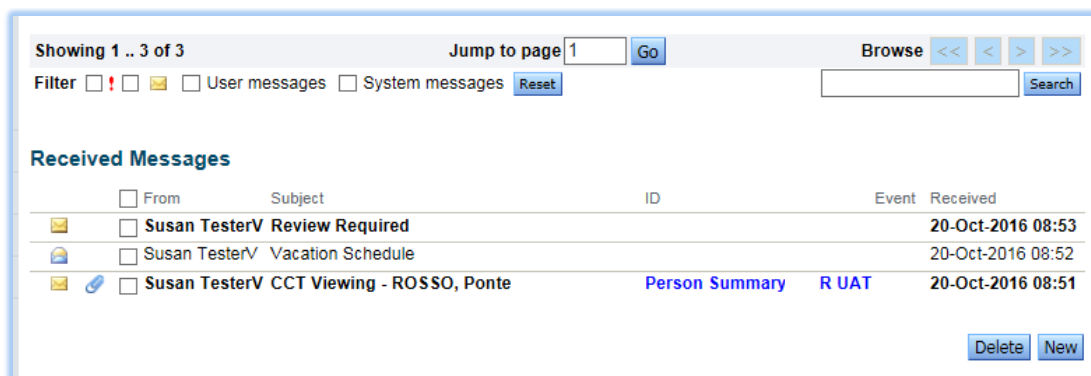
- **Urgent**  **Messages:** Allows a user to view all urgent messages
- **Unread**  **Messages:** Allows a user to view all messages that have not been read
- **User Messages:** Allows a user to view all messages sent by other IAR users
- **System Messages:** Allows a user to view all messages sent by the Administrator
- **Reset:** Allows the user to reset the filter criteria




Users may also perform a text search to identify text in subject line or body of a message. Users can enter the text and then click the **Search** button.







RECEIVED MESSAGES: SEARCH

The following six (6) columns appear on the **Received Messages** screen:



From	Subject	ID	Event	Received
 Susan TesterV	Review Required			20-Oct-2016 08:53
 Susan TesterV	Vacation Schedule			20-Oct-2016 08:52
 Susan TesterV	CCT Viewing - ROSSO, Ponte	Person Summary	R UAT	20-Oct-2016 08:51

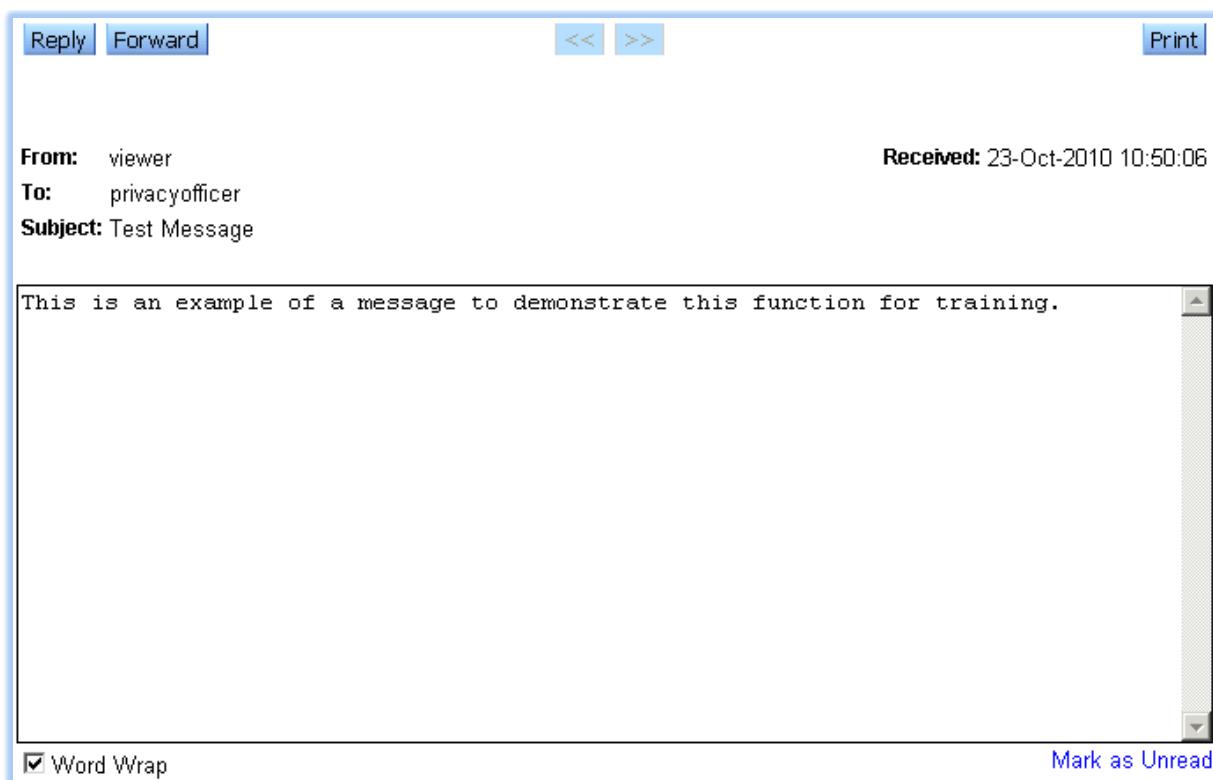
RECEIVED MESSAGES

- **Icons:**
 - The  icon indicates an unread message.
 - The  icon indicates a read message.
 - The  icon indicates an attachment is included in the message.
 - The  icon indicates an important message.
- **From:** Displays the name of the IAR user who sent the message.
- **Subject:** Displays the subject line of the message.
- **ID:** If applicable, provides a link to the Person Summary page for the person identified in the message subject. Note: This applies only to Coordinated Care Plans.
- **Event:** This column is not used by the IAR.
- **Received:** Displays the date the message was received.

Note: Users can sort the list by any column (except icons) by clicking on the column heading link.

From this screen, a user may also delete a message that is no longer required, or send a new message to an IAR user, using the buttons below the message.

When the message is selected, the user may reply to the received message, forward the received message, print the received message and/or mark the message as unread.





Reply Forward << >> Print

From: viewer **Received:** 23-Oct-2010 10:50:06
To: privacyofficer
Subject: Test Message

This is an example of a message to demonstrate this function for training.

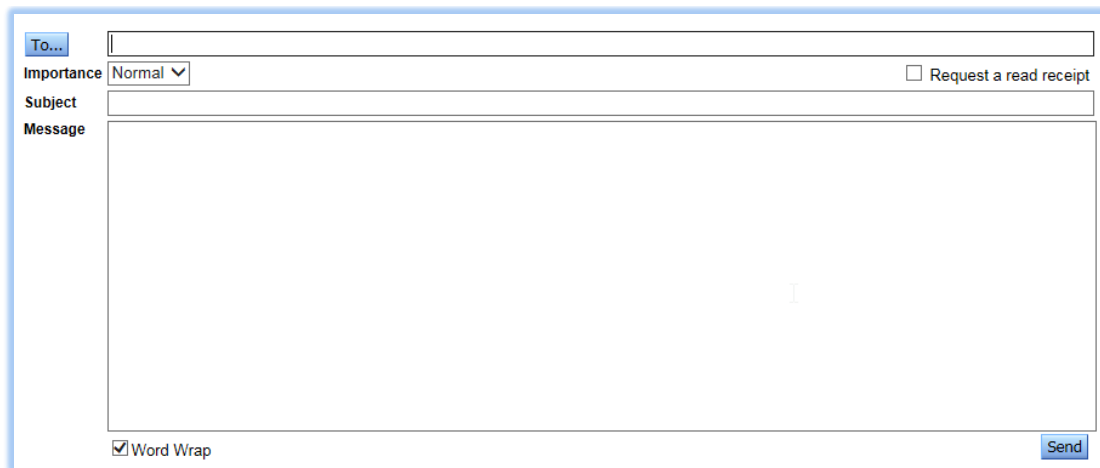
☒ Word Wrap Mark as Unread

SAMPLE RECEIVED MESSAGE

Users may use the navigation   icons to easily view the next or previous received message.

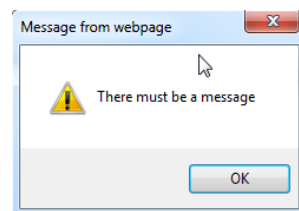
New Messages

Users may send new messages to other IAR users. The recipient's User ID can be typed directly into the **To:** field or, by clicking the **To:** button. A recipient can be identified from the resulting **User Search** screen.



NEW MESSAGE

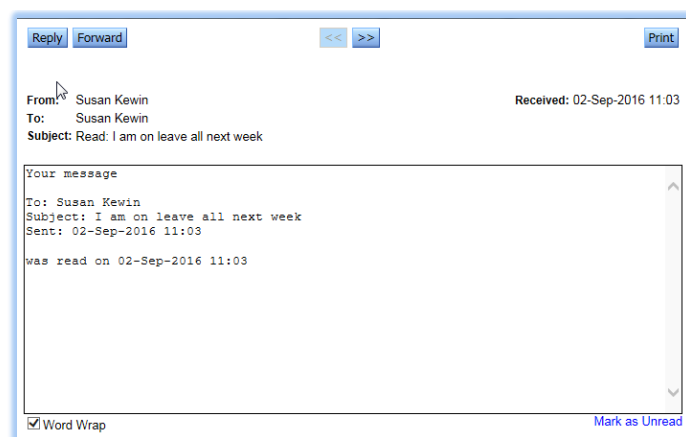
Users can change the message's importance and enter text in the subject the subject field, but users must enter text in the message field before clicking the **Send** button to send the message. An alert is displayed if a user attempts to send a message without any content.



ERROR MESSAGE

Request a Read Receipt




When creating a new message, users can check the 'Request a read receipt' checkbox ☐ Request a read receipt if they would like to receive a message to let them know when the message recipient has read the message.



READ RECEIPT MESSAGE

Sent Messages

Users may view messages they have sent to other IAR users.

Sent Messages		
<input type="checkbox"/> To	Summary	Sent
 <input type="checkbox"/> Susan Kewin	A review of this patient's ...	02-Sep-2016 11:10
 <input type="checkbox"/> Susan Kewin	Please note that I am on va...	02-Sep-2016 11:09
 <input type="checkbox"/> Susan Kewin	This is an example of a mes...	02-Sep-2016 10:49
		<input type="button" value="Delete"/> <input type="button" value="New"/>

SENT MESSAGES

Deleting a Message

A message can be deleted by selecting its associated checkbox and clicking the **Delete** button. Deleting a message must be confirmed and cannot be undone.

Appendix A: Audit Log Event Types

Different Event Types in the Clinical Log

Events	Explanation
User Events	
User Authentication	When IAR displays the username and password screen (1st step in the user login process)
Login	After the user credentials are validated, it is considered a login (3rd step in the user login process)
Logout	User finishes and he/she is logged out from IAR
Account Status Change	User account status change (i.e., active/inactive); for example as a result of multiple unsuccessful logins
Password Change	User changes password on My Details page
Security Change	Not applicable for the IAR installation
Concerto Events	
Open Application	Applications are internal to the IAR, e.g., home page, person demographics, open an assessment document, open an assessment list
Open Document	User opens a specific assessment
Context Change	Change person or patient name in Person Search
Other Events	
Account Validation	After user has provided the username and password, IAR checks if the credentials are correct in the database (2nd step in the user login process)
Add Group Membership	IAR Administrator Activity
Add Role Group Membership	IAR Administrator Activity
Add Role Membership	IAR Administrator Activity
Add mapping agent	IAR Administrator Activity
Assign Privacy Policy	IAR Administrator Activity
Authenticated Login	Not applicable for the IAR installation
Background task	IAR Administrator Activity
Configuration	IAR Administrator Activity
Configure CCOW context manager	IAR Administrator Activity
Copy Entry Point to Application	IAR Administrator Activity
Create Custom Privacy Policy	IAR Administrator Activity
Create Entry Point	IAR Administrator Activity
Create External Identifier Type	IAR Administrator Activity
Create Information Type	IAR Administrator Activity
Create Login Disclaimer	IAR Administrator Activity
Create Role	IAR Administrator Activity
Create User	IAR Administrator Activity
Database Export	IAR Administrator Activity
Database Merge	IAR Administrator Activity
Destroy Entry Point	IAR Administrator Activity
Destroy Information Type	IAR Administrator Activity

Events	Explanation
Download CSV file	User clicks the Download CSV link, generates a CSV file, and opens or saves it on his/her computer
Edit Custom Privacy Policy	IAR Administrator Activity
Edit Login Disclaimer	IAR Administrator Activity
Edit Privacy Policy	IAR Administrator Activity
Join common context	Not applicable for the IAR installation
Leave common context	Not applicable for the IAR installation
Password Reset Request	User requests a password reset (e.g., clicks 'Forgot Your Password?' link from login page or resets his/her password)
Print Request	User selected a PRINT function
Privacy Override	Not applicable for the IAR installation
Privacy prevented user message from being sent	Message notification to user indicating that a message, containing a link to a person and an assessment (i.e., Coordinated Care Plan) was not forwarded to another user(s) due to that person having a consent block
Purged expired Tokens	IAR Administrator Activity
Remove External Identifier Type	IAR Administrator Activity
Remove Group Membership	IAR Administrator Activity
Remove Role	IAR Administrator Activity
Remove Role Membership	IAR Administrator Activity
Remove User	IAR Administrator Activity
Remove mapping agent	IAR Administrator Activity
Rename Entry Point	IAR Administrator Activity
Rename User	IAR Administrator Activity
Reset Custom Privacy Policy	IAR Administrator Activity
Resolve User ID	System verification that the user account exists at time of login
Search Performed	User conducted a person search
Shut Down	IAR Administrator Activity
Start Up	IAR Administrator Activity
Submission Upload Submission	User initiates or performs manual upload of an assessment
Undo Recent Changes	IAR Administrator Activity
Update External Identifier Type	IAR Administrator Activity
Update user details	IAR Administrator Activity
User Accepted Login Disclaimer	When user is prompted with the user login disclaimer, and the user clicks Accept
User Cancelled Login Disclaimer	When user is prompted with the user login disclaimer, and the user clicks Cancel
User Custom Authentication	IAR Administrator Activity
View Submission Upload Page	User accesses the Upload page from the Submissions men