

# **Integrated Assessment Record**

## **Consolidated DSA, Privacy, Security and Consent Management Training**

**November 2016**

# Introduction

# Purpose of Training

- Provide a thorough understanding of the privacy and security key processes that support IAR as mentioned in the Data Sharing Agreement
- Provide guidelines to implement these privacy and security processes in each HSP in compliance with privacy legislation
- Begin planning the integration of the IAR processes into your existing HSP processes
- Help you meet the IAR implementation milestones

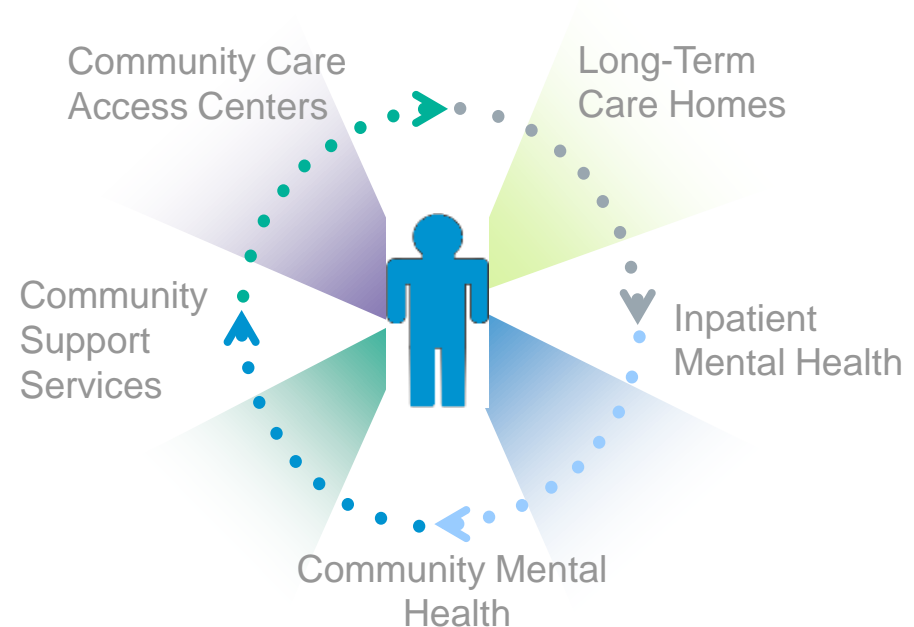
# Agenda

1. Introduction
2. Data Sharing Agreement (DSA)
3. Privacy and Security Processes
  - Incident Management
  - Consent Management
  - Client Privacy Rights Support
  - Audit Log Review
  - Privacy Review
  - User Account Management
  - Enterprise Master Patient Index
4. Communications
5. Awareness and Training
6. Next Steps and Reminders

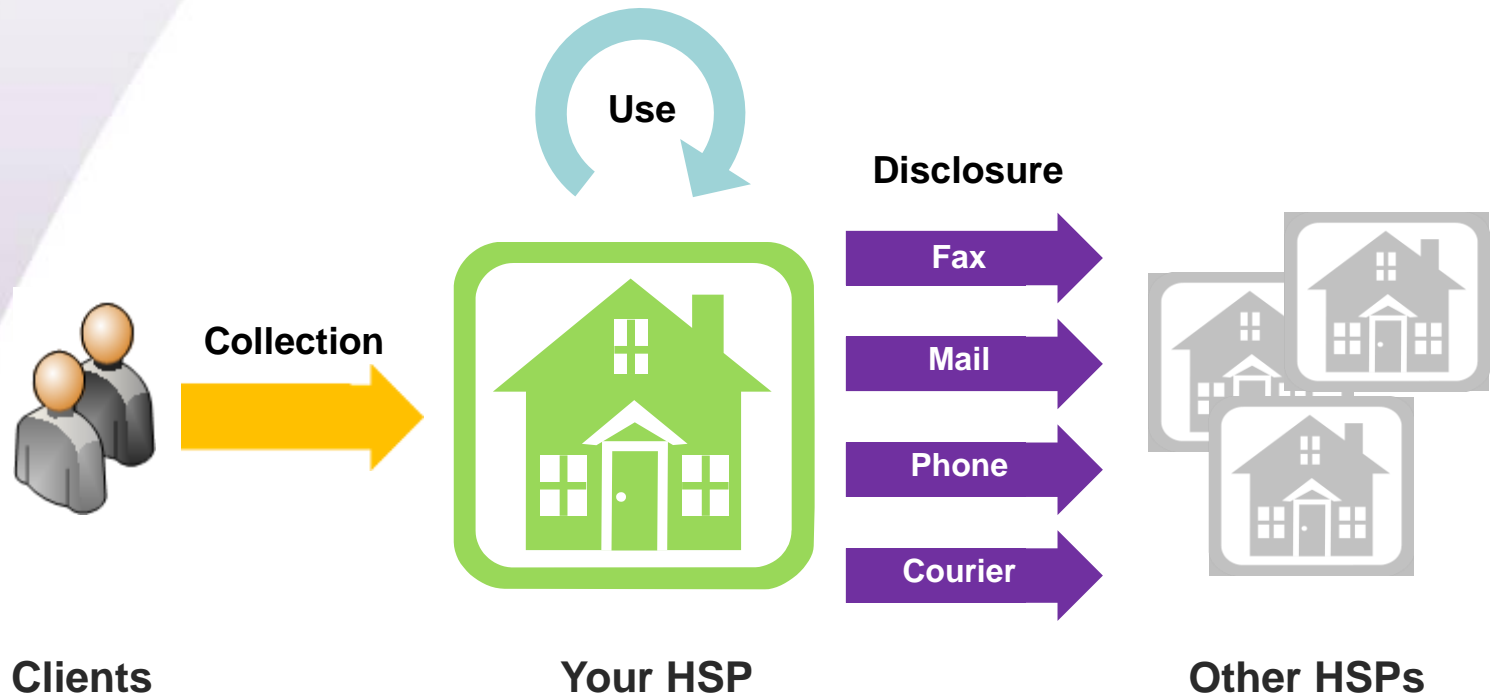
# What is the Integrated Assessment Record (IAR)?

A tool that provides a central repository for data collected from multiple assessments for clients and allows health service providers within the circle of care to view a client's previous assessment information from other care providers.

HSPs can use IAR to electronically view timely client assessment information in a secure manner, improving information management and enabling collaborative care planning.



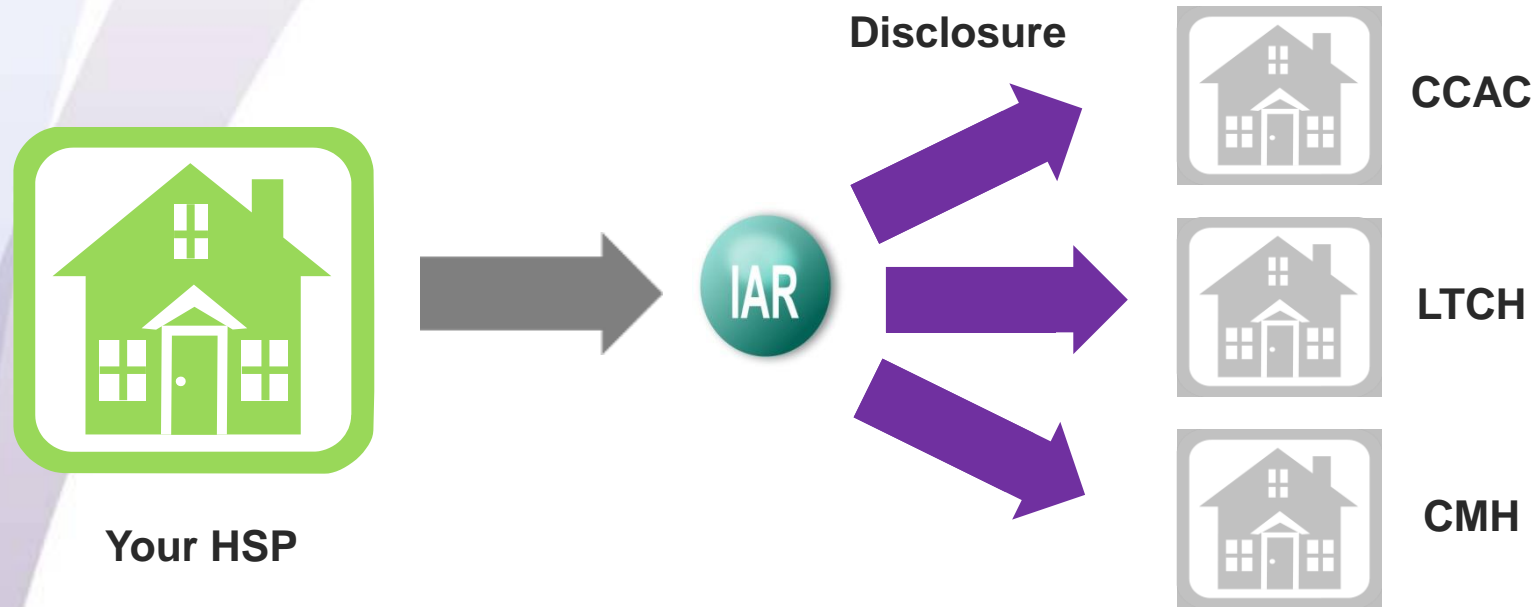
# Information Flow: Today



**Governed and supported by:**

Your HSP's  
privacy policy  
and processes

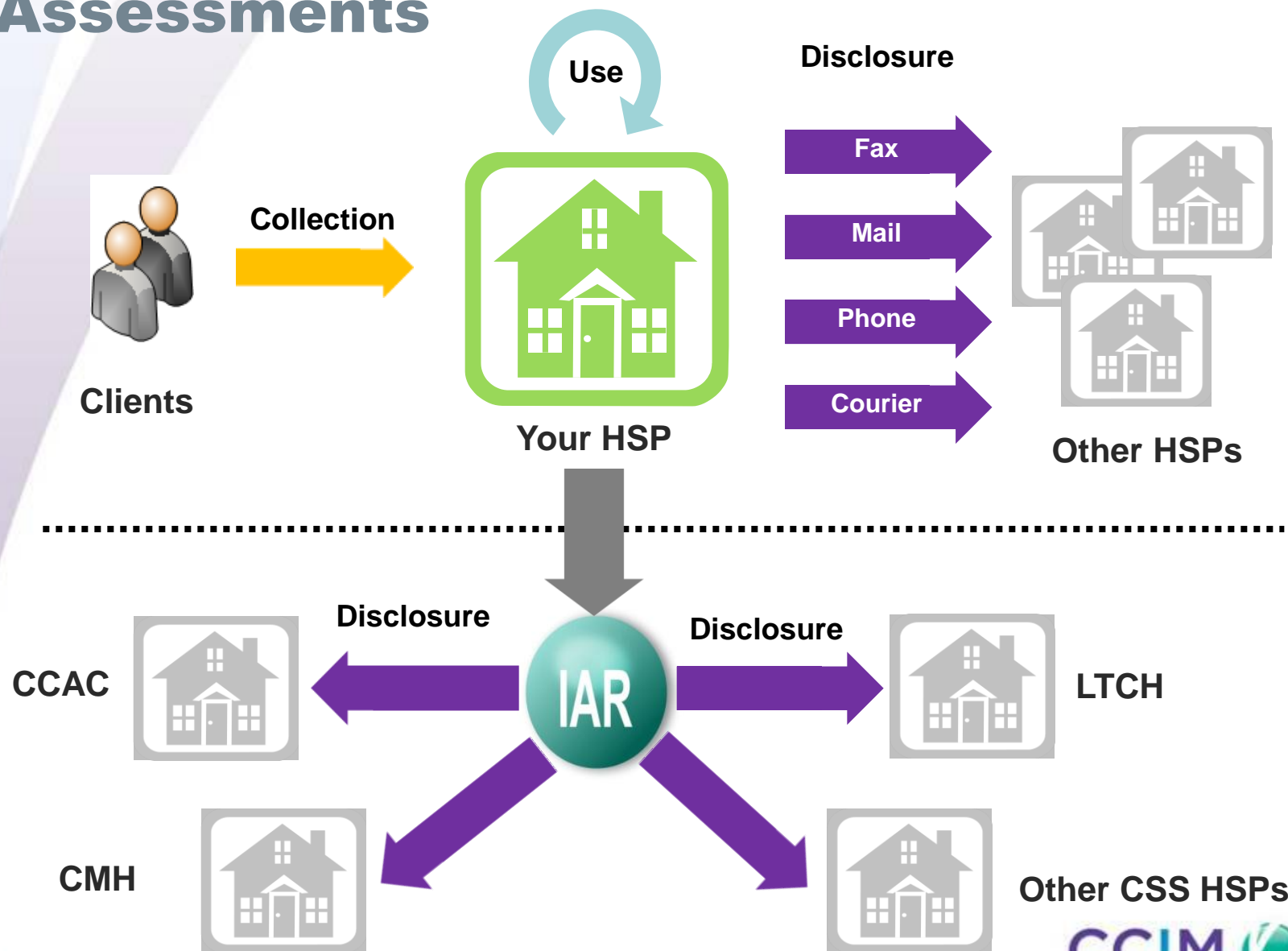
# Information Flow: IAR



Governed and supported by:



# Collection, Use and Disclosure of Assessments





# What is Privacy?

Privacy is the **right of an individual to control** the collection, use and disclosure of his/her personal information.

# Health Information Custodian

- “Health information custodian” means a person or organization (described in PHIPA) who has custody or control of Personal Health Information as a result of or in connection with performing the person’s or organization’s powers or duties or the work.
- The HSP who collects/uses/discloses the assessment is the Health Information Custodian (HIC) for the assessment – in its role as a HIC, the HSP has to fulfill their obligations as prescribed in PHIPA

# Health Information Network Provider

PHIPA defines this legal term as “a person [or organization] who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.”  
O. Reg. 329/04, s. 6 (2).

# Collection, Use and Disclosure

Privacy activities are described using three terms:

**Collect:** An HSP has 'collected' PHI when it has gathered, acquired, received or obtained information about a client by any means from any source.

**Use:** An HSP 'uses' PHI when it handles or deals with PHI that it has collected.

**Disclose:** An HSP discloses PHI when it makes information in its custody available to other HSPs or to other people outside of the HSP.

# Ontario Health Information Privacy Legislation

## PHIPA – Personal Health Information Protection Act

- Ontario's privacy in healthcare legislation introduced in 2004
- PHIPA is informed by the **10 privacy principles** set out in the *Canadian Standards Association Model Code for the Protection of Personal Information*
- The Act regulates how patients' (or clients') Personal Health Information is collected, used, retained, transferred, disclosed, provided access to and disposed of.
- The Act applies to a variety of organizations and individuals within the health care sector, including but not limited to, *health information custodians* (e.g., hospitals and health care practitioners), *agents to HIC* (who can be either organizations or individuals, and who are authorized to act for or on a health information custodian's behalf), health information network provider (HINP).

# **IAR HINP and HIC Privacy Obligations**

# HINP Privacy and Security Obligations

- Designate a Health Information Network Provider (HINP) Privacy Officer
- Sign the Data Sharing Agreement (DSA)
- Coordinate consent/consent directive management
- Coordinate incident management
- Coordinate the support of client's privacy rights
- Manage user accounts in IAR
- Review IAR logs
- Perform Threat and Risk Assessment (TRA) and Privacy Impact Assessment (PIA)
- Publish privacy practices, plain language description of IAR services, safeguards for IAR services, summary of PIA/TRA

# HIC/HSP Privacy and Security Obligations

- Designate a privacy contact person (HSP Privacy Officer)
- Sign the Data Sharing Agreement (DSA)
- Manage client's consent and consent directive
- Manage privacy incidents
- Support client's privacy rights
- Manage user accounts
- Review logs
- Manage client's demographics in Enterprise Master Patient Index (EMPI)
- Other HSP's general privacy obligations (i.e., publish privacy practices, data accuracy)

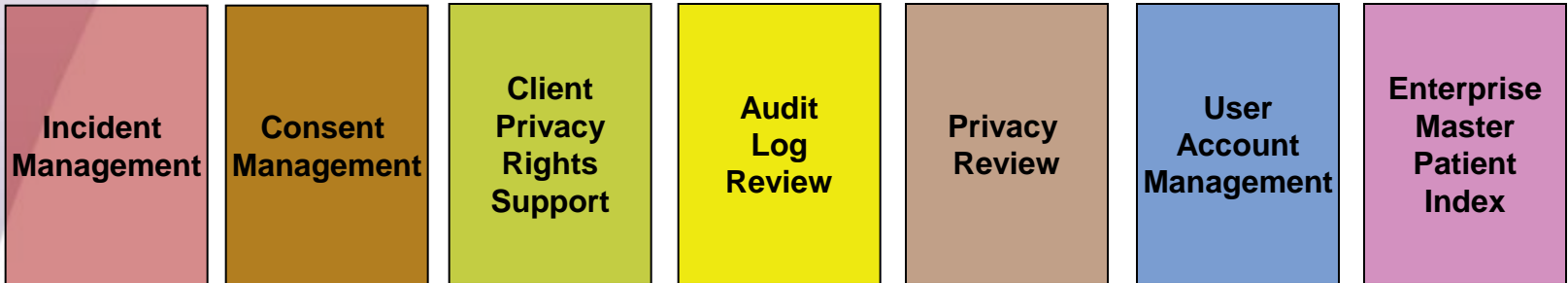


# **IAR Privacy and Security Implementation Framework**

# Privacy and Security Key Processes

## IAR Privacy & Security Implementation Framework

### DATA SHARING AGREEMENT (DSA)



Communication ● Awareness and Training

Privacy and Security Support

# Data Sharing Agreement

- Formal agreement between parties who agree to share data
  - Define the terms and conditions governing the data sharing
  - Establish the accountabilities and responsibilities with regards to data sharing
  - Define the obligations and rights of each participant
  - Describe the PHI privacy and security requirements
- Instil trust among participants to enable the data sharing
- DSA is available on the CCIM website:  
<https://www.ccim.on.ca/IAR/Private/Pages/Security%20and%20Privacy%20ToolKit.aspx>

# DSA Structure - Articles

- Article 1 – Definitions and Interpretation
- Article 2 – Purpose and Application of Agreement
- Article 3 – Statutory Compliance
- Article 4 – Personal Health Information
- Article 5 – Management and Coordination
- Article 6 – Participant Obligations
- Article 7 – Participant Privacy and Security Practices
- Article 8 – Term and Termination
- Article 9 – Liability and Indemnification
- Article 10 – Dispute Resolution
- Article 11 – General

# DSA Structure - Schedules

- Schedule A – Parties to the Agreement
- Schedule B – Existing Agreements
- Schedule C – Provincial Integrated Assessment Record Solution
- Schedule D – Form of Adhesion
- Schedule E – Plain Language Description of Network Services and Security
- Schedule F – Safeguards Regarding Confidentiality; IAR Confidentiality and Security
- Schedule G – Enterprise Master Patient Index System
- Schedule H – Reporting Services
- Schedule I – Consent Call Centre Services
- Schedule J – The Privacy and Security and Data Access Committees

# DSA Key Content

- **Purpose of the Agreement**

- To outline responsibilities, obligations and rights of each participant for sharing client / patient PHI through shared system
- To outline role and responsibilities of the Health Information Network Provider (HINP) with respect to PHI

- **Participants of the Agreement**

- Health service providers (HSPs) – Health Information Custodian (HIC)
- Osler and HSN as IAR HINP and Agents
- TSSO as IAR HINP, EMPI HINP and Agent

# DSA Key Content

- **Authority to Upload Assessment**
  - Each participant that collects data to be uploaded to the shared system acknowledges they are authorized by law to collect and upload it
- **Data Custodian**
  - Personal Health Information belongs to the client / patient regardless of which HSP submitted it to the shared system
  - The HSP who submits assessments is the health information custodian (HIC) for the assessments
  - The HINP provides electronic services to enable the data sharing and is NOT the owner / custodian of the assessments

# DSA Key Content

- **Project Governance**

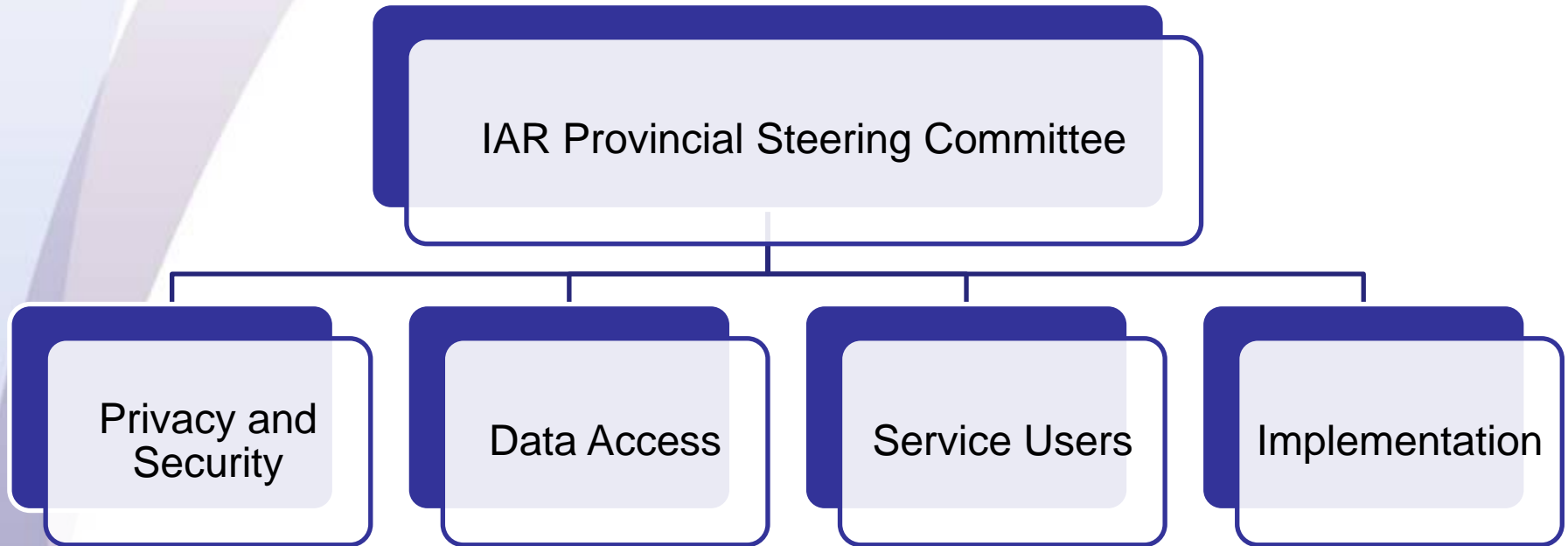
- The IAR Provincial Steering Committee is designated to review and approve new HSP applications to join the DSA, and any uses of assessment data, and request an audit if required
- Privacy and Security Committee develops privacy and security processes and supporting artifacts
- Data Access Committee reviews and provides recommendations on reporting and secondary data uses

- **Termination**

- An HSP may withdraw from the agreement or be terminated for default
- The agreement may also be terminated if certain special circumstances arise
- Upon termination or withdrawal, a Participant must: (1) suspend access by its users to the Shared System, and; (2) cease uploading PHI to the Sharing System
- Upon termination or withdrawal, participants will liaise with the Provincial Steering Committee regarding responsibilities that remain in regard of their data, or to arrange deletion of the data



# IAR Governance Structure



*IAR Governance operates within project scope and budget as approved by MOHLTC*

# DSA Key Content

- **Integrated Assessment Record (IAR) System**
  - A sharing system that allows care providers to share assessment data to facilitate collaborative client/patient care
  - Provides a central repository for assessment data
  - Permits participants to upload assessment data
  - Permits authorized users to view assessment data
- **Enterprise Master Patient Index (EMPI) System**
  - An electronic system to store and manage client / patient information from multiple source systems through multiple IAR instances
  - Identifies and links records across these source systems
  - Allows participants to uniquely identify client records

# DSA Key Content

- **Reporting Services**

- Sets out that a Reporting Environment will be established and maintained at TSSO, who will provide Reporting Services as directed by the governance bodies
- Reporting Services consist of production of reports for HICs, fulfillment of permitted data transfers (i.e. transfers under enabling legislation), and possibly true secondary uses or research uses
- Allows IAR HINPs as Agents to allow transfer of assessment data to TSSO where it is staged and the reports/transfers are performed
- Permits authorized users to view assessment data

- **Consent Call Centre (TSSO)**

- Clients call to make IAR level consent directives
- Operatives use the EMPI for authentication
- Results in messages to the IAR HINP Privacy Officers to apply directives
- No access to assessment data and can't change assessment level directives
- Do collect PHI (HCN and directive) so act as Agents

# DSA Key Content

- **Data Access Committee**
  - Reviews and provides recommendations on secondary uses or transfers of data
  - Operates under Terms of Reference from the IAR Provincial Steering Committee
  - Logs and publishes all uses
  - If a use involves PHI and is not permitted by enabling legislation, HICs may “opt-out” their data from such uses
  - Research would need pre-approved REB approval from an appropriate REB

# DSA Key Content

- **Permitted Use**

- Only authorized users from each participant may access client / patient assessment data on a need to know basis for the purpose of providing health care
- Any secondary use of the assessment data must be reviewed by the Data Access Committee and approved and the IAR Provincial Steering Committee

# DSA Key Content

- **Sharing Demographic Information through EMPI**
  - The EMPI solution exchanges Client/Patient information with multiple instances of the IAR solution in Ontario
  - Client/Patient information stored in the EMPI is used by all HSPs that are participating in multiple instances of the IAR
  - In exchanging Client/Patient information with the EMPI, each HIC must have the implied or express consent of the Client/Patient to collect, use and disclose PHI for the purposes of providing health care or assisting with the provision of health care

# DSA Key Content

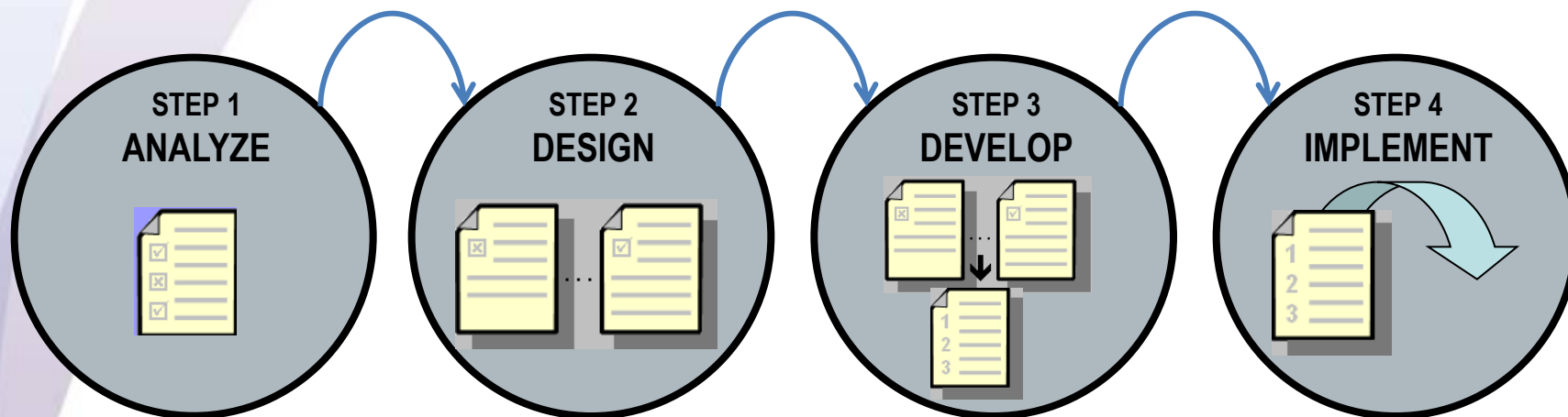
- **Participants' Obligations**
  - HSPs must implement processes to manage privacy in a collaborative way including:
    - Consent management
    - Incident management
    - Client privacy right support
    - Audit log review
    - User account management
  - HINPs must provide support for IAR privacy management (as listed above)

# DSA Key Content

- **Ensuring Compliance with the Agreement**
  - Each participant must conduct a privacy self-assessment annually for review by the Privacy and Security Committee
  - IAR Provincial Steering Committee may request an audit on non-HSPs with unaddressed gaps
- **Subpoena**
  - In the event that the HINP receives a court order (or similar request) requiring the disclosure of some or all of a Participant's Confidential Information, the HINP shall work with the HIC to determine how to respond to the request
- **General Legal Terms**



# Privacy and Security Process Implementation Steps



1. **Analyze** existing internal processes with the requirements presented and determine gaps
2. **Design** new process or process steps to address the gaps
3. **Develop** the required processes, process steps or supporting artifacts
4. **Implement** the newly designed and developed process or steps (remember to include training and communications for HSP staff)

**Incident  
Management**

# **Integrated Incident Management**

# Incident Management

- What is Incident Management? The ability to provide end-to-end management of a series of events that are initiated in response to a privacy or security breach
- Integrated incident management process must be established to coordinate the incident response activities among all participating organizations, which includes:
  - Detection
  - Escalation, notification and reporting
  - Incident handling (containment, eradication, recovery)
  - Lessons learned
- The process will interface with each HSP's incident management process and will focus on collaboration and cooperation activities

# Example of Incidents

- Printed patient assessment information is left in public area (e.g., coffee shop)
- Theft, loss, damage, unauthorized destruction or modification of patient records
- Inappropriate access to patient information by unauthorized users
- Out of the ordinary user activity as indicated during a regular log review
- User account and password was compromised
- Network infrastructure is attacked by hackers
- Violation of joint security and privacy policies or procedures

# Incident Management Assumptions

- Incident management processes exist at both health information custodian (HIC) and health information network provider (HINP) organizations
- Privacy Officer role exists at HICs and HINP
- Existing HIC level incident management process has identified incident contact person (e.g., Privacy Officer)
- Incidents can be reported through the incident contact person at the HICs

# Integrated Incident Management Approach

- Four phases in the integrated incident management process:
  - Detection
  - Escalation
  - Handling
  - Reporting
- The most responsible party activates internal processes to handle the incident
- The party that receives incident report escalates incident to the most responsible party
- The most responsible party updates the Incident Registry at HINP and notifies affected clients

# Privacy Breach Protocol

- Information and Privacy Commissioner (IPC) recommends that the HINP develop a privacy breach protocol
- The protocol enables the HINP and participating HSPs to respond quickly and in a coordinated way during a privacy breach
- Roles and responsibilities are defined
- Investigation and containment are effective and efficient
- Remediation is easy to implement

# Incident Management Process Maps

- Incidents can be detected or reported from the following parties:
  1. HIC
  2. Client or third party of the HIC
  3. HINP
  4. Third parties (e.g., agents or service providers) of HINP
- Processes are developed based on the four parties defined above

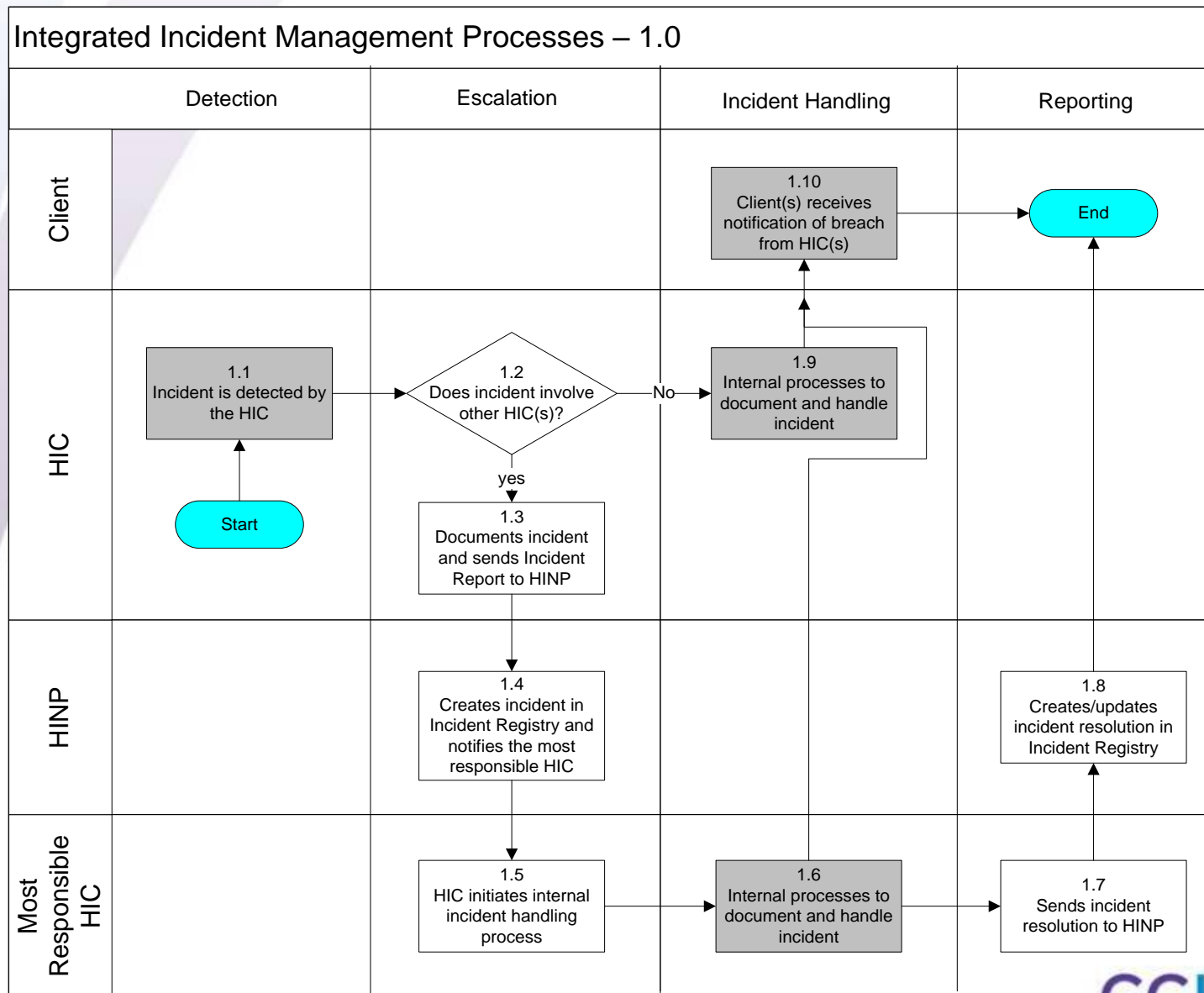


# Scenario 1 — Incident Detected by HIC

HIC detected an incident, such as:

- Printed patient assessment records were lost
- User account and password were compromised
- Network at HIC was broken into by hackers  
(suspect IAR upload files have been accessed)

# 1.0 Incident Detected by HIC

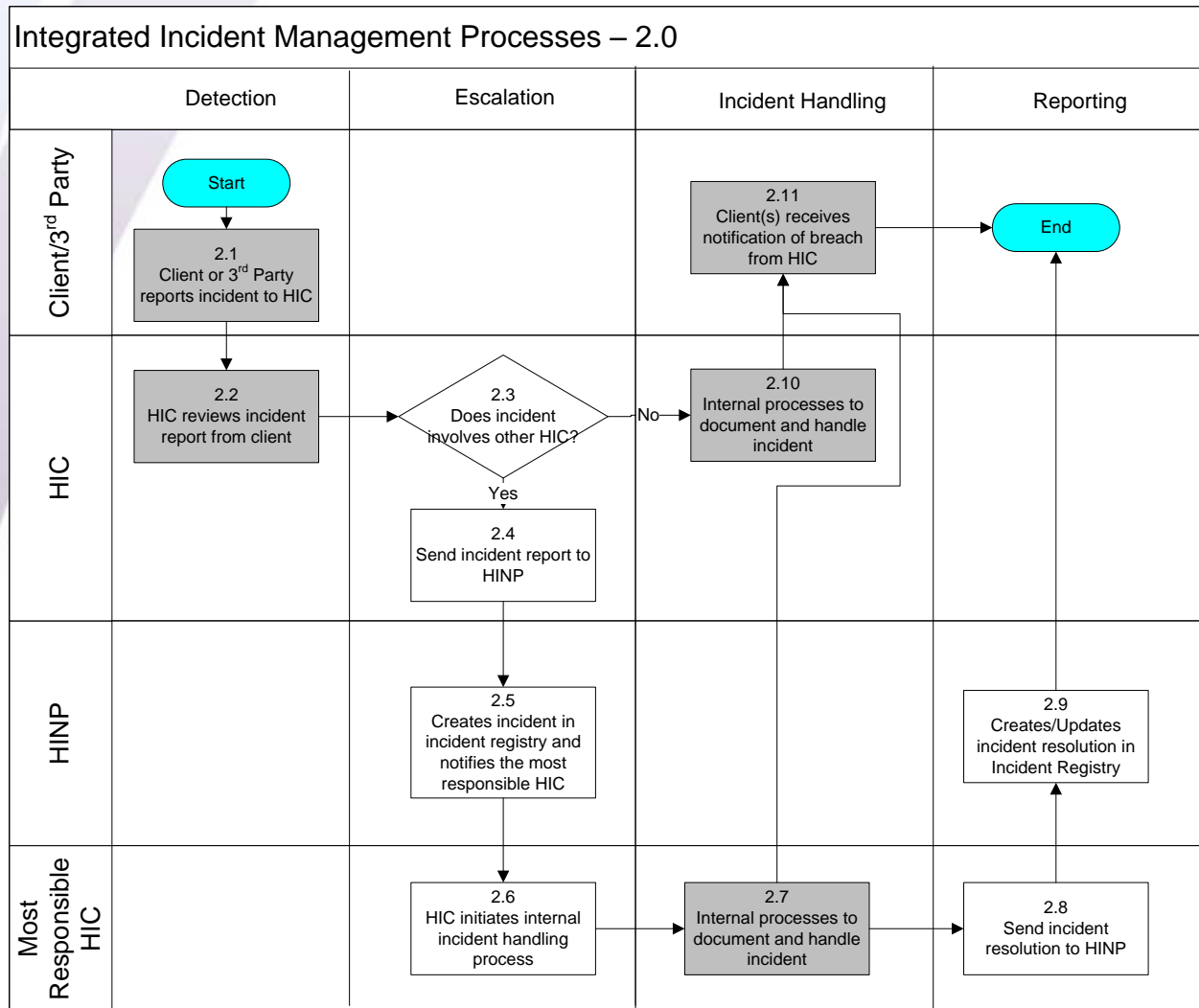


\*Shaded boxes indicate existing steps in HSPs

## Scenario 2 – Incident Reported by Client / Third Party

- A client / third party reports an incident to a participating HSP, such as:
  - “My ex-spouse working in your organization accessed my medical information and used it in our child custody case. Why can he / she access my medical record?”
- A third party (non-client) found printed assessment information on HSP letterhead left at local coffee shop

# 2.0 Incident Reported by Client / Third Party of HIC

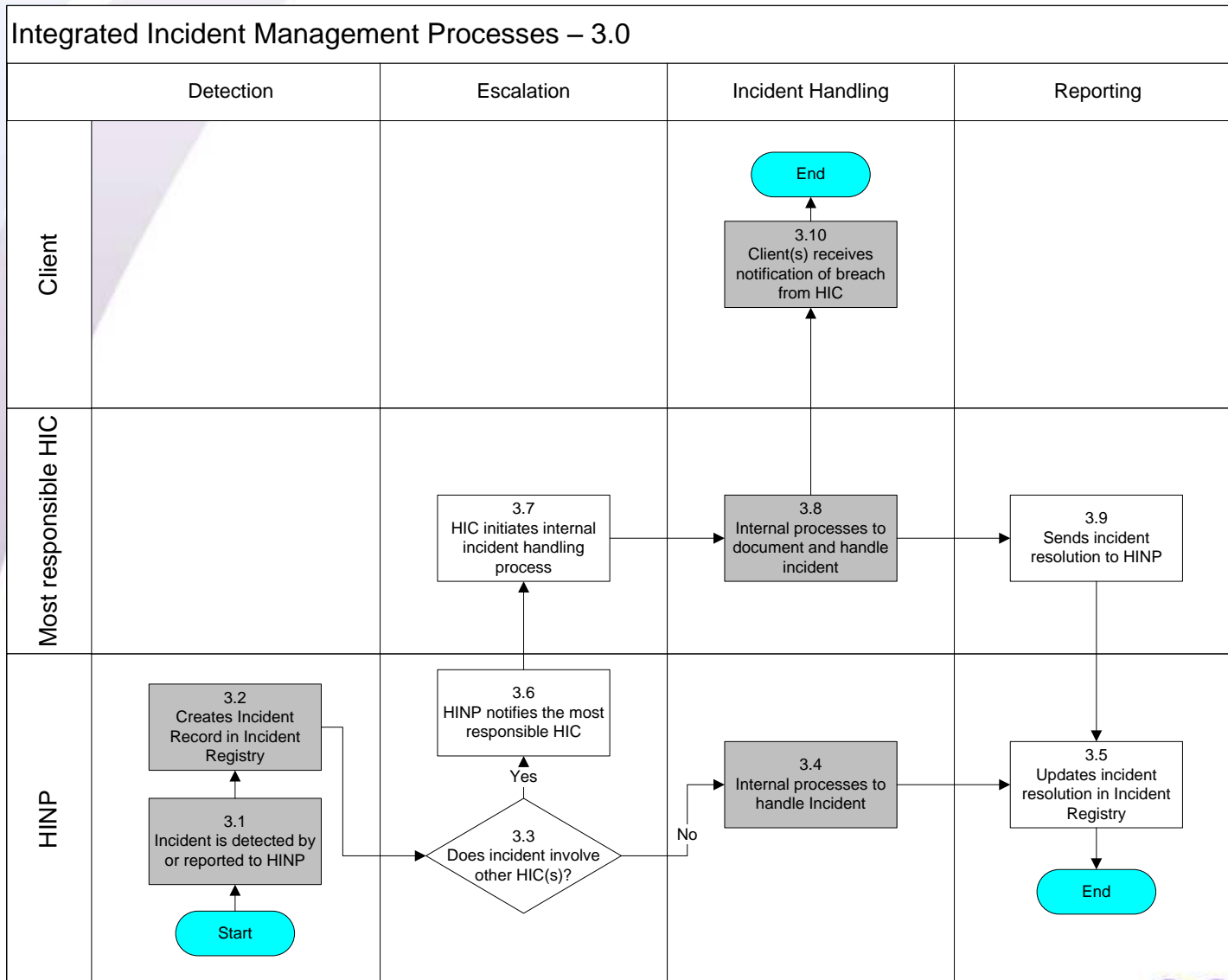


\*Shaded boxes indicate existing steps in HSPs.

# Scenario 3 — Incident Detected by HINP

- HINP detected an incident, such as:
  - IAR backup data unaccounted for (lost or stolen)
  - Potential misuse of access is identified
  - Extraordinary user activity as indicated by regular review

# 3.0 Incident Detected by HINP

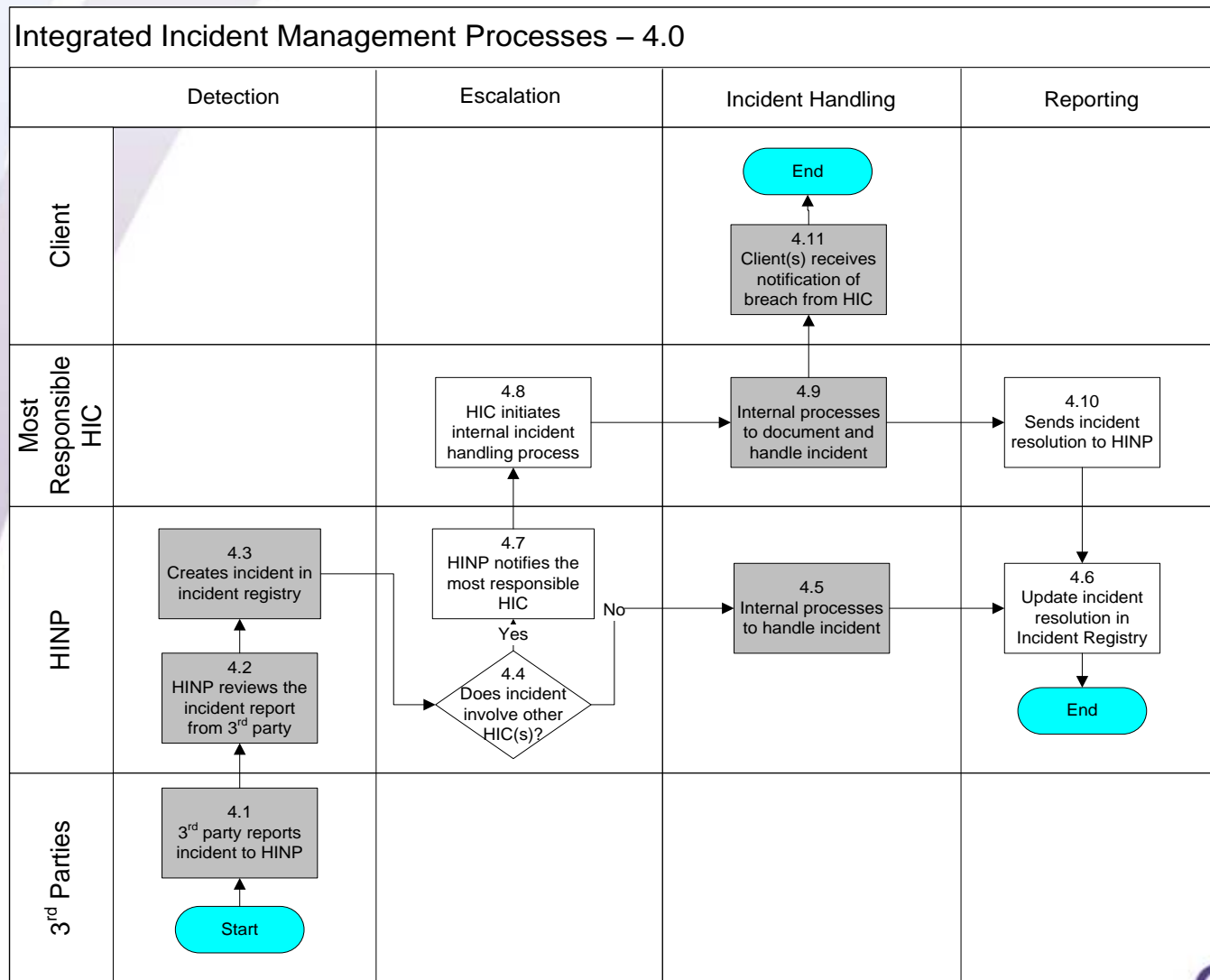


\*Shaded boxes indicate existing steps in HSPs.

## Scenario 4 – Incident Reported by Third Party of HINP

- Third party may report an incident to HINP, such as:
  - Record management service provider reports to HINP that one IAR data backup tape is missing during transit
- Data backup tape that contains server and system data is missing

# 4.0 Incident Reported by Third Party of HINP

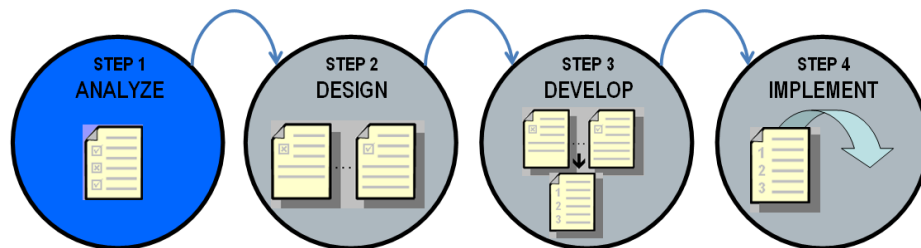


\*Shaded boxes indicate existing steps in HSPs.



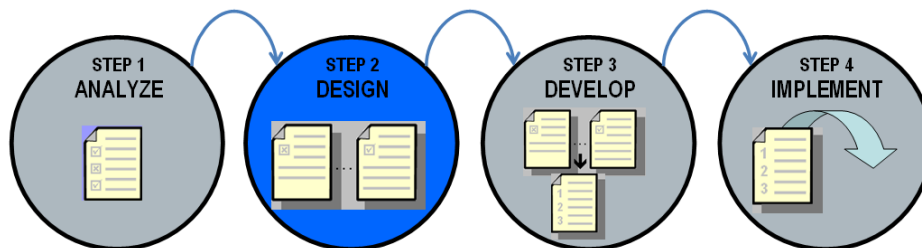
# Incident Management: Analyze

- Map and review existing (internal) incident handling and management process and supporting artifacts
  - Incident handling process
  - Client notification process
  - Investigation, containment and recovery process
  - Communication mechanism to client, staff and third parties (i.e., poster / brochure / website)



# Incident Management: Design

- Review each integration point
  - Detection
  - Escalation
  - Handling
  - Reporting
- Make decision on each integration point
- Update the existing process

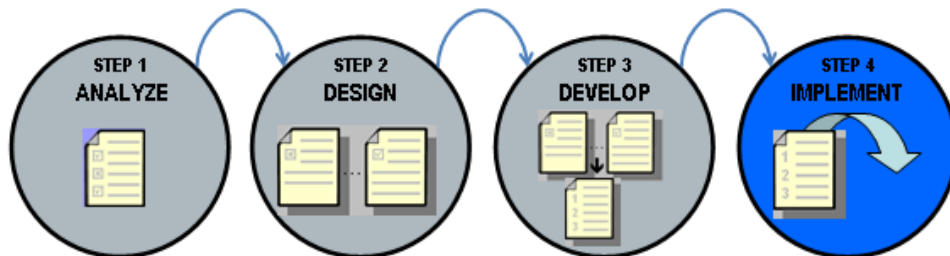


# Integration Points and Questions

Detection	<p>How do staff, clients and third parties know who to contact if they uncover an incident?</p> <p>What information is needed from the incident reporter?</p> <p>What happens after the incident is reported to you or your team?</p>
Escalation	<p>Who would communicate with HINP Privacy Officer if incident involves other HSPs?</p> <p>How would you prepare incident report and information to assist incident escalation to other HSPs?</p> <p>When the HINP escalates to your organization, do you or your team know what to do next?</p> <p>How do you communicate this process to members of your incident handling team?</p>
Handling	<p>Review existing incident handling process for investigation, containment and recovery</p> <p>When and how do you involve the IT operations team (if needed)</p> <p>Review procedure to notify client (if their PHI is breached)</p>
Reporting	<p>Explore ways to review incident logs and gather lessons learned</p>

# Incident Management: Implement

- Internal approval of revised/new process(es)
- Provide training and awareness to all staff members in your organization (not just clinicians or IAR users)
- External communications (clients and third parties)
  - Poster, brochure, corporate website, centralized e-mail box

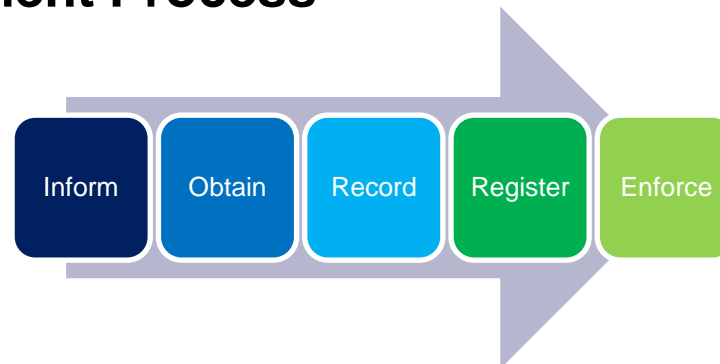


**Consent  
Management**

# **Consent Management**

# Consent Management — Overview

- Enables client control over how their personal health information (PHI) is collected, used, disclosed and shared
  - Ensures compliance with PHIPA
- **Consent Directive**
  - A client's instruction on how their Personal Health Information can be collected, used and disclosed
- **Consent Model**
  - Informed consent
  - Implied and express consent
  - Scope of consent directive
  - Structure of consent form (if required)
- **Consent Management Process**



# Informed Consent — Elements of Informed Consent

Clients should be informed about:

- **What** information about them is being collected, used and disclosed
- **Why** their information is being collected, use and disclosed (i.e., The purposes of the collection, use or disclosure, as the case may be (2004, c. 3, Sched. A, s. 18 (5).)
- **How** information is being collected, used and disclosed and with **whom**
- **Individual' s right** to give or withhold consent (2004, c. 3, Sched. A, s. 18 (5))
- The **positive and negative consequences** of giving, withholding or withdrawing consent

# Implied and Express Consent Types

**Implied Consent** – refers to situations in which it is **reasonable to infer** that the client is consenting and it is not necessary to specifically (or expressly) ask for the client's Consent.

**Express Consent** – refers to situations where Consent is given explicitly, **either orally or in writing**. Express Consent can be signed or checked off on a list.

***The key is to ensure the consent obtained is valid.***



# Consent Form – Excerpt from Implementation Guide

<<HSP Name>>

## Consent Directive to Sharing Assessment Data

We are constantly working to provide you with health care services that meet your needs and enable you to seek those services that you want or need at organizations across the province. In doing so, we may need to share your assessment data via fax or an electronic sharing system with other Health Service Providers, who need to review the assessment data in order to provide services to you.

You have the right to withhold or withdraw your consent to share your personal health information at any time.

We may need to share the assessment with other Health Service Providers, who will need to review it in order to provide services to you. Do you consent to the sharing of your assessment?

Yes, I consent	No, I don't consent	To the sharing of the <<assessment ID>> collected by <<HSP Name>> <<on DATE >>. I understand my choice will only be applied to the sharing of this assessment with other health service providers via fax or an electronic sharing system, and will be effective within <<#>> Business Days. Note: This consent does <i>not</i> apply to the copies of my assessments that other HSP has already received.
Yes, I consent	No, I don't consent	To the sharing of all my previous assessments, collected by <<HSP Name>>. I understand my choice will only be applied to the sharing of assessments collected by <<HSP Name>> with other health service providers and will be effective within <<#>> Business Days. Note: This consent does <i>not</i> apply to the copies of my assessments that other HSPs have already received.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

(MM/DD/YYYY)

Substitute Decision-Maker (if applicable):

Name: \_\_\_\_\_

Date of Birth : \_\_\_\_\_

(MM/DD/YYYY)

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

(MM/DD/YYYY)

Client/Patient Information (information are collected for patient identification) The fields below are used for the purposes of identifying the individual who is consenting so that their Consent can be properly managed.

Name: \_\_\_\_\_

Date of Birth: \_\_\_\_\_

(MM/DD/YYYY)

Telephone No: \_\_\_\_\_

Address: \_\_\_\_\_

An electronic sharing system is used to share your assessment data with other Health Service Providers, who need to review the assessment data in order to provide services to you. If you wish to consent or withhold your consent to the sharing of all your assessments in the electronic sharing system, please contact the support centre by calling Telephone: (###) ###-####.

Please refer to the <<brochure/poster >> for additional information provided regarding the collection, use and disclosure of your personal health information.  
<<Contact Information / Website>>

# Sample Brochure

## Your Privacy Choices

Please speak to your usual care provider or our Privacy Officer, if you want to:

**See your own assessment:** You can request a copy of your assessment at any time.

**Correct your own assessments:** You can ask to have information in your assessment corrected or updated.

**Opt Out:** You may choose not to share your assessment information with other health service providers. You may also choose to have your basic personal information (like name, phone number, city) blocked from health care workers who view the IAR.

<<Insert potential Positive and negative consequences for sharing or not sharing the assessment>>

To choose to withhold your consent to share your assessment information or your basic identifying information, call the IAR Consent Call Centre toll free at: 1-855-585-5279 (TTY 1-855-973-4445).

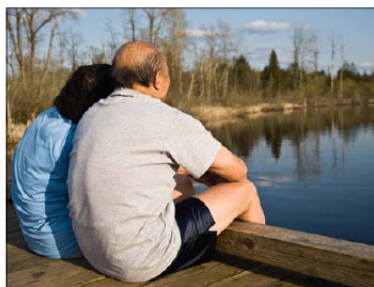
If you would like to know more about how your personal health information is handled and shared with our partner organizations, feel free to ask our Privacy Officer. They will be happy to answer any questions that you might have.

<<insert privacy officer contact information>>

## The Privacy Commissioner

If you have any issues or concerns about how your health information is being handled, you have the right to contact the **Information and Privacy Commissioner of Ontario** at:

2 Bloor Street East, Suite 1400  
Toronto, ON M4W 1A8  
Telephone: 416-326-3333  
or, 1-800-387-0073  
Online: <http://www.ipc.on.ca>



## Privacy and Your Assessment



## A Guide to the Collection, Use and Sharing of Your Personal Health Information

<HSP logo here>

# Sample Brochure

## Your Personal Health Information

Your Personal Health Information (PHI) is important in allowing us to provide you with better services. Often times that information is used when performing assessments to determine your health service and support needs.

Your assessment may include details on:

- Your physical and mental health
- Your personal health history
- <<add/change information in the assessment >>

Unless you tell us not to, we share your assessment information with other health service providers who will provide you with support now and in the future.

## Sharing Your PHI

We use a secure electronic system to share your health information with other health service providers. This allows them to view the information they need to provide you with the services you need.

If you have agreed to share your PHI, the information in your assessment will be used to:

- Provide health support and services based on your needs
- Make sure your providers have the most up-to-date and complete record of your health history and needs
- Help us see where there might be gaps or overlaps so we can provide services where they are most needed
- Make sure everyone is getting the right support and services



## Privacy and Security of Your Information

The personal health information collected in your assessment belongs to you. The privacy and protection of your PHI is a priority. In the assessment process, we only collect the health information we need in order to determine your service and support needs. This information cannot be used for any other purposes without your permission.

- Your health information is kept in a secure place
- Your health information will only be viewed by authorized people who deliver your services
- All health services providers have signed contracts to keep your information confidential
- When a person views your information, it is recorded in a log. This log is reviewed regularly to make sure there has been no unauthorized access to your information.
- Information is stored and/or disposed of according to the law
- We will investigate any suspected breach or unauthorized access to your personal health information

# Sample Poster

<HSP LOGO HERE>

## Privacy and Your Assessment



## Know Your Rights

### Sharing your assessment information is important . . .

Unless you tell us not to, your personal assessment information will be shared electronically with other health service providers who will provide you with support now and in the future. Sharing assessments gives health service providers in your community the most up-to-date information about you so they can better serve your needs.

Your assessment may contain information on:

- ▶ Your mental and physical health
- ▶ Your personal and health history
- ▶ <<Insert other information the assessment may contain>>

### Your assessment information is protected.

The information you give us in your assessment can only be used by authorized staff involved in providing you with health support and services. Providers caring for you must keep your information confidential.

**When it comes to assessment information, you can choose to:**

- ▶ **Request to see your own assessment at any time**
- ▶ **Ask for corrections or updates**
- ▶ **Tell us if you do not want us to share your assessment or basic identifying information**

To learn how your assessment information is being used and shared, you have the right to contact our Privacy Officer at: <<insert contact info>>

Withholding consent in the IAR means that all of your assessments will not be viewable even by those who are providing you with service. You can reach the IAR Consent Call Centre to instruct to hide your assessments from view by calling toll free at 1-855-585-5279 (TTY 1-855-973-4445).

If you have concerns about your personal health information and how it is handled you have the right to contact the Information and Privacy Commissioner of Ontario at: 2 Bloor Street East, Suite 1400, Toronto, ON, M4W 1A8 | Telephone 416, 326, 3333 or 1-800-387-0073



# Message Script

## The collection, use, disclosure (share) of client's assessment

We will/would like to complete the assessment with you to identify the support and service you need. The assessment will cover **<<Description of Information that may be part of the assessment>>**. We collect and use your personal health information during the assessment in order to provide you with services that suit your individual needs. We also use your information to coordinate service planning with other Health Service Providers in order to provide you with better service.

## Sharing of client's assessment

If you agree, your information may also be shared via an electronic sharing system with other agencies that provide services to you.

## What your Consent means

Your information may only be shared with other agencies with your Consent.

If you do not want to share your assessment information with other agencies, you can let me know today or inform our staff anytime in the future, and we will make sure the assessment will not be shared. We also use a centralized electronic system to share assessments among partner agencies. The electronic system stores all of your assessment from **<<HSP name>>** and other agencies. If you don't want any of the assessment information shared in the electronic system, please contact the Consent Call Centre support centre, who will ensure that no one will be able to access your assessments. You can also have your basic identifying information blocked from sharing if you wish to have no trace of you available to other health care workers. You should know that your consent directive will take effect in **two business days**.

Optional: If you give us your consent, this may mean:

**<<Positive and negative consequences for sharing the assessment>>**. If you choose to withdraw your consent and not share your assessment, this may mean: **<<Positive and negative consequences for not sharing the assessment>>**.

## Your privacy rights

You can request a copy of the assessment information in your file by contacting us. You also have the right to request a correction or amendment to your assessment information, or log a complaint if you feel that we have not addressed your privacy concern correctly.

## More information or questions?

If you would like to know more about how your personal health information is handled and shared with agencies, you can contact the privacy officer at the **<<HSP name>>**. They will help you understand what it means to share your assessment and will be able to answer your questions. Please contact our designated privacy contact at **<<contact information>>**.

For more details see IAR Privacy, Security and Consent Management Training manual, Tab 3, Appendix C of the Integrated Consent Management Process or page 64 in the same guide on CCIM website.

# Group Discussion

- Discuss at your table what your current process is for informed consent.
  - What methods do you use?
    - Posters
    - Brochures
    - Face to face discussion
- What methods do we want to add or change in the future?
- What types of material would you develop to support the future method of informing?
- What do we currently tell our clients?
- **What will we tell our clients about IAR?**

# IAR Consent Model

IAR supports two levels of Consent Directive:

- HSP-level Consent Directive applied to the assessments collected by the individual HSP
- IAR-level Consent Directive applied to all assessments in IAR relating to a client

# HSP-Level Consent Directive

- HSP will obtain consent/Consent Directive from the client and register the consent in the assessment tool
  - Consent Directive, along with the assessment, will be uploaded to IAR
  - IAR will inherit the consent flag submitted along with the individual assessment and automatically enforce the Consent Directive in IAR
- Alternatively, the HSP can log in to the IAR consent interface to register the Consent Directive manually
  - Only the assessments from the HSP will be affected

***HSPs need to determine whether their software can upload the consent flag, or if they will need to do this manually***



# IAR-Level Consent Directive

- To register the IAR-level Consent Directive, the client can call the Consent Call Centre:

**Regular Toll-free: 1-855-585-5279**

**TTY Toll-Free: 1-855-973-4445**

- Consent to share in the IAR means all of the client's assessments across HSPs will be shared with participating HSPs that provide care to the client
  - If consent is withheld in the IAR, all of the client's assessments already in the IAR, and uploaded in the future, will be locked and participating HSPs will **not** be able to view them
  - Clients who feel at risk having their demographic information viewable in IAR even if their assessment is blocked can opt for complete PI Suppression
- The more restrictive Consent Directive (either HSP-level or IAR-level) will be enforced

HELP LOGO HERE

## Privacy and Your Assessment



### Know Your Rights

**Sharing your assessment information is important . . .**

Unless you tell us not to, your personal assessment information will be shared electronically with other health service providers who will provide you with support now and in the future. Sharing assessments gives health service providers in your community the most up-to-date information about you so they can better serve your needs.

Your assessment may contain information on:

- ▶ Your mental and physical health
- ▶ Your personal and health history
- ▶ <<Insert other information the assessment may contain>>

**Your assessment information is protected.**

The information you give us in your assessment can only be used by authorized staff involved in providing you with health support and services. Providers caring for you must keep your information confidential.

**When it comes to assessment information, you can choose to:**

- ▶ Request to see your own assessment at any time
- ▶ Ask for corrections or updates
- ▶ Tell us if you do not want us to share your assessment or basic identifying information

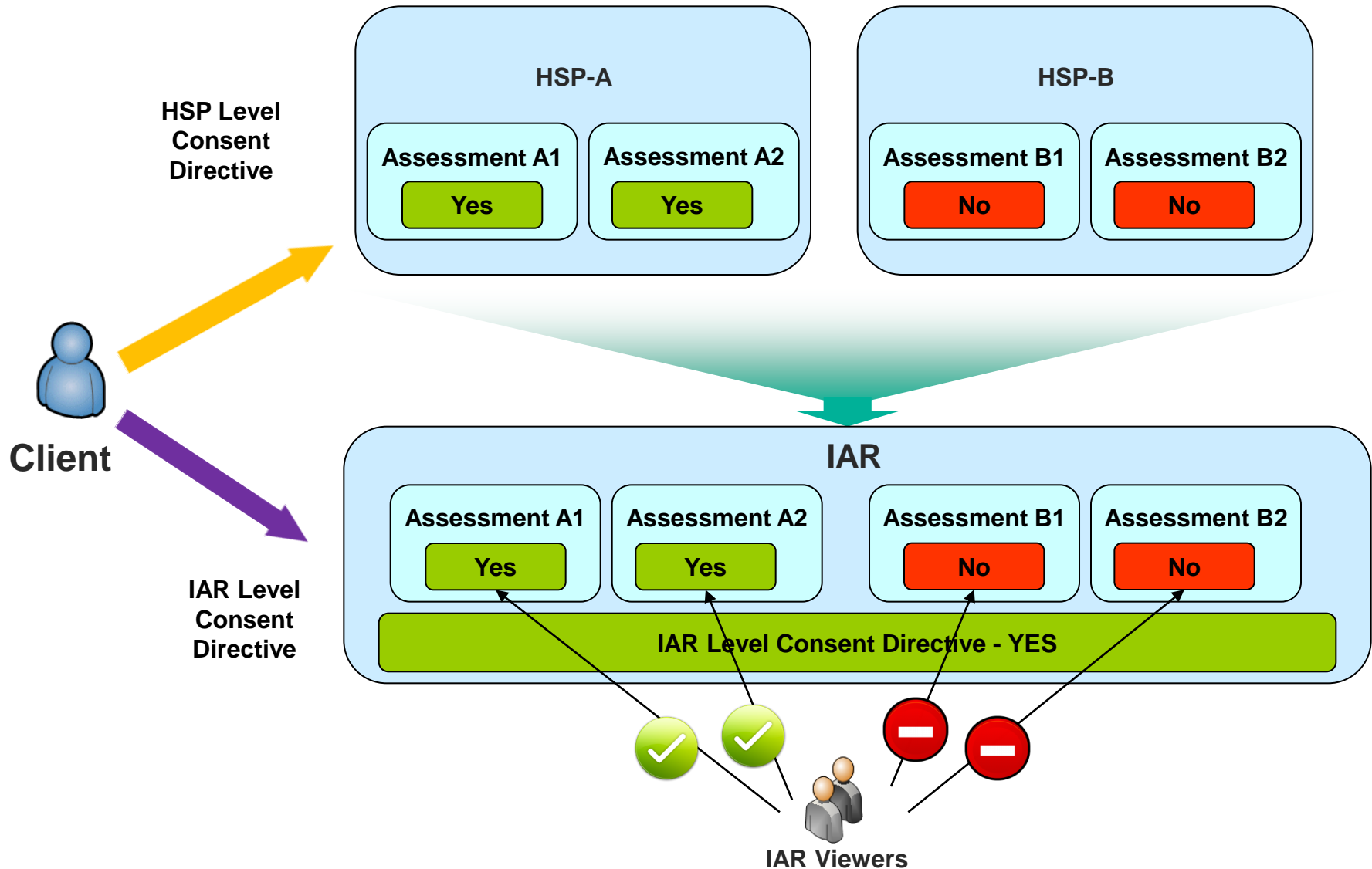
To learn how your assessment information is being used and shared, you have the right to contact our Privacy Officer at: <<insert contact info>>

Withholding consent in the IAR means that all of your assessments will not be viewable even by those who are providing you with service. You can reach the IAR Consent Call Centre to instruct to hide your assessments from view by calling toll free at 1-855-585-5279 (TTY 1-855-973-4445).

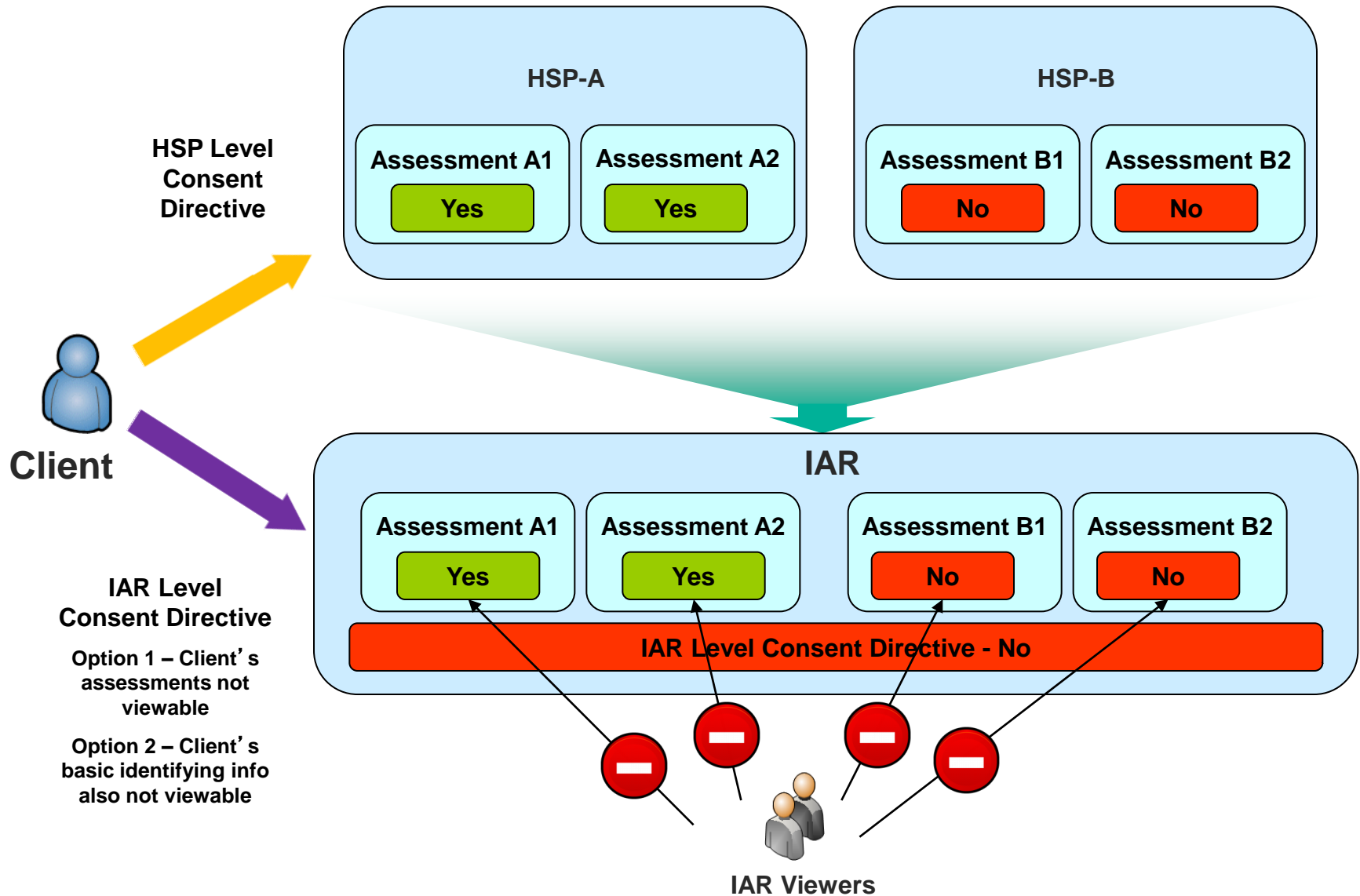
If you have concerns about your personal health information and how it is handled you have the right to contact the Information and Privacy Commissioner of Ontario at: 2 Bloor Street East, Suite 1400, Toronto, ON, M4W 1A8 | Telephone 416, 326, 5333 or 1-800-387-4073

[www.ccim.on.ca/IAR/Private/Pages/Security%20and%20Privacy%20Toolkit.aspx](http://www.ccim.on.ca/IAR/Private/Pages/Security%20and%20Privacy%20Toolkit.aspx)






# How Consent Works in IAR



# How Consent Works in IAR (cont'd)



# IAR Consent Directive in Effect

0Susan TesterPLOGOUT

COMMON

MONITORING

MESSAGING

WORKLISTS

PERSON SEARCH

Person Search

OPERATIONAL REPORTS

PRIVACY REPORTS

ABOUT IAR

## Person Search

Ontario Health Card Number \*

OR Person Attribute Search

Last Name \*

Bosh

First Name \*

Chris

Date of Birth \*

11-Jul-1959

Sex

Select

Street


Unit/Suite/Apt.

Postal/Zip Code

Phone

Search


Clear

<input type="checkbox"/>	Score	Last Name	First Name	Alias	Sex	Date of Birth	City	Phone
<input type="checkbox"/>	 10.4	Bosh	Chris		Male	11-Jul-1959	Toronto	4161112244






Add checked results to worklist

Replace worklist with checked results

Results 1-1



# IAR Consent Directive with PI Suppression in Effect

0Susan TesterPLOGOUT

COMMON

MONITORING

MESSAGING

WORKLISTS

PERSON SEARCH

PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

ABOUT IAR

Person Search

Ontario Health Card Number \*

OR Person Attribute Search

Last Name \*

Wayne

First Name \*

Bruce

Date of Birth \*

14-Oct-1943

Sex

Select

Street

Unit/Suite/Apt.


Postal/Zip Code

Phone

Search

Clear

No result found for your search criteria. This could either be because: (1) you provided only a First Name and Last Name (please include additional search criteria and resubmit), (2) you misspelled your search criteria (please check and resubmit), or (3) there is no data that matches the search criteria because it is not in the system or consent for sharing has been withheld by the client (PHIPA s.20(2)).



# HSP Assessment Consent Directive in Effect

SANCHEZ Jo (M/67 years)

Assessment Listing

Assessment Document

Showing All [Mark All As Read](#)

Group By Assessments/Record Type

Assessment Listing

OCAN FULL (1 / 1)

### Person Demographics

[Follow Coordinated Care Plan](#)

Personal Information		Addresses	Aliases
Sex	Male	77 Jo Avenue July13, , JoCity, ON, A0K7G5,	Fifi
Language	French		
Date of Birth	29-Dec-1948		
Phone	*****765		

### Timeline

Restricted documents exist

reset zoom

Coord. Care Plan  
RAI-MH  
RAI-MDS-2.0  
interRAI-CHA  
OCAN  
interRAI-CA  
RAI-HC  
interRAI-PS

Oct 2014 Feb 2015 Jun 2015 Nov 2015 Mar 2016 Jul 2016 Dec 2016

### Assessments

Type	Record Type	Reference Date	Assessed At	
OCAN FULL	(Prior to) discharge	30-Jun-2015	TESTORG	<a href="#">Summary</a> <a href="#">Detail</a>

Message from webpage



Restricted documents exist

OK

# Scenarios: Client Needs HSP Help

1. Client is not comfortable or not able to call the Consent Call Centre by himself / herself
2. Client does not have enough information to identify himself / herself
3. Client has a substitute decision maker (SDM) who wants to provide a Consent Directive on his / her behalf

# Client Needs Help with Calling the Consent Call Centre

- The clinician or case worker can help the client place the call to the Consent Call Centre
- If the client needs assistance navigating through the process during his / her encounter with the Consent Call Centre customer service representative (CSR), the clinician or case worker may help the client by repeating the message from the CSR or explaining what information is required
- Some basic identifying information about the clinician or case worker will be asked by the CSR to identify the client and link his / her Consent Directive to the correct assessments in IAR
- The client will still need to provide the consent to the Consent Call Centre himself / herself



# Client Needs Help Identifying Self

- If the client does not have a Health Card Number, a fixed address or a telephone number, the client is required to place the call to the Consent Call Centre from an HSP
- The Consent Call Centre CSR will request the assistance of the clinician or case worker to help verify the identity of the client
- The client will provide the consent to the Consent Call Centre
- Some basic information about the clinician will be asked by the Consent Call Centre

# SDM Needs Help Identifying Themselves

- If the client has a Substitute Decision Maker (SDM) providing the Consent Directive on their behalf, the SDM is required to place the call to the Consent Call Centre from an HSP — the Consent Call Centre CSR will request the assistance of the clinician or case worker to help verify the identity of the SDM
- The CSR will ask the clinician or case worker for information to validate the clinician or case worker as an authorized person from the HSP, including the clinician's name, HSP name, HSP phone number, IAR user ID, etc.
- Once the identity of the SDM is verified through the clinician or case worker, the SDM will continue the encounter with the Consent Call Centre, and provide the client's Consent Directive to the CSR

# Integration Points

## Consent Model

- Informing the client: What to say, how to say it
- Implied or express consent
- Scope of the Consent Directive
- Structure of Consent form

## Consent Process

1. When to inform the client
2. When and how to obtain and update consent
3. How to record the consent directive in a central location, and who performs this activity
3. Register/Update Consent Directive
  - How to register Consent Directives
  - Who registers Consent Directives
4. Enforcing Consent Directive
  - How to effectively enforce the Consent Directive

**Client  
Privacy  
Rights  
Support**

# **Client Privacy Rights Support**

# Client Privacy Rights Support Process

- Integrated client privacy support process (service desk) to fulfill Health Information Custodian's (HIC) privacy obligation to:
  - Provide access to their Personal Health Information (PHI) upon client's request
  - Make correction to PHI upon client's request
  - Handle client's challenge concerning compliance with privacy legislation
- The process will interface with each HSP's existing process and will focus on collaboration and cooperation activities

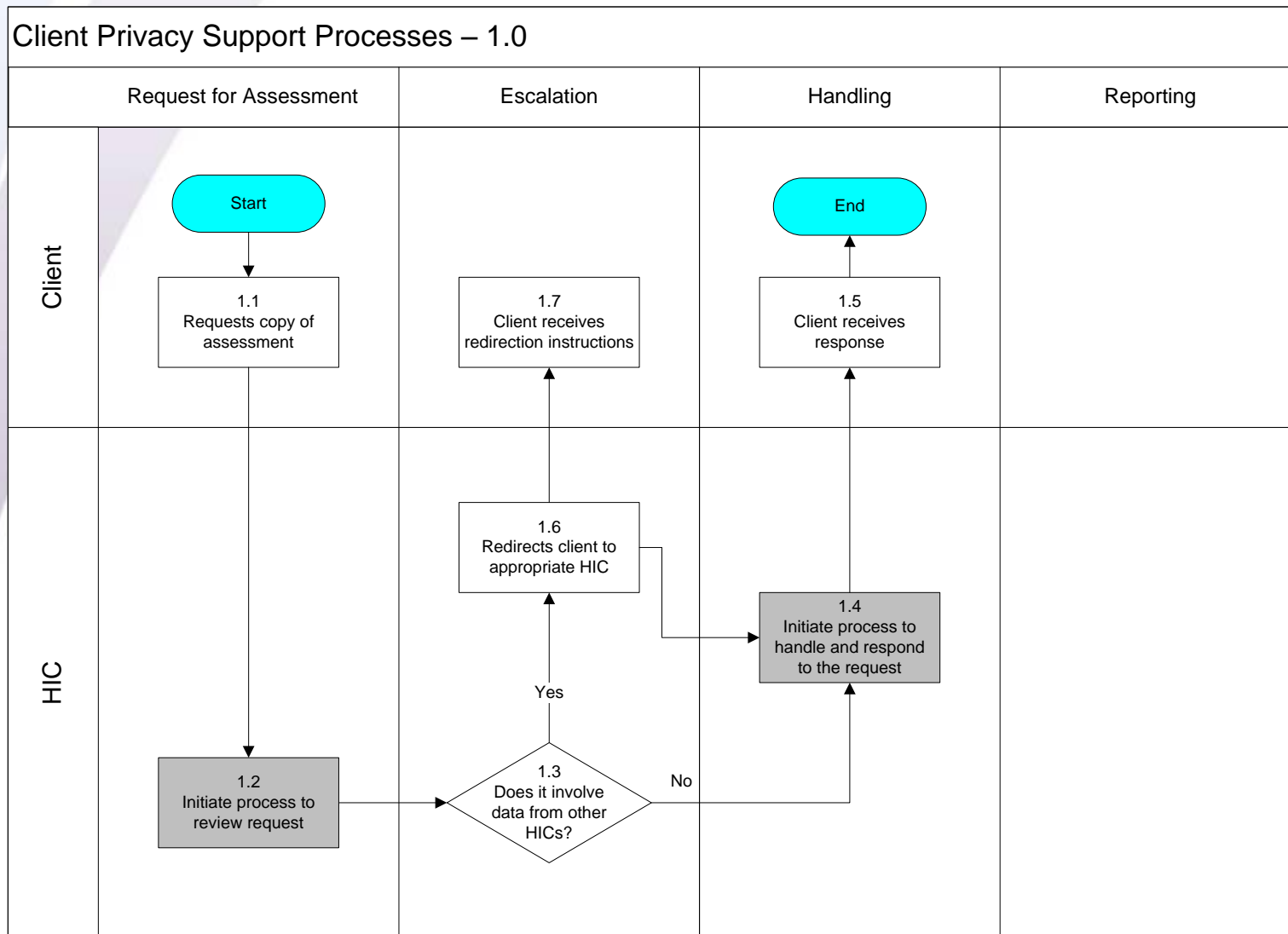
# Approach

- If the request to access or change the assessment or the complaint relates solely to information in the custody or control of a single HIC, local processes are used
- If the request to access or change the assessment involves other HICs, the HIC identifies the other involved HICs for the client
- If the complaint involves more than one HIC, the HINP identifies the most responsible HIC to handle the response

# Client Privacy Rights Support Assumptions

- Each HIC has in place policies and procedures to support client privacy rights
- HICs only release and correct information within their custody or control
- HINP will only participate or coordinate the privacy complaint management process
- IAR is a repository of information that originates from multiple HICs and is not considered the source of truth for that information

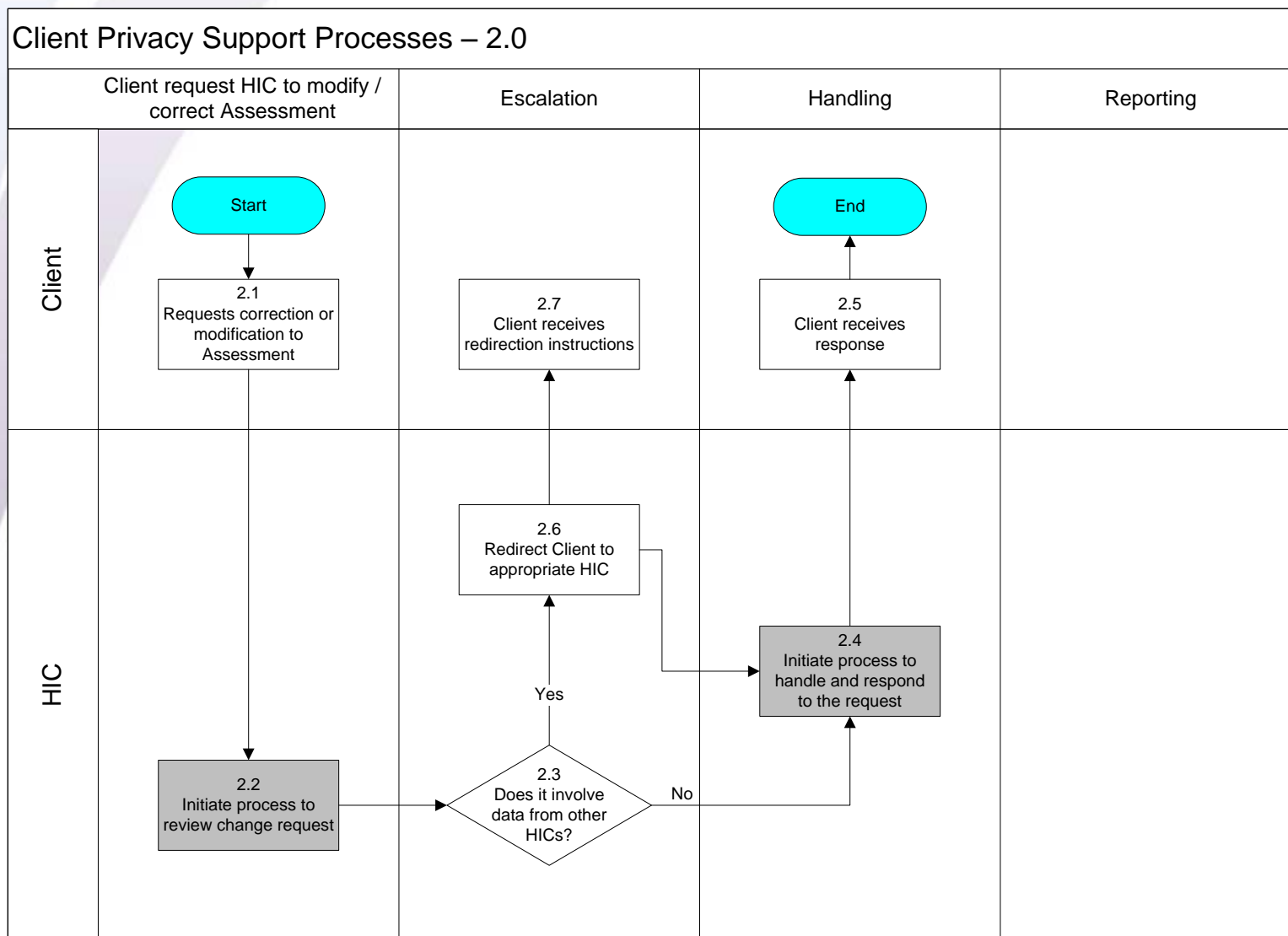
# 1.0 – Request a Copy of Assessment



\*Shaded boxes indicate existing steps in HSPs.

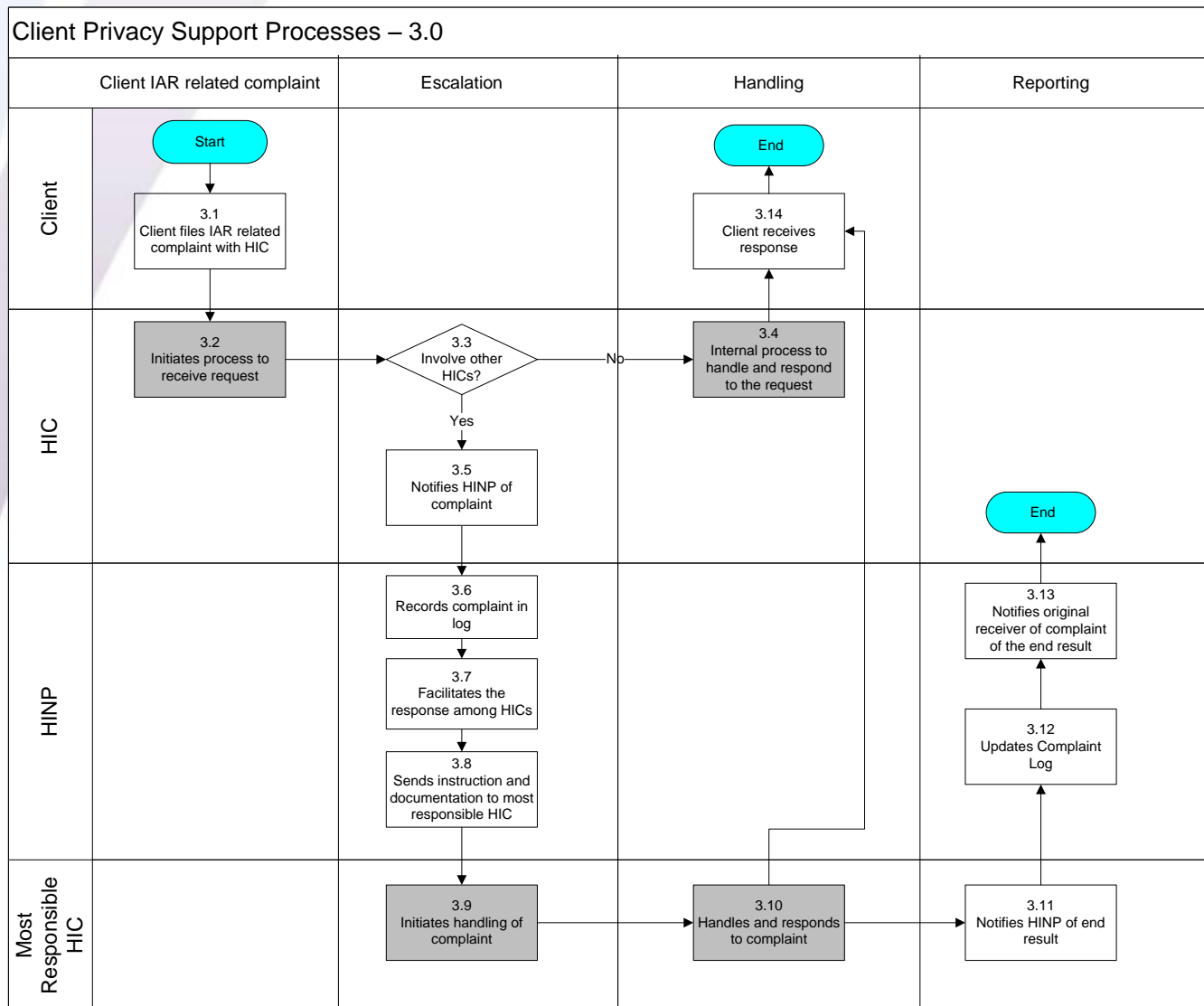


## 2.0 – Request a Correction to Assessment



\*Shaded boxes indicate existing steps in HSPs.

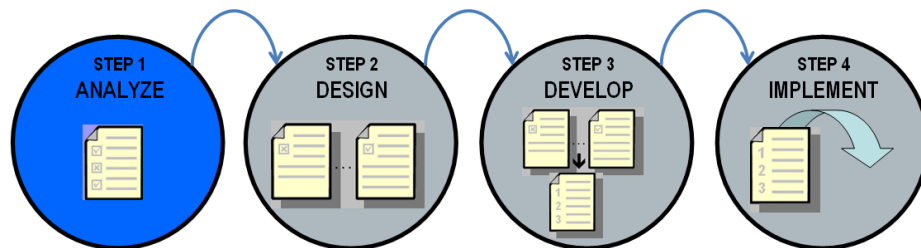
## 3.0 – File a Complaint With the HIC



\*Shaded boxes indicate existing steps in HSPs.

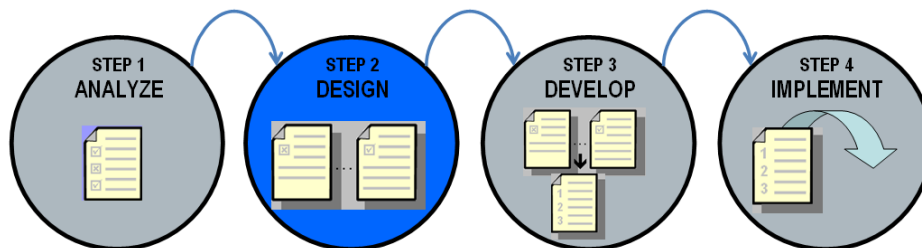
# Client Privacy Rights Support: Analyze

- Map and review existing Client Privacy Right Support process and supporting artifacts
  - Client Request Form
  - Patient Privacy Right Complaint Form
  - Patient Privacy Right Complaint Report



# Client Privacy Rights Support: Design

- Review each integration point
  - Determine if request to view / access / change involves other HSPs
  - Standard re-direct letter / form template to respond to client
  - Keep Privacy Officer contact list handy for response to client
  - Determine if the filed complaint involves other HSPs
  - Establish a communication mechanism with the HINP for escalation of privacy complaint
- Make decision on each integration point on the next slide
- Update the existing process

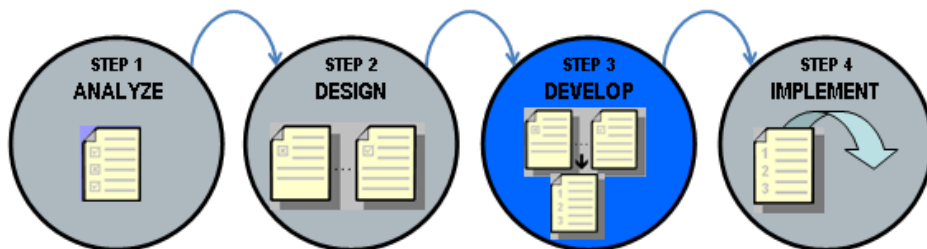


# Design Integration Points

- **Client requests a copy of an assessment**
  - How do you use IAR to determine if the request involves other assessments from HSPs?
  - Redirect client to make request to other HSPs – make use of the provided form template
- **Client requests change to assessment**
  - Use IAR to determine if request involves other HSPs
  - Review process of consulting with staff if changes can be made or not
  - Use form template to respond to client
- **Client files privacy complaint**
  - Who reviews complaint and determines if other HSPs are involved?
  - Review communication mechanism with HINP to escalate the privacy complaint that involves other HSPs

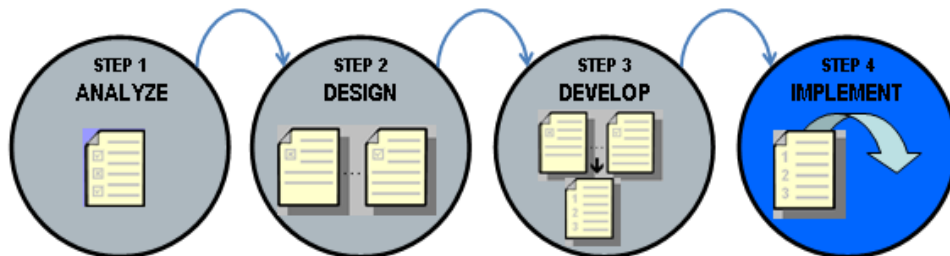
# Client Privacy Rights Support: Develop

- Review the samples provided
- Determine if you will update your existing materials:
  - Process maps
  - Client Request form, if needed
  - Client Request Response form, if needed
  - Patient Privacy Right Complaint form, if needed
  - Patient Privacy Right Complaint report, if needed



# Client Privacy Rights Support: Implement

- Show the process to senior management for approval
- Communicate the process to all staff
- Provide training and awareness to your clinical staff or health record personnel
- Establish a communication mechanism with the HINP (email or phone call)



**User  
Account  
Management**

# **User Account Management**



# IAR Roles and User Account Management

- User account management process must be established to ensure only authorized users with business need can access the IAR:
  - Users within each organization can access IAR systems only for the purpose of providing health care
  - User account request has to be reviewed and approved
  - User account must be disabled immediately when user leaves the organization

# IAR Business Roles and User Accounts: Approach

- For Continued IAR services each HSP need
  - IAR Application User Accounts
  - Business Sustainment User Roles

# IAR Application User Accounts (for HSP's)

**The IAR Application User Accounts are as follows:**

- IAR Viewer
- IAR Uploader
- IAR Privacy Officer
- WebService Uploader Account

# IAR User Account Management: Approach

- User Account Management is centralized
- IAR Support Centre at CCIM acts as the single point of contact for all HSPs participating in IAR
- HINP is responsible for all user account administration activities (creation, update, change and removal)
- Each HSP is asked to identify and submit the name of its user authority and user coordinator to CCIM

# IAR User Account Management

## HSP Responsibilities

- Each participating organization has a designated person to authorize user access to IAR called a **User Authority (UA)**
  - A UA should be someone in management or someone who has knowledge of who should use IAR
- Each participating organization has a designated contact person for day-to-day user account management activities called a **User Coordinator (UC)**
  - A UC is responsible for liaising with the Support Centre for modification or update of user details, and removal of user account when user no longer requires access

# IAR User Responsibilities

- Every IAR user has to be authorized by an HSP
- Every IAR user must read the IAR User Agreement before receiving a user account (HSP responsibility)
- Every IAR user has to read and accept the IAR User Agreement before access (on screen, upon login)
- User accounts are disabled immediately when users no longer require access

# IAR User Account Management Process Maps

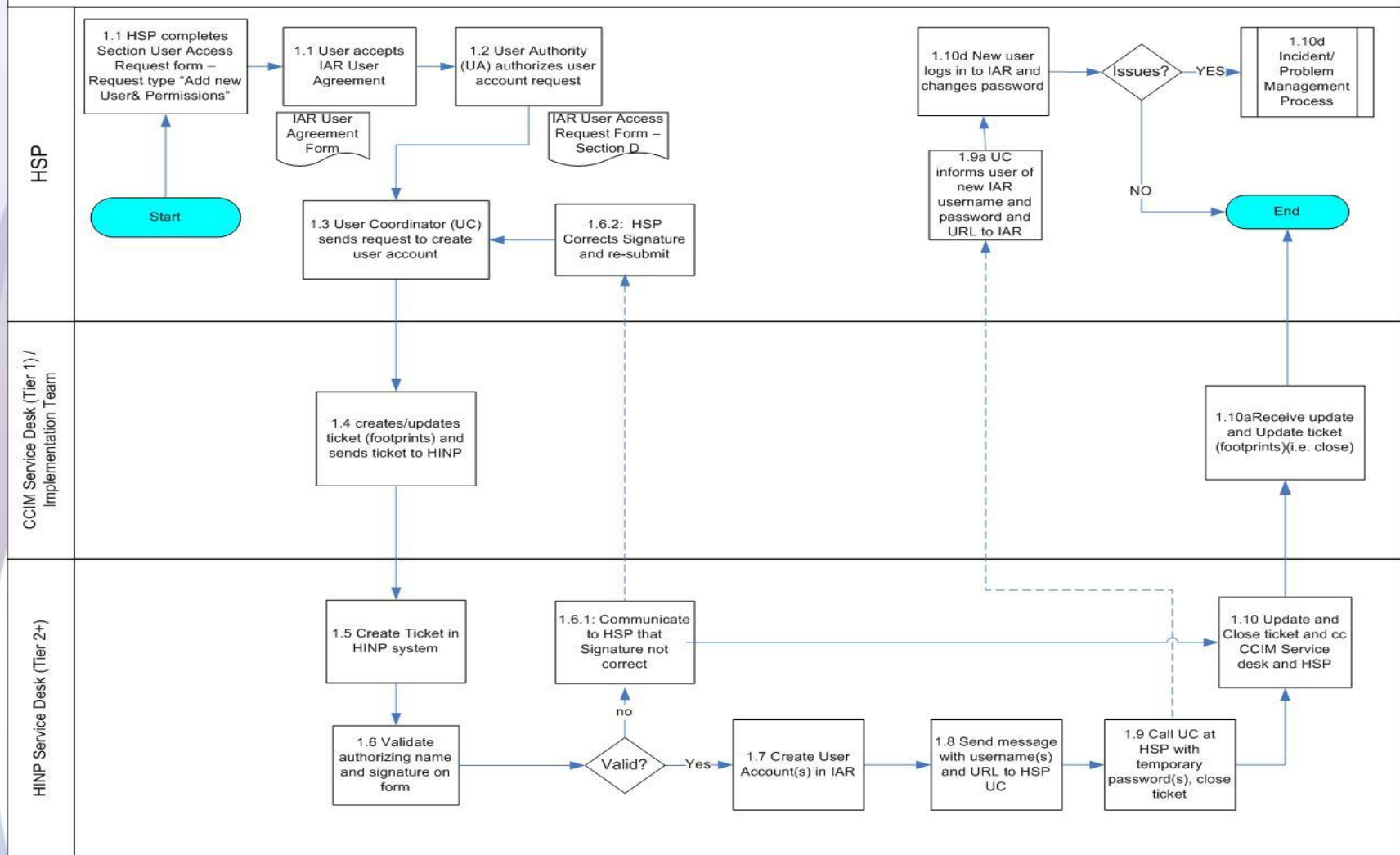
HSP can:

1. Request a new user account to access IAR
2. Request a change or update of user account information (e.g., phone number, location, email, etc.)
3. Request to remove one or multiple user accounts (e.g., user left organization, user no longer has IAR access)
4. Password Reset and Reactivate User Account

Processes are developed based on these four IAR User Account Scenarios

# 1.0 Creation of New Users

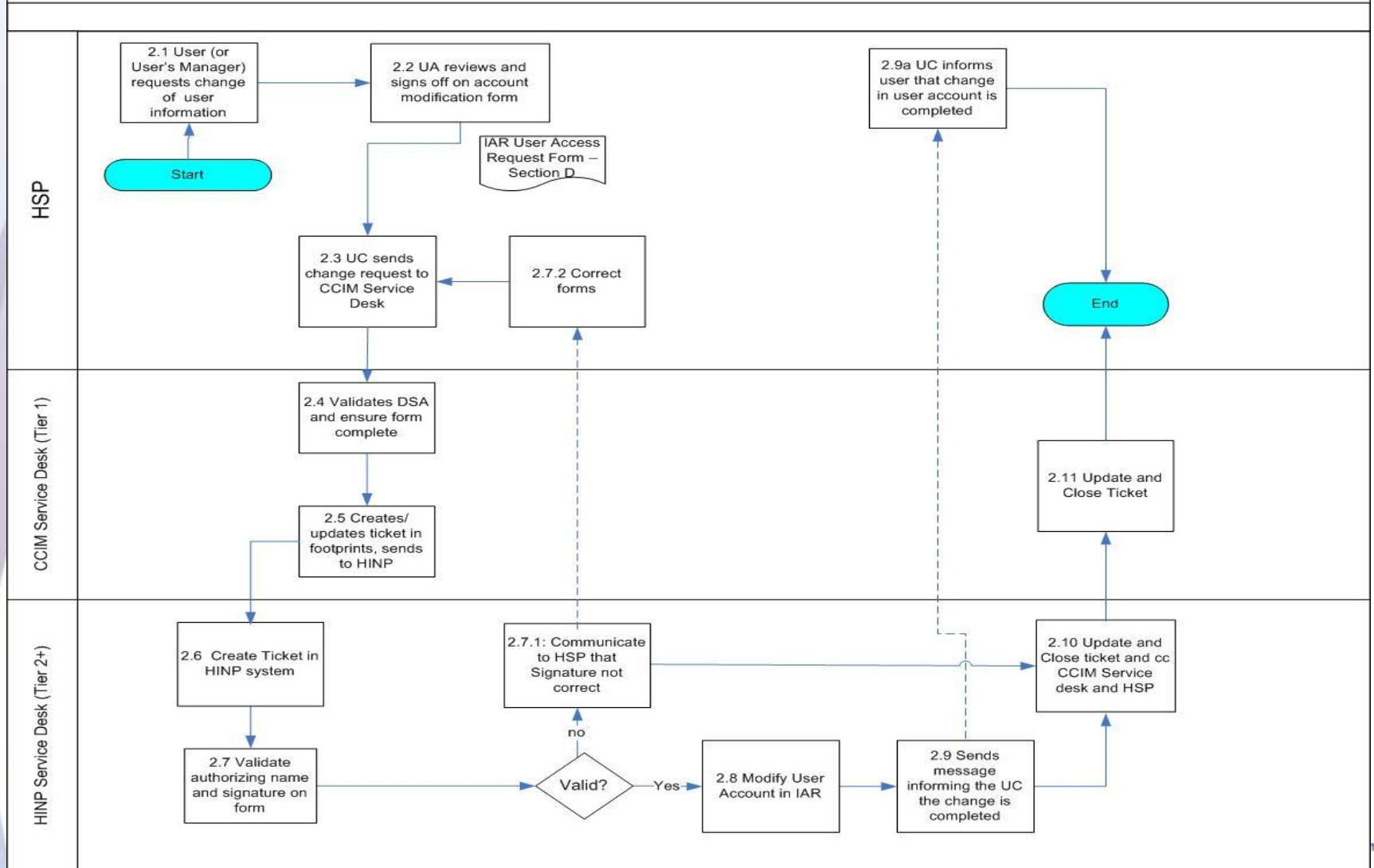
## 1.0 User Account Management – Add Users Request





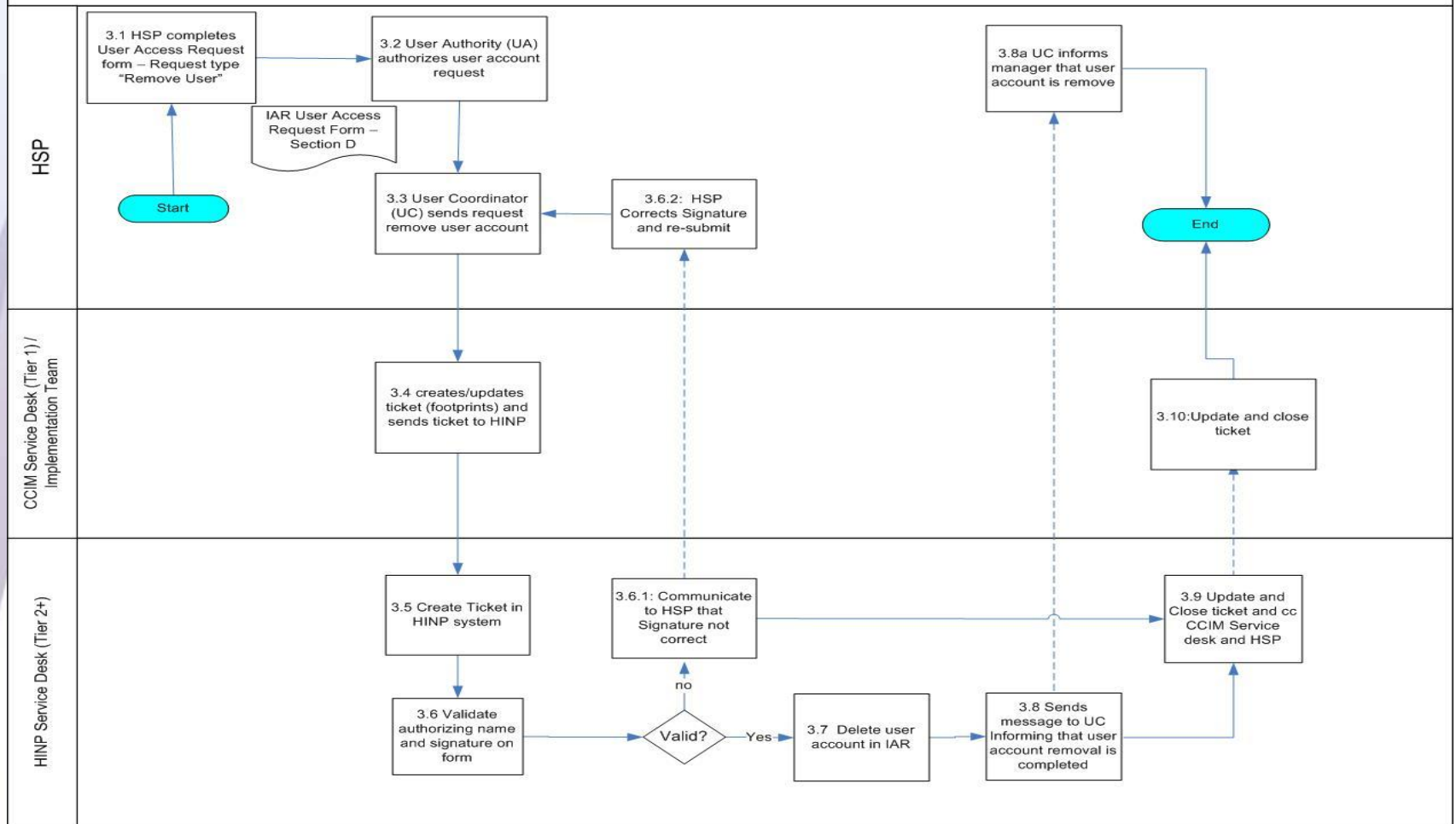
## 2.0 Request to Change

### 2.0 User Account Management – User Account Changes (Name and Permissions)



# 3.0 Removal of Users

## 3.0 User Account Management – User Removal Request





# IAR Business Sustainment Roles

- As IAR system matures several role have been identified and grouped as Business Sustainment Roles There roles are as follows:
  - User authority Role
  - User Coordinator Role
  - Privacy Officer
  - EMPI Lead (also Known as Data Quality Lead)
  - Technical Lead / WebService Contact

# IAR Business Sustainment Role Management:

- IAR Support Centre at CCIM acts as the single point of contact for all HSPs participating in IAR
- User Authority and Privacy Officer Roles cannot be filled by the same person
- HINP maintains the user list for each role at each HSP
- HSP's are Encouraged to identify backups for each role as well
- UA can Authorise Users for each role except UA roles
- Privacy Officers can Authorise UA roles

# IAR Business Sustainment Role Management HSP Responsibilities

- Each participating organization has to identify the users for each Business Sustainment Role.
  - A UA should be someone in management or someone who has knowledge of who should use IAR
  - PO will be responsible for all Privacy issues (including privacy Complaints) and privacy log Reviews
  - A UC is responsible for liaising with the Support Centre for modification or update of user details, and removal of user account when user no longer requires access
  - The EMPI lead is responsible for resolving Client (Patient) demographic issues within the EMPI
  - The Technical lead is responsible for technical issues for connecting to IAR and also for Web Services Uploader Account

# IAR Business Sustainment Role Management Process Maps

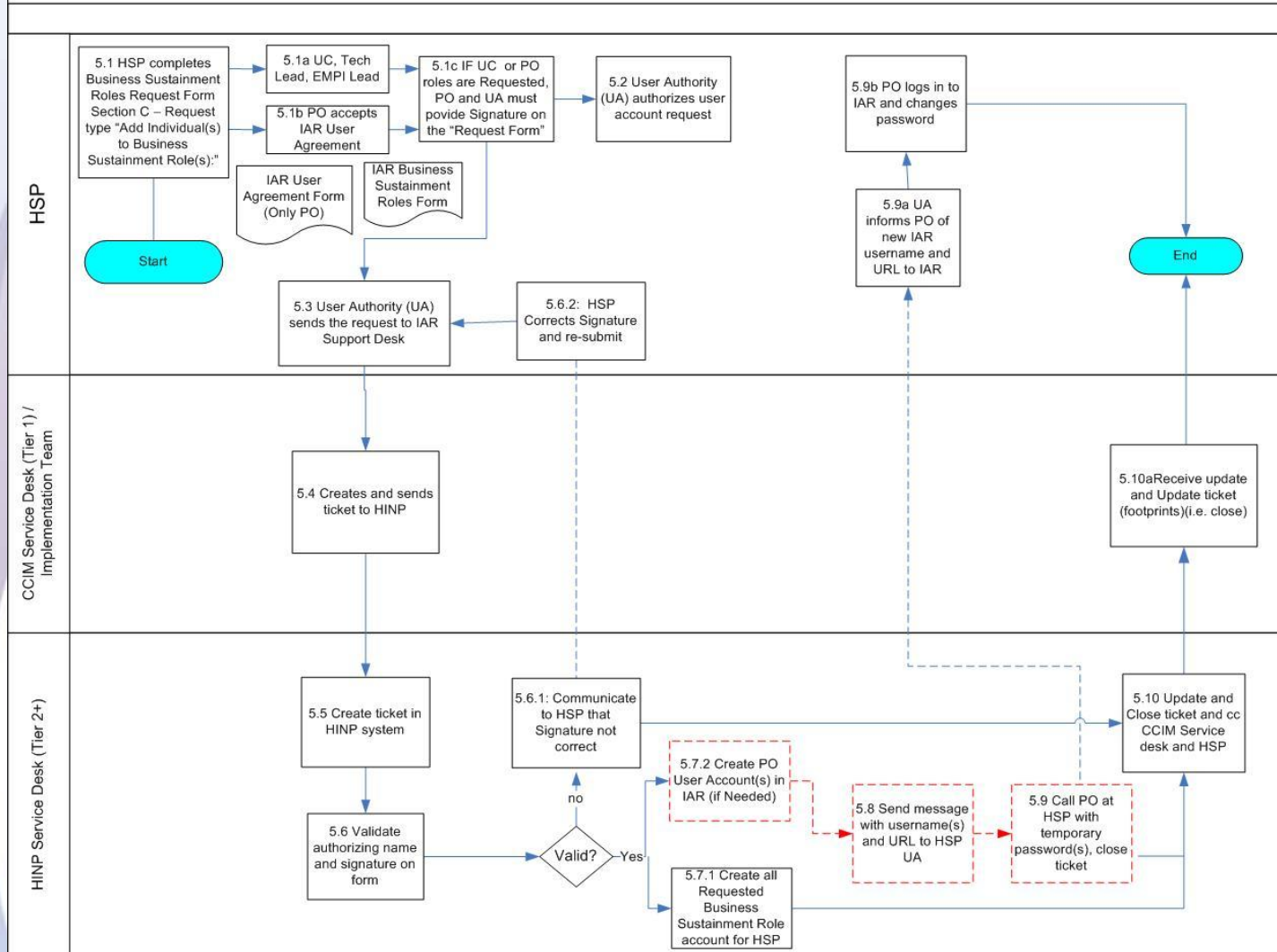
1. Add a user for any of the Business Sustainment Role except UA (e.g. PO, UC, Technical Lead, EMPI Lead)
2. Add a user for UA Role
3. Change or update of user information (e.g., phone number, location, email, etc.) for any of the Business Sustainment Role except UA
4. Change or update of user information for UA Role
5. Request to remove one or multiple users for any of the Business Sustainment Role except UA
6. Request to remove one or multiple users for UA Role

Business Sustainment Role Management processes are developed based on the above six scenarios



# 5.0 Create (or Add) All Business Sustainment Role Users (Except User Authority)

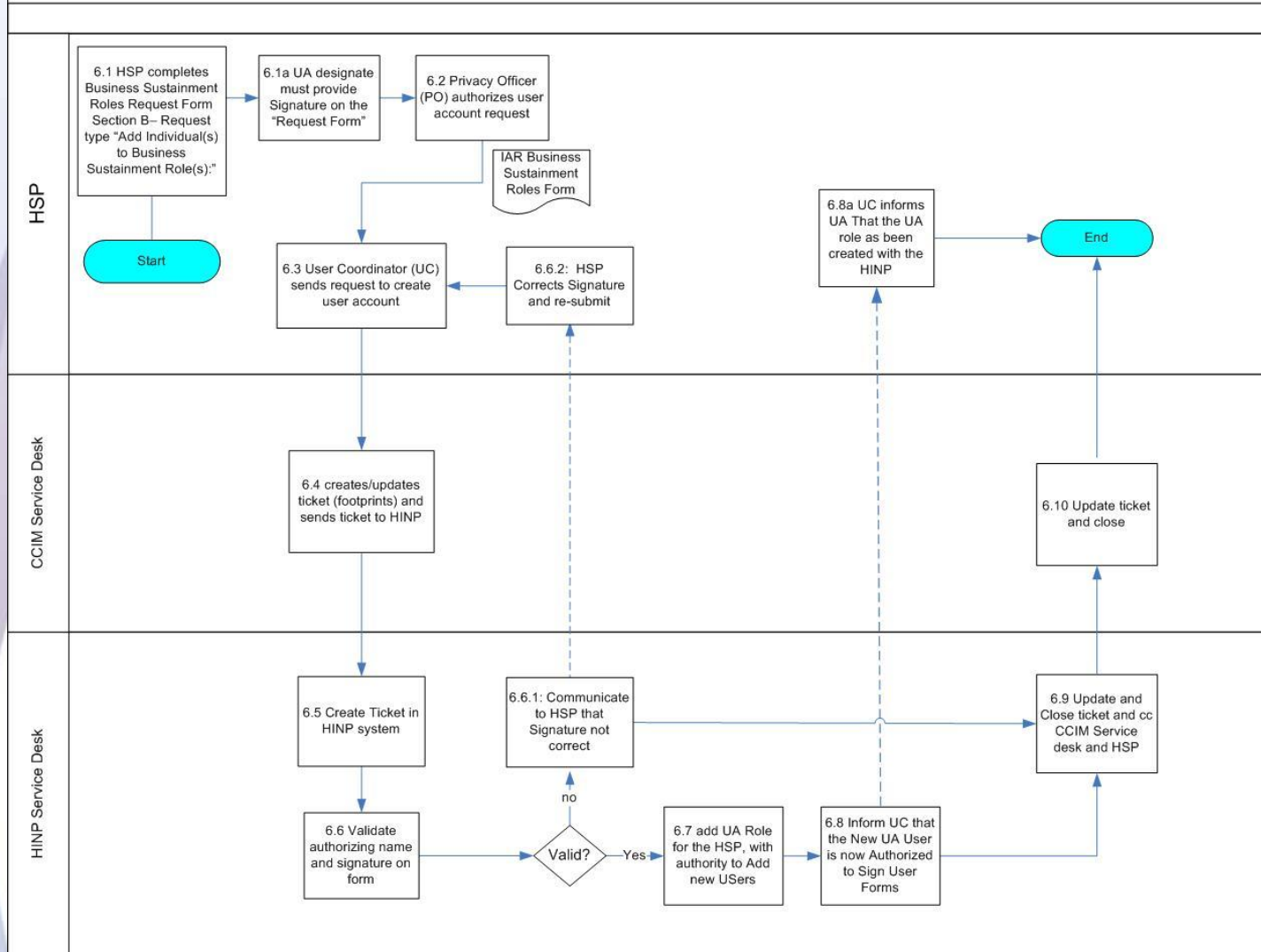
## 5.0 User Account Management – Add Users Request (All Business Sustainment Role Except User Authority)





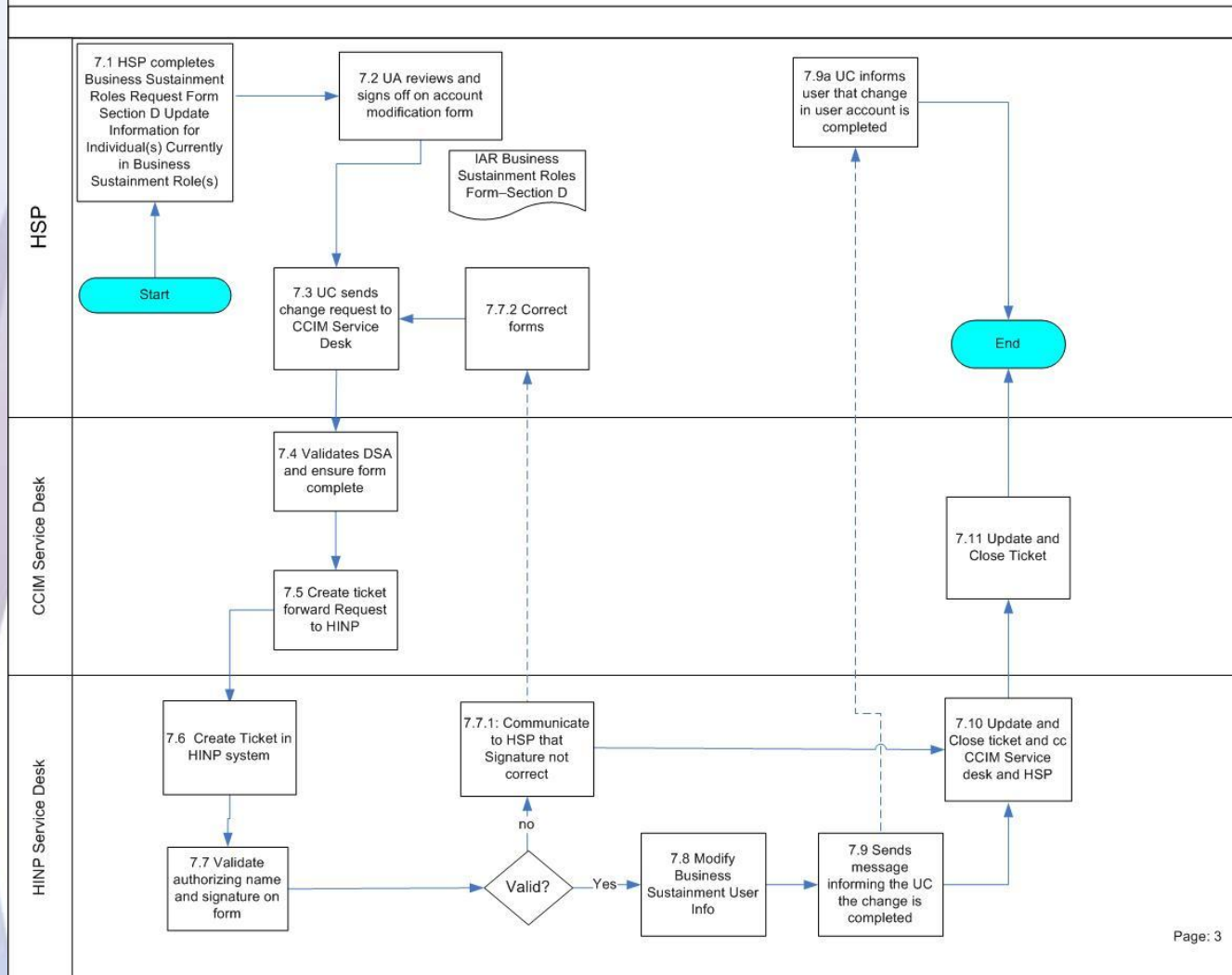
## 6.0 – Create User Authority Role User

### 6.0 User Account Management – Add Users Request (User Authority)



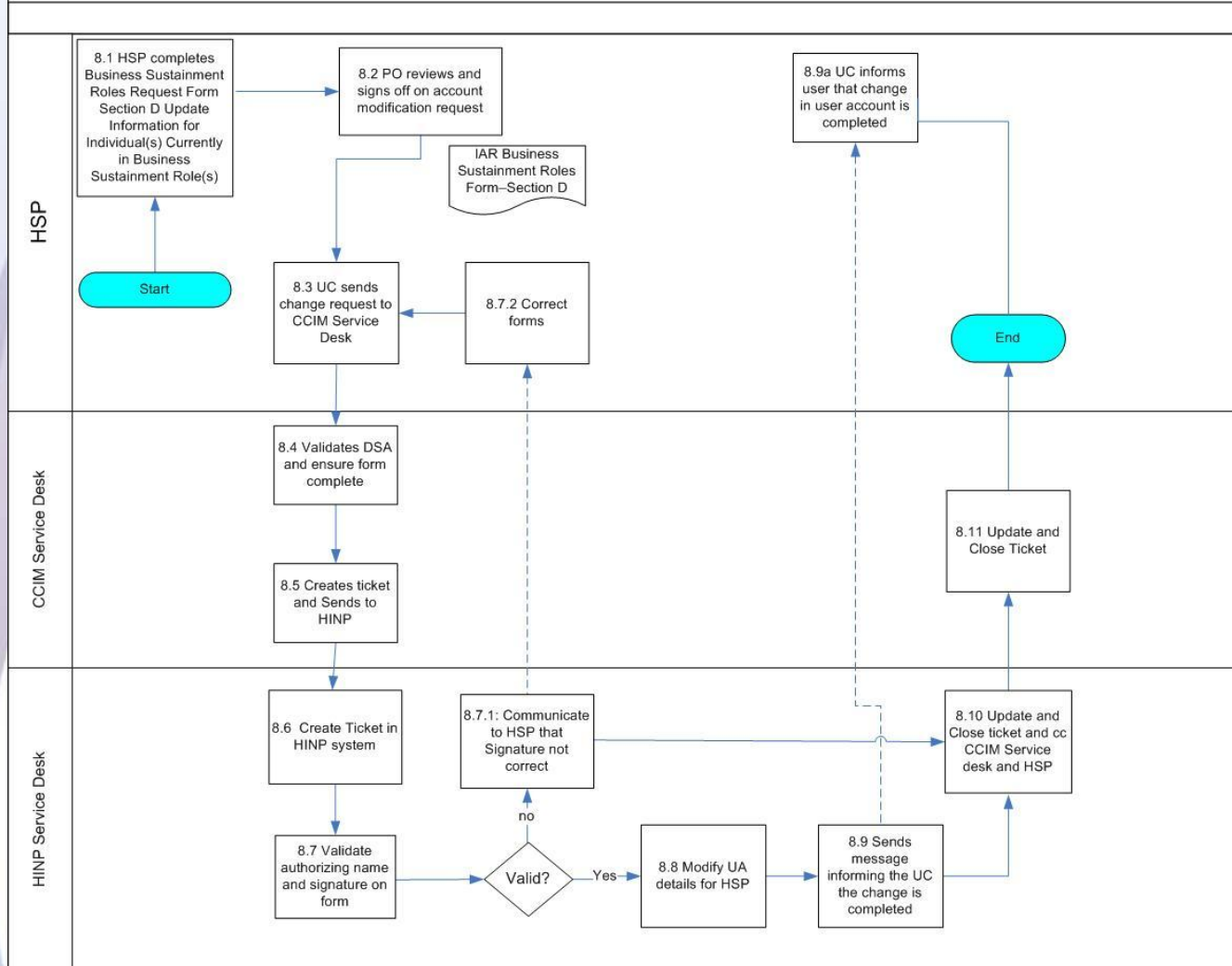
# 7.0– Update All Business Sustainment Role (Except User Authority)

## 7.0 User Account Management – Update Users Request (All Business Sustainment Role Except User Authority)



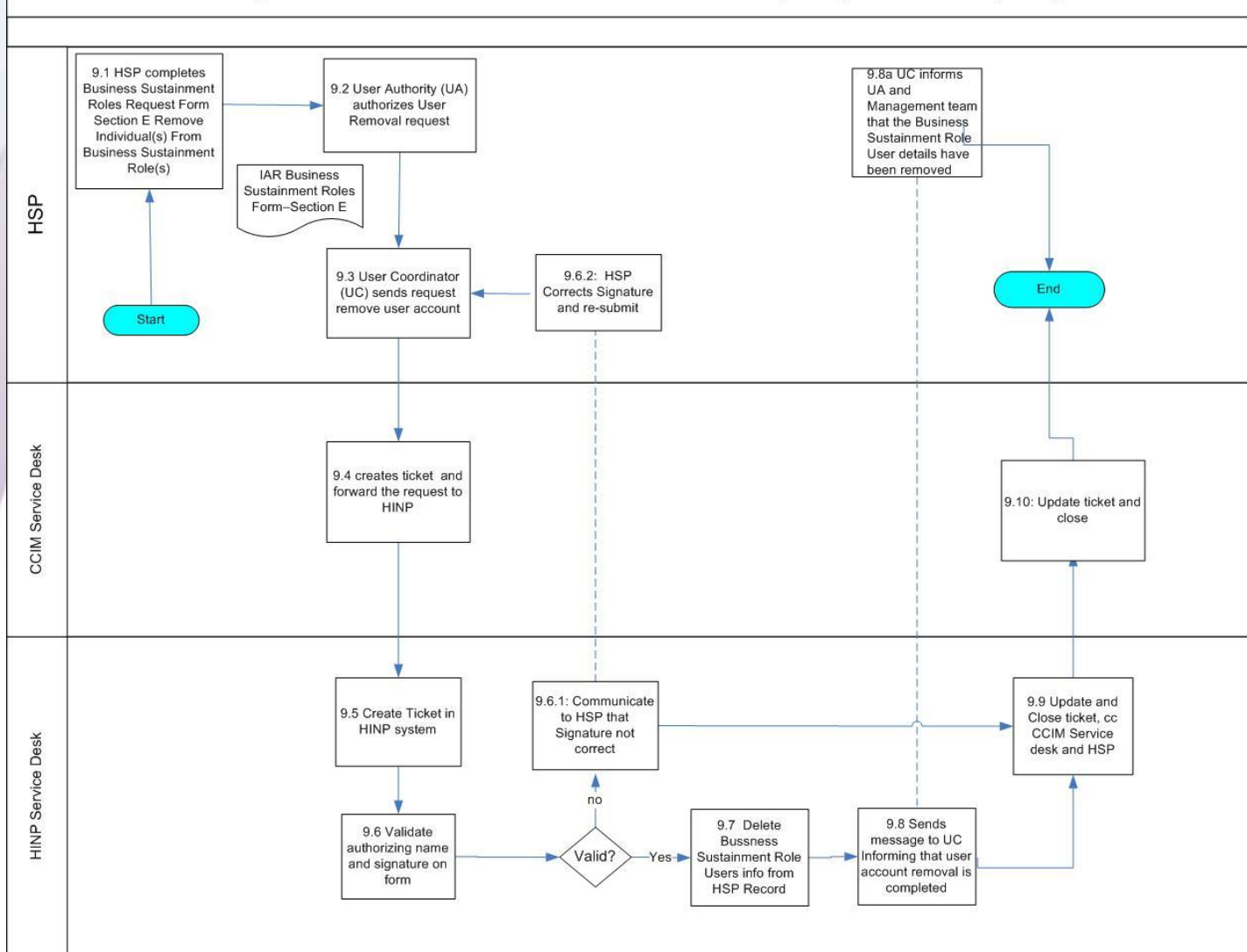
# 8.0 – Update (or Change) User Authority Role User

## 8.0 User Account Management – Update UA Request (Business Sustainment Role)



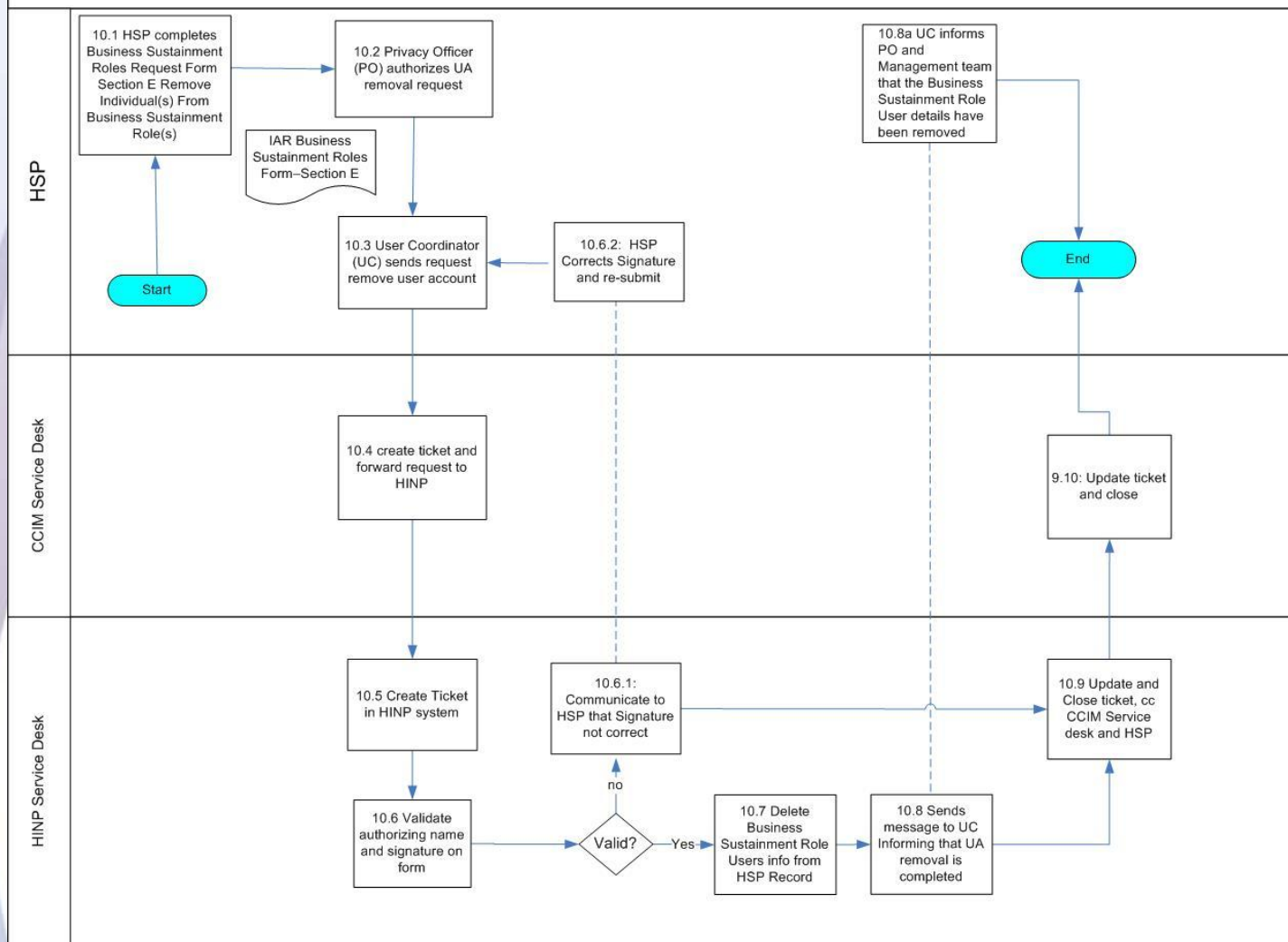
# 9.0 – Remove All Business Sustainment Role (Except User Authority)

9.0 User Account Management – Business Sustainment User Removal Request (All Roles Except UA)



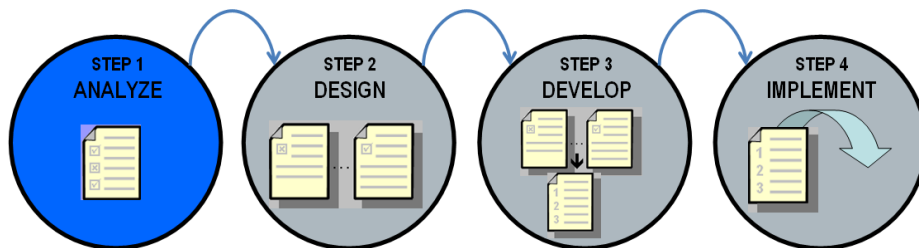
# 10.0 – Remove User Authority Role User

## 10.0 User Account Management – UA Removal Request



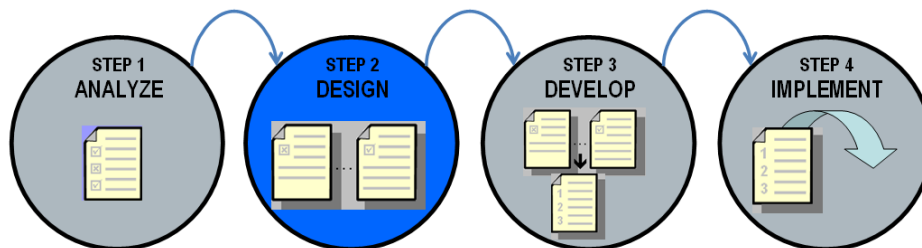
# User Account Management: Analyze

- Map and review existing User Account Management process
  - How are current IT user accounts being provisioned?
  - Are there any existing processes you can leverage?
  - Who initiates user account creation/change/removal?
  - Who authorizes user account creation?
  - Who authorizes user account change or removal?



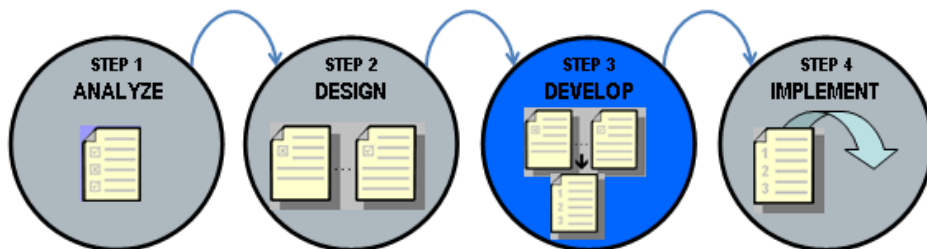
# User Account Management: Design Integration Points

- Creating new user account after implementation (non-bulk)
- Changing user details, such as phone number, work locations, or name
- Remove user account when user no longer requires IAR access (e.g., due to change of job function or departure from the organization)



# User Account Management: Develop

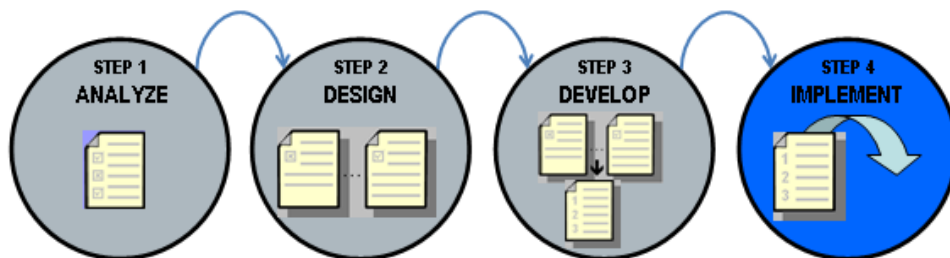
- Obtain decisions on each integration point
  - Who is to be the User Authority?
  - Who is to be the User Coordinator?
  - Do you need multiple UAs and/or UCs?
- Get your Executive Lead to appoint the UA and UC
- Update the existing IT account provision process (if needed)





# User Account Management: Implement

- Approve the process by senior management
- Communicate the process to all staff
- Provide training and awareness to the User Authority (UA) and User Coordinator (UC), and perhaps all IAR users



# Integrated Assessment Record

**P&S  
Audit  
Log  
Review**

## Privacy and Security Audit Log Review

# Privacy and Security Audit Log Review

## Why is it Important?

- Enhanced public awareness (media attention - audit log reviews help protect privacy)
- *The Personal Health Information Protection Act* (PHIPA) requires custodians to take steps to ensure that personal health information (PHI) in their custody or control is protected against theft, loss and unauthorized use or disclosure. An audit log is recognized as an important tool to meet this legislated requirement

# Privacy and Security Audit Log Review

## Why is it Important?

- The Information and Privacy Commissioner has produced a paper called 'Detecting and Deterring Unauthorized Access to Personal Health Information'. The paper states that 'logging, auditing and monitoring is an effective deterrent to unauthorized access', and goes further to state that 'Custodians should develop a policy and procedures for logging, auditing and monitoring all electronic information systems containing personal health information'

# Fact and Misconception about IAR Logging and Auditing

- **Facts:**

- HSPs are consistently required to meet expectations set out by IAR DSA, PHIPA and various IPC guidelines

- **Misconception**

- HSPs believe that auditing is not required on a regular basis or is beyond their capability or is someone else's responsibility

# Privacy and Security Audit Log Review

## Supporting Information

- Organizations must have controls in place that regulate access to sensitive IAR Assessments including CCP data, and procedures to regularly review IAR (CCT Viewer) audit logs and user access activity
- Privacy and security audit logs and reports play an important role in access review and breach investigations. An audit log review process must be established to identify privacy breaches and/or security incidents

# Privacy and Security Audit Log Review

## Supporting Information

- **HIC:** Organizational level privacy logs should be reviewed by local Privacy Officers regularly, depending on the volume and perceived risk level, to detect unauthorized access to PHI
- **HINP:** Global privacy logs should be reviewed for investigation purposes only by HINP Privacy Officers (e.g. if an incident occurs and a HINP needs to perform an investigation). Security event logs should be reviewed daily or weekly by a HINP Administrator to detect errors or security incidents

# Privacy & Security Log Review Guidelines

- Privacy & security audit log review is conducted by HSPs and HINPs
  - HSP Privacy Officer reviews local audit logs and reports for potential incidents
- HINPs are involved if the log review at the HSP uncovers an incident requiring the HINP to assist in the investigation
- A HINP Privacy Officer reviews audit logs for potential incidents that affect the IAR and the HINP IT infrastructure
  - HINP communicates to HSP if an incident is uncovered at the HINP that affects other HSPs (*\*this triggers the Integrated Incident Management process*)



# Privacy & Security Log Review Guidelines

- Establish a review schedule and routine
- Understand user activity baseline
- Look for out-of-ordinary activities and events:
  - Unauthorized access
  - Excessive client searches
  - Excessive assessment searches

# Privacy & Security Log Review Guidelines

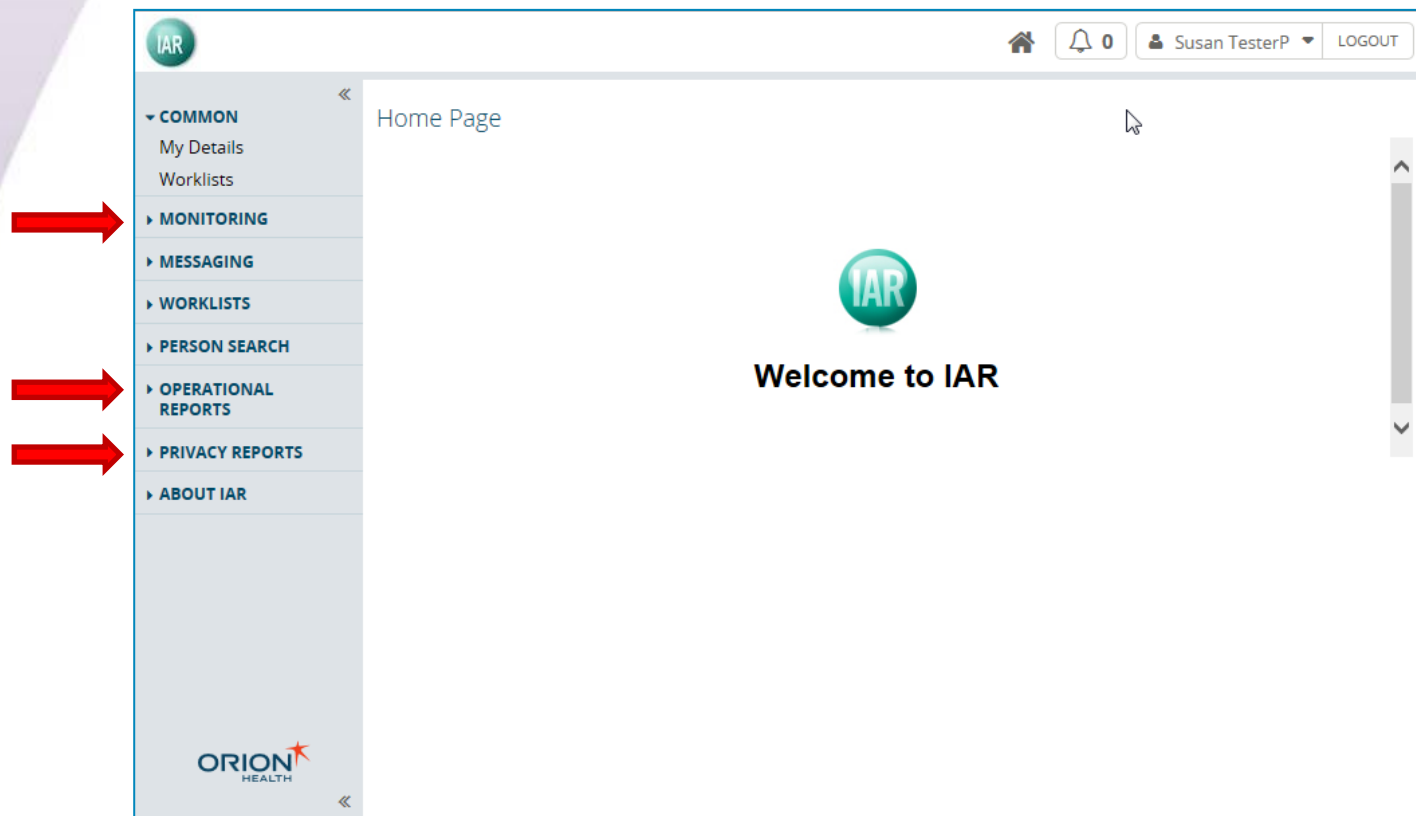
- Normal Privacy and Security audit log review activities:
  - Review the operations reports on a regular basis suited to your organization's need
  - Review the Privacy reports on a regular basis to ensure user activities are within the baselines established for them
  - Check the logs for any out-of-the ordinary activities
  - Review PS8 to review inactive users who have not logged in for over 90 days

# Privacy & Security Log Review Guidelines

- Advanced log review activities
  - Review privacy logs
  - Review clinical logs
  - Review logins by users who have not logged in for over 90 days
  - Review PS5 report with users to validate they only accessed PHI in the course of providing healthcare to clients

# Logs and Reports Available to HSP Privacy Officers

- Monitoring tab
- Operational reports
- Privacy reports



# IAR Reports Disclaimer

Please review the disclaimer at the bottom of each privacy report. It is important and constitute legal obligation while reviewing the Privacy Reports.

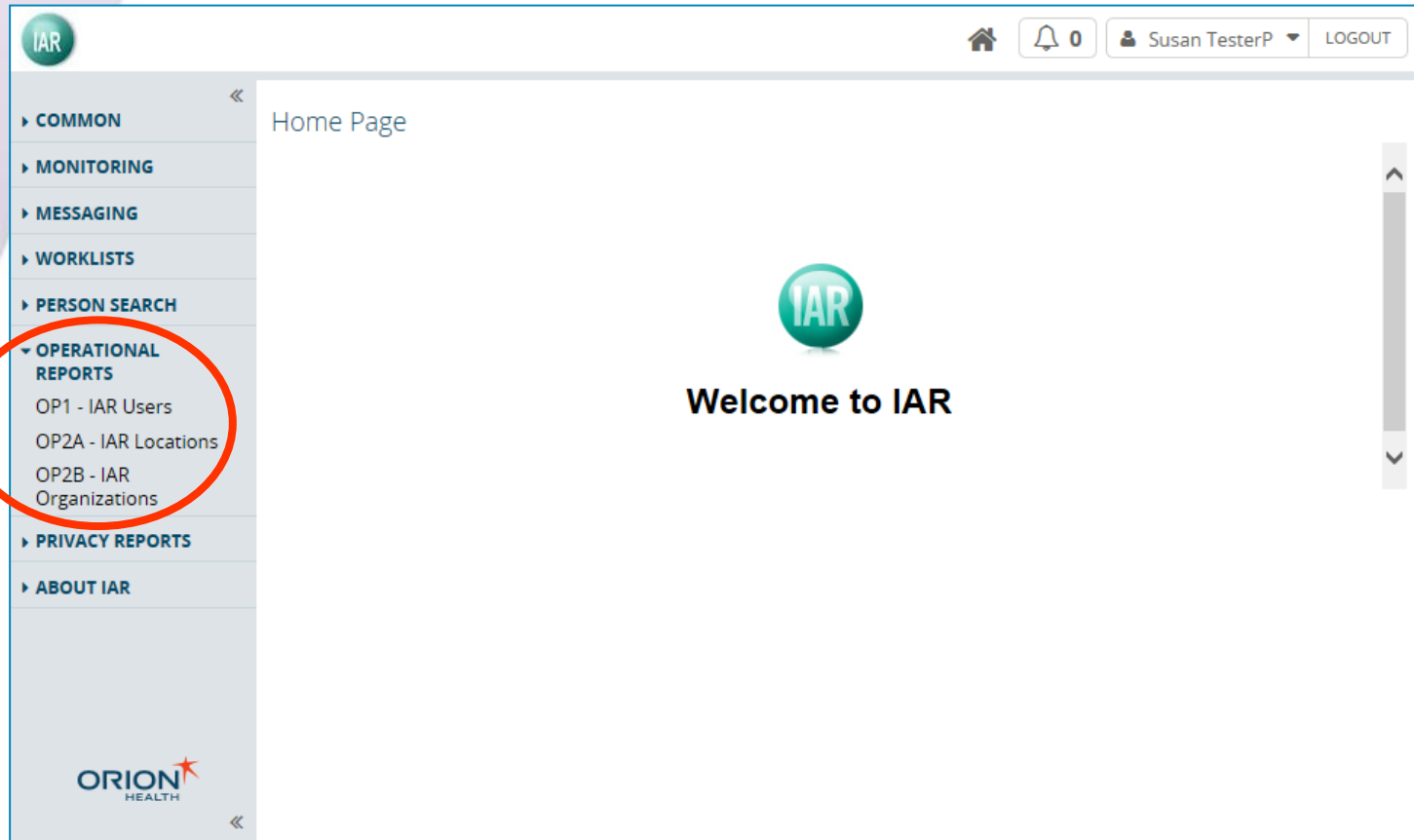
[« Previous](#) | [Next »](#)

Results 1-25 of 186 [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

# Operational Reports

- OP1 – List of IAR Users
- OP2 A – List of IAR Locations
- OP2 B – List of IAR Organizations



# OP1 – List of IAR Users

OP1 - IAR Users

Organization

CMHA-Simcoe County Branch

LHIN

User Status

All

Role

Last Login Date

From:

To:

User ID

☒ 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
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Central Privacy Officer	cpo_DK		Enabled	01 Nov 2013 09:26:23		3	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Privacy Officer	AIPrivacyLocal	, Umar	Enabled	17 Mar 2014 15:19:03	alan.lyons@ccim.on.ca	4	1
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Privacy Officer	Susan.TesterPrivacyOfficer	TesterP, Susan	Enabled	07 Oct 2016 14:13:03		6	11
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	Susan.TesterUploader	TesterU, Susan	Enabled	06 Oct 2016 15:14:41		17	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	auploader	uploader, Adrian's	Disabled	21 Sep 2010 14:05:44		4	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	uploader	Uploader, IAR	Disabled	06 May 2011 10:32:16	aslam.chagani@xwave.com	512	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	uploaderuploadernicholas		Disabled	22 Nov 2010 12:59:00		1	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	uploaderuploaderuploaderuploader		Disabled	29 Sep 2011 10:25:21		2	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	TestUpload	Upload, Test	Enabled			347	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	cuv	uploader/viewer, ccim	Enabled	08 Sep 2016 10:28:55	manuela.palcu@gmail.com	4624	2688
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	cuvDK		Enabled	20 Sep 2016 14:15:35	jason.hsiung@ccim.on.ca	218	219
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	cuv_MP	uploader, viewer	Enabled	21 Sep 2016 10:13:13	manuela.palcu@ccim.on.ca	680	504
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	dtran		Enabled	20 Sep 2016 09:45:52		391	94
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Viewer;Uploader	cuvLHIN_11	Uploader/Viewer, LHIN11	Enabled	16 May 2013 12:01:59		33	6
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Viewer;Uploader	cuv_JH	Uploader, Viewer	Enabled	21 Sep 2016 11:01:46	Jason.Hsiung@ccim.on.ca	81	74

Results 1-15

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

OP1 - IAR Users

Organization

CMHA-Simcoe County Branch

LHIN

User Status

All

Role

Last Login Date

From:

To:

User ID

☒ 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
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Central Privacy Officer	cpo_DK		Enabled	01 Nov 2013 09:26:23		3	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Privacy Officer	AIPrivacyLocal	, Umar	Enabled	17 Mar 2014 15:19:03	alan.lyons@ccim.on.ca	4	1
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Privacy Officer	Susan.TesterPrivacyOfficer	TesterP, Susan	Enabled	07 Oct 2016 14:13:03		6	11
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	Susan.TesterUploader	TesterU, Susan	Enabled	06 Oct 2016 15:14:41		17	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	auploader	uploader, Adrian's	Disabled	21 Sep 2010 14:05:44		4	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	uploader	Uploader, IAR	Disabled	06 May 2011 10:32:16	aslam.chagani@xwave.com	512	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	uploaderuploadernicholas		Disabled	22 Nov 2010 12:59:00		1	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader	uploaderuploaderuploaderuploader		Disabled	29 Sep 2011 10:25:21		2	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	TestUpload	Upload, Test	Enabled			347	0
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	cuv	uploader/viewer, ccim	Enabled	08 Sep 2016 10:28:55	manuela.palcu@gmail.com	4624	2688
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	cuvDK		Enabled	20 Sep 2016 14:15:35	jason.hsiung@ccim.on.ca	218	219
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	cuv_MP	uploader, viewer	Enabled	21 Sep 2016 10:13:13	manuela.palcu@ccim.on.ca	680	504
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Uploader;Viewer	dtran		Enabled	20 Sep 2016 09:45:52		391	94
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Viewer;Uploader	cuvLHIN_11	Uploader/Viewer, LHIN11	Enabled	16 May 2013 12:01:59		33	6
396	CMHA-Simcoe County Branch	12-North Simcoe Muskoka	Viewer;Uploader	cuv_JH	Uploader, Viewer	Enabled	21 Sep 2016 11:01:46	Jason.Hsiung@ccim.on.ca	81	74


Results 1-15

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

ORION  
HEALTH

CCIM  Community  
Care  
Information  
Management  
ACCESS TO INFORMATION

127

## OP2A — List of IAR Locations

OP2A - IAR Locations

IP Address

Location Name

Search

Reset

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 - Enaahitg 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
781 - ST. JOSEPH'S CARE GROUP		11337745
935 - THUNDER BAY REGIONAL HEALTH SCIENCES CENTRE		11337746
959 - HOPITAL REGIONAL DE SUDBURY REGIONAL HOSPITAL		11337735
965 - SAULT AREA HOSPITAL		11337738
972 - Mental Health Centre Penetanguishene-Regional Division		11337741
Everywhere	***	262145

Results 1-19

Printer Friendly Version

Download CSV results

OP2A - IAR Locations

IP Address

Location Name

Search

Reset

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 - Enaahitg 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
781 - ST. JOSEPH'S CARE GROUP		11337745
935 - THUNDER BAY REGIONAL HEALTH SCIENCES CENTRE		11337746
959 - HOPITAL REGIONAL DE SUDBURY REGIONAL HOSPITAL		11337735
965 - SAULT AREA HOSPITAL		11337738
972 - Mental Health Centre Penetanguishene-Regional Division		11337741
Everywhere	***	262145

Results 1-19

Printer Friendly Version

Download CSV results

OP2A - IAR Locations

IP Address

Location Name

Search

Reset

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 - Enaahitg 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
781 - ST. JOSEPH'S CARE GROUP		11337745
935 - THUNDER BAY REGIONAL HEALTH SCIENCES CENTRE		11337746
959 - HOPITAL REGIONAL DE SUDBURY REGIONAL HOSPITAL		11337735
965 - SAULT AREA HOSPITAL		11337738
972 - Mental Health Centre Penetanguishene-Regional Division		11337741
Everywhere	***	262145

Results 1-19

Printer Friendly Version

Download CSV results



# OP2B — List of IAR Organizations

- COMMON
- MONITORING
- MESSAGING
- WORKLISTS
- PERSON SEARCH
- OPERATIONAL REPORTS
  - OP1 - IAR Users
  - OP2A - IAR Locations
  - OP2B - IAR Organizations**
- PRIVACY REPORTS
- ABOUT IAR

[LOGOUT](#)

## OP2B - IAR Organizations

Organization 
LHIN

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

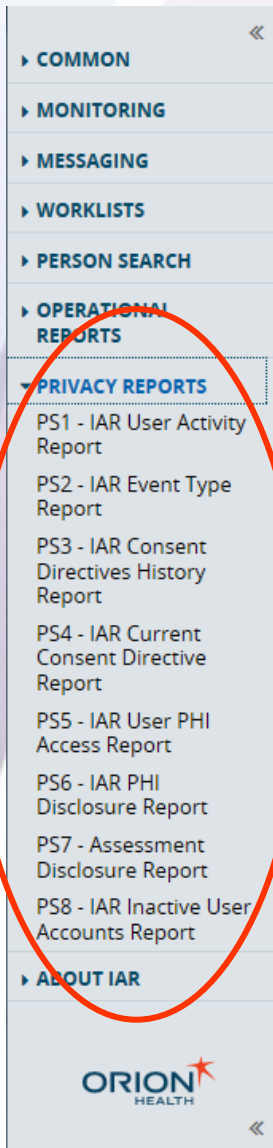
Organization ID	Organization Name	LHIN	Date Activated	Date Deactivated	GMT Offset
317	NORTH SHORE COMMUNITY SUPPORT SERVICES, INC. (NSCSS)	13-North East	19-Jul-2010		GMT -05:00
3177	Dummy Org 3177 for testing	14-North West	20-Jun-2012		GMT -05:00
3360	Dummy Org 3360 for testing	14-North West	20-Jun-2012		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
781	ST. JOSEPH'S CARE GROUP	14-North West	19-Jul-2010		GMT -05:00
790	790 TEST	11-Champlain	10-Sep-2012		GMT -05:00
791	791 TEST	11-Champlain	10-Sep-2012		GMT -05:00
935	THUNDER BAY REGIONAL HEALTH SCIENCES CENTRE	14-North West	19-Jul-2010		GMT -05:00
959	HOPITAL REGIONAL DE SUDBURY REGIONAL HOSPITAL	13-North East	19-Jul-2010		GMT -05:00
965	SAULT AREA HOSPITAL	13-North East	19-Jul-2010		GMT -05:00
972	Mental Health Centre Penetanguishene-Regional Division	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00
A12	Test Alphanumeric Short	11-Champlain	28-Jul-2011		GMT -05:00

[« Previous](#)
[Next »](#)

Results 1-25 of 26
[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

# Privacy Reports



- 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 Query
- PS8 – Inactive Users Accounts Report

# PS1 – User Activity Report

COMMON

MONITORING

MESSAGING

WORKLISTS

PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

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

PS1 - IAR User Activity Report

Date Range From: 30-09-2016 To: 07-10-2016

Search Reset

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.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584407			Search Performed	IAR - Person Registry, Person Search	Success	07 Oct 2016 10:26:35
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584408			Search Performed	IAR - Person Registry, Person Search	Success	07 Oct 2016 10:27:17
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584411			Search Performed	IAR - Person Registry, Person Search	Success	07 Oct 2016 10:27:45
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584413	552	Cantor Amy	Context Change	Patient	Success	07 Oct 2016 10:29:37
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584415	552	Cantor Amy	Open Application	IAR - User Homepage, Summary View	Success	07 Oct 2016 10:29:37
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584412			Search Performed	IAR - Person Registry, Person Search	Success	07 Oct 2016 10:29:37
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584427			Search Performed	IAR - Person Registry, Person Search	Success	07 Oct 2016 10:31:40
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584496			Search Performed	IAR - Person Registry, Person Search	Success	07 Oct 2016 10:36:52

ACCESS TO INFORMATION

131

# PS2 – Event Type Report

COMMON

MONITORING

MESSAGING

WORKLISTS

PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

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

PS2 - IAR Event Type Report

Date Range \* From: 30-09-2016 To: 07-10-2016 Event Status

All Logins
Failed Logins
Successful Logins

Search Reset

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	584396	User Authentication	Susan.TesterPrivacyOfficer	Success	07 Oct 2016 10:26:25
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584488	User Authentication	Susan.TesterPrivacyOfficer	Success	07 Oct 2016 10:36:45
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584547	User Authentication	Susan.TesterPrivacyOfficer	Success	07 Oct 2016 10:41:35
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584612	User Authentication	Susan.TesterPrivacyOfficer	Success	07 Oct 2016 10:49:15
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584631	User Authentication	Susan.TesterPrivacyOfficer	Invalid login attempt	07 Oct 2016 14:12:41
Susan.TesterPrivacyOfficer	TesterP, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch	-	Privacy Officer;	Enabled	10.41.0.98	584637	User Authentication	Susan.TesterPrivacyOfficer	Success	07 Oct 2016 14:13:16
Susan.TesterUploader	TesterU, Susan	345   ALPHA COURT NON-PROFIT HOUSING CORPORATION; 396   CMHA-Simcoe County Branch; 463   CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY; 651   ROYAL OTTAWA HEALTH CARE GROUP; 763   PEMBROKE REGIONAL HOSPITAL NewName: Concerto; 781   ST. JOSEPH'S CARE GROUP;	-	Uploader;	Enabled	10.41.0.98	582464	User Authentication	Susan.TesterUploader	Invalid login attempt	30 Sep 2016 09:38:02

# PS3 – IAR Consent Directives History Report

- COMMON
- MONITORING
- MESSAGING
- WORKLISTS
- PERSON SEARCH
- OPERATIONAL REPORTS
- PRIVACY REPORTS
  - 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

Susan TesterP
LOGOUT

## PS3 - IAR Consent Directives History Report

Person Search Bosh, Chris; 
Date Range From: 08-10-2015 To: 07-10-2016

Search
Reset


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		1504	Bosh, Chris		IAR		GRANT			07 Oct 2016 10:41:03
IAR		1504	Bosh, Chris		IAR		DENY			07 Oct 2016 10:40:57
IAR		1504	Bosh, Chris		IAR		GRANT			07 Oct 2016 10:39:07
IAR		1504	Bosh, Chris		IAR		DENY			07 Oct 2016 10:35:28

Results 1-4
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

# PS3 – IAR Consent Directives History Report

## Search Criteria Options

Home 0 Susan TesterP LOGOUT

- COMMON
- MONITORING
- MESSAGING
- WORKLISTS
- PERSON SEARCH
- OPERATIONAL REPORTS
- PRIVACY REPORTS
  - 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

### PS3 - IAR Consent Directives History Report

Person Search \*  Date Range \* From: 08-10-2015 To: 07-10-2016

Enter search criteria about

#### Criteria - Person Search

Select a favorite search

Ontario Health Card Number \*

OR Person Attribute Search

Last Name \*  First Name \*

Date of Birth \*   ☒

Sex

Street

Unit/Suite/Apt.

Postal/Zip Code

Phone

Score	Health Card Number	Last Name	First Name	Alias	Sex	Date of Birth	City	Phone
5.4	5254562399	Bosh	Chris		Male	11-Jul-1959	Toronto	4161112244

Results 1-1

# PS4 – IAR Current Consent Directive Report

- COMMON
- MONITORING
- MESSAGING
- WORKLISTS
- PERSON SEARCH
- OPERATIONAL REPORTS
- PRIVACY REPORTS
  - 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

Susan TesterP
LOGOUT

## PS4 - IAR Current Consent Directive Report

Person Search Bosh, Chris;

Search
Reset

Organization ID	Organization Name	Person ID	Person Name	Alias Name	Consent Directive Type	Assessment ID	Consent Directive	Data Feed Support	Request Date	Effective Date
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	9110225	GRANT	UNSUPPORTED	29 Nov 2011	29 Nov 2011 14:19:13
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	9110224	GRANT	UNSUPPORTED	29 Nov 2011	29 Nov 2011 14:19:13
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	33174121	DENY	UNSUPPORTED	24 Nov 2011	24 Nov 2011 10:51:02
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	9110223	DENY	UNSUPPORTED	23 Nov 2011	24 Nov 2011 14:24:43
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	33174122	GRANT	UNSUPPORTED	23 Nov 2011	24 Nov 2011 10:48:34
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	9110222	GRANT	UNSUPPORTED	23 Nov 2011	24 Nov 2011 10:06:34
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	9110221	DENY	UNSUPPORTED	23 Nov 2011	24 Nov 2011 10:06:34
345	ALPHA COURT NON-PROFIT HOUSING CORPORATION	CCAA6328555122RAI-MH	Bosh, Chris		HSP	33174125	DENY	UNSUPPORTED	23 Nov 2011	24 Nov 2011 10:06:34

« Previous
Next »

Results 1-25 of 72
 [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.



# PS4 – IAR Current Consent Directive Report

## Search Criteria Options

COMMON

MONITORING

MESSAGING

WORKLISTS

PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

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

PS4 - IAR Current Consent Directive Report

Person Search

Search

Reset

Enter search criteria about

Criteria - Person Search

Select a favorite search

Ontario Health Card Number

OR Person Attribute Search

Last Name

Bosh

First Name

Chris

Date of Birth

11-07-1959

Sex

Select

Street

Postal/Zip Code

Phone

Unit/Suite/Apt.

Search

Clear

Reset

Enter a new favorite search

Score	Health Card Number	Last Name	First Name	Alias	Sex	Date of Birth	City	Phone
10.4	5254562399	Bosh	Chris		Male	11-Jul-1959	Toronto	4161112244

Results 1-1



## 137

**CCIM**  Community  
Care  
Information  
Management

ACCESS TO INFORMATION

# PS5 – User PHI Access Report

## Search Criteria Options

The screenshot displays the PS5 - IAR User PHI Access Report interface. On the left is a navigation menu with categories: COMMON, MONITORING, MESSAGING, WORKLISTS, PERSON SEARCH, OPERATIONAL REPORTS, and PRIVACY REPORTS. The PRIVACY REPORTS section is expanded, showing options like PS1 - IAR User Activity Report, PS2 - IAR Event Type Report, PS3 - IAR Consent Directives History Report, PS4 - IAR Current Consent Directive Report, and PS5 - IAR User PHI Access Report (which is selected). The main content area is titled 'PS5 - IAR User PHI Access Report'. It features a search bar with 'User ID' and a magnifying glass icon, and a date range selector set from '30-09-2016' to '07-10-2016'. Below these are 'Search' and 'Reset' buttons. A modal window titled 'Criteria - User Search' is open, showing search criteria: 'User ID' (empty), 'Full Name' (Susan), 'Last Name' (empty), 'Member of' (dropdown), and 'Show Deleted Users' (radio buttons for No and Yes, with 'No' selected). It also has 'Search' and 'Reset' buttons. Below the modal is a table with three columns: 'User ID', 'Full Name', and 'Description'. The table contains four rows of user data. At the bottom of the modal is a link for 'Printer Friendly Version'.

PS5 - IAR User PHI Access Report

User ID  Date Range From: 30-09-2016 To: 07-10-2016

Search Reset

Criteria - User Search

User ID  Member of

Full Name Susan Last Name  Show Deleted Users ☒ No ☐ Yes

Search Reset

User ID	Full Name	Description
Susan.TesterBusRep	TesterB, Susan	
Susan.TesterPrivacyOfficer	TesterP, Susan	
Susan.TesterUploader	TesterU, Susan	
Susan.TesterViewer	TesterV, Susan	

[Printer Friendly Version](#)



# PS6 – IAR PHI Disclosure Report

## Search Criteria Options

The screenshot displays the PS6 - IAR PHI Disclosure Report interface. On the left is a sidebar with a menu under 'PRIVACY REPORTS' including PS1 through PS6. PS6 - IAR PHI Disclosure Report is selected. The main area shows a search form with fields for Person Search, Date Range (30-09-2016 to 07-10-2016), and a search button. A modal window titled 'Criteria - Person Search' is open, showing various search criteria fields: Ontario Health Card Number, Last Name (Bosh), First Name (Chris), Date of Birth (11-07-1959), Sex (Select), Street, Unit/Suite/Apt., Postal/Zip Code, and Phone. Below the form is a table with one result for Chris Bosh, born 11-Jul-1959 in Toronto, with a score of 10.4. The interface also includes a top navigation bar with a home icon, a notification bell with 0 alerts, a user profile for Susan TesterP, and a logout button.

PS6 - IAR PHI Disclosure Report

Person Search \*  Date Range \* From: 30-09-2016 To: 07-10-2016

Search Reset

Enter search criteria above and hit 'Sea

### Criteria - Person Search

Select a favorite search

Ontario Health Card Number \*

OR Person Attribute Search

Last Name \*  First Name \*

Date of Birth \*   ☒ Sex

Street

Unit/Suite/Apt.

Postal/Zip Code

Phone

Search Clear Reset Enter a new favorite search

Score	Health Card Number	Last Name	First Name	Alias	Sex	Date of Birth	City	Phone
10.4	5254562399	Bosh	Chris		Male	11-Jul-1959	Toronto	4161112244

Results 1-1

# PS7 – Assessment Disclosure Report

- COMMON
- MONITORING
- MESSAGING
- WORKLISTS
- PERSON SEARCH
- OPERATIONAL REPORTS
- PRIVACY REPORTS**
  - 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

Susan TesterP
LOGOUT

## PS7 - Assessment Disclosure Report

Date Range \* From: 30-09-2016 To: 07-10-2016 Organization \* CMHA-Simcoe County Branch


Search Reset





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
akhan	khan, abdullah		-	10.41.0.101	4232	Linson Ashley		-	Context Change	Patient	Success	06 Oct 2016 12:59:10
akhan	khan, abdullah		-	10.41.0.101	4232	Linson Ashley	2255	396-CMHA-Simcoe County Branch	Open Document	OCAN - Initial OCAN	Success	06 Oct 2016 12:59:45

Results 1-2 [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

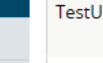
# PS8 – Inactive Users Report




 0
  Susan TesterP
  LOGOUT

<<

- ▶ COMMON
- ▶ MONITORING
- ▶ MESSAGING
- ▶ WORKLISTS
- ▶ PERSON SEARCH
- ▶ OPERATIONAL REPORTS
- ▼ PRIVACY REPORTS
  - 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



<<

## PS8 - IAR Inactive User Accounts Report

User ID	User Name	User Role	User Account Creation Date	Last Successful Login Date	Days of Inactivity	Is User Account Disabled
AlPrivacyLocal		Privacy Officer	23 Oct 2012 14:38:13	17 Mar 2014 15:19:03	935	No
AlPrivacyLocal		Privacy Officer	23 Oct 2012 14:38:13	17 Mar 2014 15:19:03	935	No
Austin		Viewer	20 Nov 2013 14:59:47		1052	No
Austin		Uploader	20 Nov 2013 14:59:47		1052	No
AustinH		Viewer	25 Nov 2013 15:14:14	26 May 2015 15:43:19	500	No
AustinH		Uploader	25 Nov 2013 15:14:14	26 May 2015 15:43:19	500	No
Oneidqaiair.privacy		Privacy Officer	12 Feb 2014 17:06:55	20 Feb 2014 12:27:25	960	Yes
Oneidqaiair.uploader@oneid.on.ca		Uploader	07 Feb 2014 16:32:02	19 Feb 2014 14:44:06	961	No
Oneidqaiair.viewer		Viewer	12 Feb 2014 17:02:13	24 Feb 2014 11:15:48	956	No
Oneidqaiair.viewer		Uploader	12 Feb 2014 17:02:13	24 Feb 2014 11:15:48	956	No
TestUpload	Test Upload	Uploader	22 Jun 2010 15:30:38		2299	No
TestUpload	Test Upload	Uploader	22 Jun 2010 15:30:38		2299	No
TestUpload	Test Upload	Viewer	22 Jun 2010 15:30:38		2299	No
TestUpload	Test Upload	Viewer	22 Jun 2010 15:30:38		2299	No

# Report Format

IAR

COMMON

MONITORING

MESSAGING

WORKLISTS

PERSON SEARCH

OPERATIONAL REPORTS

OP1 - IAR Users

OP2A - IAR Locations

OP2B - IAR Organizations

PRIVACY REPORTS

ABOUT IAR

ORION HEALTH

Home

0

Susan TesterP

LOGOUT

OP2B - IAR Organizations

Organization  LHIN  North Simcoe Muskoka

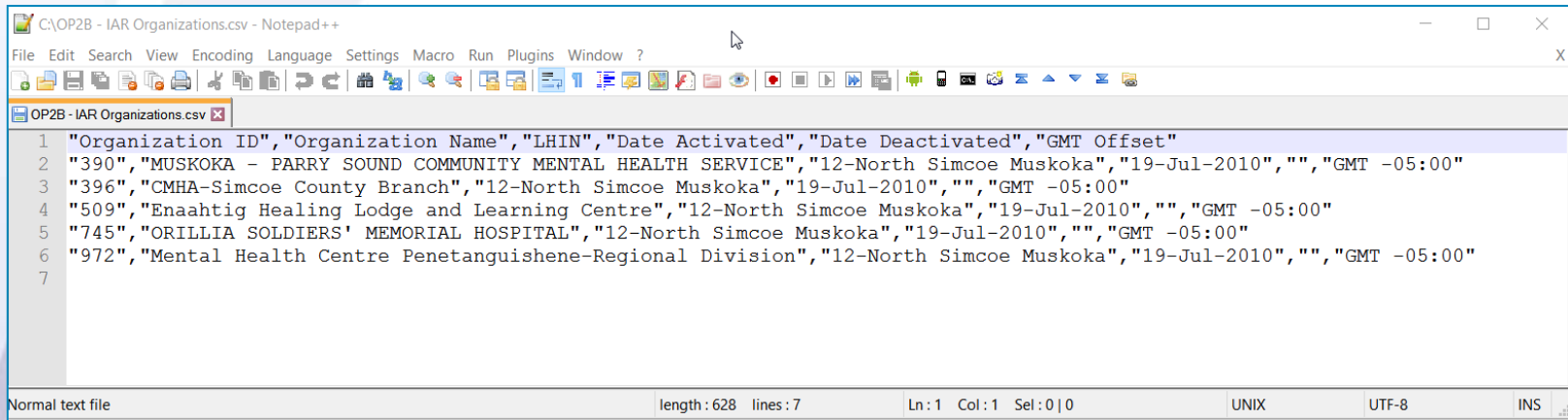
Search Reset

Organization ID	Organization Name	LHIN	Date Activated	Date Deactivated	GMT Offset
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
509	Enahtig Healing Lodge and Learning Centre	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00
745	ORILLIA SOLDIERS' MEMORIAL HOSPITAL	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00
972	Mental Health Centre Penetanguishene-Regional Division	12-North Simcoe Muskoka	19-Jul-2010		GMT -05:00

Results 1-5 [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

# Report in CSV Format



```
C:\OP2B - IAR Organizations.csv - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
OP2B - IAR Organizations.csv
1 "Organization ID","Organization Name","LHIN","Date Activated","Date Deactivated","GMT Offset"
2 "390","MUSKOKA - PARRY SOUND COMMUNITY MENTAL HEALTH SERVICE","12-North Simcoe Muskoka","19-Jul-2010","","GMT -05:00"
3 "396","CMHA-Simcoe County Branch","12-North Simcoe Muskoka","19-Jul-2010","","GMT -05:00"
4 "509","Enaahutig Healing Lodge and Learning Centre","12-North Simcoe Muskoka","19-Jul-2010","","GMT -05:00"
5 "745","ORILLIA SOLDIERS' MEMORIAL HOSPITAL","12-North Simcoe Muskoka","19-Jul-2010","","GMT -05:00"
6 "972","Mental Health Centre Penetanguishene-Regional Division","12-North Simcoe Muskoka","19-Jul-2010","","GMT -05:00"
7
Normal text file length: 628 lines: 7 Ln: 1 Col: 1 Sel: 0|0 UNIX UTF-8 INS
```

*CSV formatted files can be imported into Excel for further analysis and formatting*



# Monitoring Logs



- **Clinical Log**
- **Current Activity Log** – logs all the activities relevant to current session
- **Privacy Log** – logs all privacy related activities
- **System Log** – logs all system activities

# Clinical Log

- Fields available to refine search

## Date Range

- Defaults to last 30 days
- Allows maximum 180 days in each query

The screenshot shows the 'Clinical Log' interface within the IAR (Intelligent Alerting and Reporting) system. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with categories: COMMON, MONITORING (selected), MESSAGING, WORKLISTS, PERSON SEARCH, OPERATIONAL REPORTS, PRIVACY REPORTS, and ABOUT IAR. Under the MONITORING category, 'Clinical Log' is selected, with other options being 'Current Activity Log', 'Privacy Log', and 'System Log'. The main content area is titled 'Clinical Log' and contains various search filters. On the left side of the main area, there are input fields for 'User ID', 'Patient ID Type', and 'Application' (with a dropdown arrow and an 'Update list' link). Below these are 'Concerto Events' (a list box with 'Open Application', 'Open Document', and 'Context Change'), 'Date' (with 'From' and 'To' date pickers showing '2016-09-07' and '2016-10-07' respectively, each with a green checkmark and a calendar icon), 'Result' (radio buttons for 'All' (selected), 'Success', and 'Fail'), and 'Organization' (with a search icon). On the right side of the main area, there are input fields for 'Patient ID', 'Patient Name', 'User Events' (a list box with 'User Authentication', 'Login', 'Logout', and 'Account Status Change'), 'Other Events' (a list box with 'Account Validation', 'Add Group Membership', 'Add Role Group Membership', and 'Add Role Membership'), 'Session', and 'Machine IP/ID'. There are also 'Update list' links next to the 'Application' and 'Other Events' list boxes. At the bottom of the main area, there is a 'Search' button and a 'Reset' link. Below the search controls, a message reads: 'Enter search criteria above and hit \'Search\''. The top of the interface features a header bar with the IAR logo, a home icon, a notification bell with '0', the user name 'Susan TesterP', and a 'LOGOUT' button. The bottom left corner of the interface shows the 'ORION HEALTH' logo. The bottom right corner of the slide features the 'CCIM' logo and the text 'Community Care Information Management' and 'ACCESS TO INFORMATION'.

Common

MONITORING

Clinical Log

Current Activity Log

Privacy Log

System Log

MESSAGING

WORKLISTS

PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

ABOUT IAR

Clinical Log

User ID

Patient ID Type

Application

Update list

Concerto Events

Open Application

Open Document

Context Change

Date \*

From: 2016-09-07

To: 2016-10-07

Result

All

Success

Fail

Organization

Search

Reset

Patient ID

Patient Name

User Events

User Authentication

Login

Logout

Account Status Change

Other Events

Account Validation

Add Group Membership

Add Role Group Membership

Add Role Membership

Update list

Session

Machine IP/ID

Enter search criteria above and hit 'Search'

ORION HEALTH

CCIM

Community Care Information Management

ACCESS TO INFORMATION

# Clinical Log

- Fields available to refine search

## User Events

- User Authentication
- Login
- Logout
- Account Status Change
- Password Change
- Security Change


## Date Range

- Defaults to last 30 days
- Allows maximum 180 days in each query

## Other Events

- Account Validation
- Add Group Membership
- Add Role Group Membership
- Add Role Membership
- Add mapping agent
- Assign Privacy Policy
- Authenticated Login
- Background Task
- Configuration
- Configure CCOW context manager
- Copy Entry Point to Application
- Create Custom Privacy Policy
- Create Entry Point
- Create External Identifier Type
- Create Information Type
- Create Login Disclaimer
- Create Role
- Create User
- Database Export
- Database Merge
- Destroy Entry Point
- Destroy Information Type
- Download CSV File
- Edit Custom Privacy Policy
- Edit Login Disclaimer
- Edit Privacy Policy
- Get User
- Join Common Context
- Leave Common Context
- Password Reset Request
- Print Request
- Privacy Override
- Privacy prevented user message from being sent
- Purged expired Tokens
- Remove External Identifier Type
- Remove Group Membership
- Remove Role
- Remove Role Membership
- Remove User
- Remove mapping Agent
- Rename Entry Point
- Rename User
- Reset Custom Privacy policy
- Resolve User ID
- Search Performed
- Shut Down
- Start Up
- Submission Upload Submission
- Undo Recent Changes
- User Accepted Login Disclaimer
- User Cancelled Login Disclaimer
- User Custom Authentication
- View Submission Upload Page


# Clinical Log – Search Results


Susan TesterP
LOGOUT

<<

- COMMON
- MONITORING**
  - Clinical Log
  - Current Activity Log
  - Privacy Log
  - System Log
- MESSAGING
- WORKLISTS
- PERSON SEARCH
- OPERATIONAL REPORTS
- PRIVACY REPORTS
- ABOUT IAR

<<



## Clinical Log

User ID

Patient ID Type

Application  [Update list](#)

Patient ID

Patient Name

User Events 

User Authentication  
Login  
Logout  
Account Status Change

Concerto Events 

Open Application  
Open Document  
Context Change

Date \* From:  To:

Result ☒ All  
☐ Success  
☐ Fail

Organization

Other Events 

Account Validation  
Add Group Membership  
Add Role Group Membership  
Add Role Membership

[Update list](#)

Session

Machine IP/ID

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

Time	User ID	Event Type	Message	Patient ID	Patient Name	Machine IP/ID	Organization	ID Type
07 Oct 2016 10:45:51	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
06 Oct 2016 16:55:38	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
06 Oct 2016 16:50:20	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
06 Oct 2016 13:32:38	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
06 Oct 2016 09:42:59	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
05 Oct 2016 15:15:19	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
05 Oct 2016 13:14:05	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
05 Oct 2016 13:06:49	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
04 Oct 2016 11:27:52	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
04 Oct 2016 11:15:27	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
03 Oct 2016 11:47:28	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI
29 Sep 2016 14:10:27	susan.testerviewer	Resolve User ID	Susan.TesterViewer			10.41.0.98	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION	Patient.Id.MPI

# Clinical Log – Log Entry Details

Audit Event Details - Windows Internet Explorer provided by CCIM






https://10.21.202.119/concerto/audit/AuditEventDetails.htm?encryptedRequest=1D01091129E529C91AD7FF31EB9A87 ✖ Certificate error

Parameter List			
ID	584742	Start Time	07-Oct-2016 16:28
Type	Open Application	Source	Concerto
Message	Integrated Assessment Repository, Role Based Clinical Log		
Result	Success		
Session ID	35442E00-8927-4B1D-B725-6CCA4AF967D3	Terminal ID	10.41.0.98
User ID	Susan.TesterPrivacyOfficer	Patient ID Type	Patient.Id.MPI

Audit Event Parameters	
Name	Value
ConcertoAccount	32D844E9-90E9-44D5-B5B7-9C61C0689C56
applicationName	Integrated Assessment Repository
entryPointName	Role Based Clinical Log
userOrgs	345;396
userOrgsDesc	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION;396 CMHA-Simcoe County Branch
userRoles	Privacy Officer;

Close

# Current Activity Log – Search Results

0Susan TesterPLOGOUT

COMMON

MONITORING

Current Activity Log

Privacy Log

System Log

MESSAGING

WORKLISTS


PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

ABOUT IAR

## 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
07 Oct 16:56:13	Susan.TesterPri...	Search Performed	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:56:09	Susan.TesterPri...	Search Performed	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:55:47	Susan.TesterPri...	Search Performed	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:55:45	Susan.TesterPri...	Search Performed	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:55:34	Susan.TesterPri...	Search Performed	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:55:33	Susan.TesterPri...	Search Performed	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:55:32	Susan.TesterPri...	Open Application	Integrated Assessment Repository, Current Activity Log		Patient.Id.MPI	
07 Oct 16:55:32	Susan.TesterPri...	Open Application	Integrated Assessment Repository, Role Based Current Activity Log		Patient.Id.MPI	

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



# Current Activity Log – Log Entry Details

Audit Event Details - Windows Internet Explorer provided by CCIM


https://10.21.202.119/concerto/audit/AuditEventDetails.htm?encryptedRequest=4BA58F3E87B559303A0E4CDDCCD5F692FAA16EDF Certificate error





Parameter List			
ID	584758	Start Time	07-Oct-2016 16:56
Type	Search Performed	Source	Concerto
Message	Integrated Assessment Repository, Current Activity Log		
Result	Success		
Session ID	35442E00-8927-4B1D-B725-6CCA4AF967D3	Terminal ID	10.41.0.98
User ID	Susan.TesterPrivacyOfficer	Patient ID Type	Patient.Id.MPI

Audit Event Parameters	
Name	Value
Application name	Integrated Assessment Repository
ConcertoAccount	32D844E9-90E9-44D5-B5B7-9C61C0689C56
Search name	Current Activity Log
Search parameter Application	
Search parameter Result	
Search parameter User ID	susan.testerviewer
userOrgs	345;396
userOrgsDesc	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION;396 CMHA-Simcoe County Branch
userRoles	Privacy Officer;

Close

# Privacy Log – Search Results



 0  Susan TesterP  LOGOUT

COMMON

MONITORING

Clinical Log

Current Activity Log

Privacy Log

System Log

MESSAGING

WORKLISTS

PERSON SEARCH

OPERATIONAL REPORTS

PRIVACY REPORTS

ABOUT IAR

## Privacy Log

User ID

Patient ID

Patient ID Type

Session

Result ☐ All ☐ Success ☐ Fail

Date From:  To:


Policy Name

Search

Reset

Time	User ID	Overridden Policy	Patient ID	Patient ID Type	Patient Name	Session ID
24 Jan 15:17:40	cuv	Custom Policy	2740	Patient.Id.MPI	Akari Alane	AD0DEE8C-75D6-4BED-97FB-FFBA80D43AF0
24 Jan 15:17:29	cuv	Custom Policy	2740	Patient.Id.MPI	Akari Alane	AD0DEE8C-75D6-4BED-97FB-FFBA80D43AF0
19 May 09:25:45	cuv	Custom Policy	1321	Patient.Id.MPI	Blossom David	DED9228A-27CC-45DC-9D5D-967C4A4F8C2A
14 Apr 13:47:21	cuv	Custom Policy	1321	Patient.Id.MPI	Blossom David	3E96A915-EAB7-40D0-92C8-8BFB3B733A75
02 Mar 07:34:44	viewer2	Custom Policy	1244	Patient.Id.MPI	Rodas James	9D59E296-45B8-4281-B2CC-9E7E9A893379
28 Feb 15:11:30	viewer2	Custom Policy	1244	Patient.Id.MPI	Rodas James	83C91DAA-4C77-4D4E-B0E9-C1CF5E19A381

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





# Privacy Log

- The privacy log captures the consent override events
- Since the consent override is not supported in IAR, therefore the privacy log contains no records at this time

# Privacy Log – Log Entry Details

Audit Event Details - Windows Internet Explorer provided by CCIM

https://10.21.202.119/concerto/audit/AuditEventDetails.htm?encryptedRequest=F956F3720F55769F92D1C5A4D66A9813859D835412 ✖ Certificate error

Parameter List			
ID	259411	Start Time	24-Jan-2012 15:35
Type	Open Application	Source	Concerto
Message	IAR - Assessments, Assessment-List		
Result	Success		
Patient ID	2740	Patient Name	Akari Alane
Session ID	AD0DEE8C-75D6-4BED-97FB-FFBA80D43AF0	Terminal ID	10.21.202.61
User ID	cuv	Patient ID Type	Patient.Id.MPI

Audit Event Parameters	
Name	Value
Patient.Co.DateTimeOfBirth	19320404000000-0500
Patient.Co.PatientName	Akari^Alane^A^A^A^A^A
Patient.Co.Sex	M
Patient.Id.MPI	2740
Patient.Id.MRN	CID2042820666RAI-HC^763
applicationName	IAR - Assessments
entryPointName	Assessment-List
userOrgs	345;463;763;360;396;745;651;965;55102;777;Abc1234567890Xyz;A12;444;390
userOrgsDesc	345 ALPHA COURT NON-PROFIT HOUSING CORPORATION;463 CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY;763 PEMBROKE REGIONAL HOSPITAL;360 CANADIAN MENTAL HEALTH ASSOCIATION - SAULT STE MARIE BRANCH;396 CMHA-Simcoe County Branch;745 ORILLIA SOLDIERS' MEMORIAL HOSPITAL;651 ROYAL OTTAWA HEALTH CARE GROUP;965 SAULT AREA HOSPITAL;55102 RAI-MH 55102;777 Dummy Org 777 for testing IAR-24;Abc1234567890Xyz Test Alphanumeric OrgID;A12 Test Alphanumeric Short;444 CMHA-CHAMPLAIN EAST;390 MUSKOKA - PARRY SOUND COMMUNITY MENTAL HEALTH SERVICE
userRoles	Viewer;Uploader;

Close

# System Log – Search Results

## Date Range

- Defaults to last 30 days
- Allows maximum 180 days in each query

The screenshot shows the IAR System Log search results page. The interface includes a sidebar with navigation links: COMMON, MONITORING (Clinical Log, Current Activity Log, Privacy Log, System Log), MESSAGING, WORKLISTS, PERSON SEARCH, OPERATIONAL REPORTS, PRIVACY REPORTS, and ABOUT IAR. The main content area is titled 'System Log' and features search filters for User ID, Date (From: 2013-12-24, To: 2013-12-24), Result (All, Success, Fail), and Event Type (Server Events: Start Up, Shut Down; Database Events: Database Import, Database Export, Database Merge). A 'Search' button and a 'Reset' link are present. Below the filters is a table with 6 columns: Time, User ID, Event Type, Message, Session ID, and IP Address. The table contains 3 rows of data for Database Export events. At the bottom, there are links for 'Printer Friendly Version' and 'Download CSV results'. The ORION HEALTH logo is in the bottom left corner.

**System Log**

User ID:

Date: From: 2013-12-24 To: 2013-12-24

Result: ☒ All ☐ Success ☐ Fail

Server Events:

Database Events:

[Reset](#)

Time	User ID	Event Type	Message	Session ID	IP Address
24 Dec 10:38:37	mihai	Database Export	/opt/orionhealth/Concerto/exports/2013_12_24.c6x.xml	015A5BAD-73F2-4881-8F6B-0894E29D3FA0	10.56.0.75
24 Dec 10:38:30	mihai	Database Export	/opt/orionhealth/Concerto/exports/2013_12_24.c6x.xml	015A5BAD-73F2-4881-8F6B-0894E29D3FA0	10.56.0.75
24 Dec 10:13:04	mihai	Database Export		5CE28743-F205-4C93-AC00-A30BAAD5C38A	10.56.0.75

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

ORION HEALTH

# System Log – Log Entry Details

Audit Event Details - Windows Internet Explorer provided by CCIM

https://10.21.202.119/concerto/audit/AuditEventDetails.htm?encryptedRequest=1A0428652F678391644D43B849FB07E Certificate error

Parameter List			
ID	387842	Start Time	24-Dec-2013 10:13
Type	Database Export	Source	Concerto
Message			
Result	Success		
Session ID	5CE28743-F205-4C93-AC00-A30BAAD5C38A	Terminal ID	10.56.0.75
User ID	mihai	Patient ID Type	Patient.Id.MPI

Audit Event Parameters	
Name	Value
ConcertoAccount	8D7D51B2-B444-4C7C-9B66-61780D33D7A5
exportApplication	IAR - Reports
filename	/opt/orionhealth/Concerto/exports/IAR - Reports-2013_12_24.c6x.xml
userOrgs	;444;763;651;463;345
userOrgsDesc	;444 CMHA-CHAMPLAIN EAST;763 PEMBROKE REGIONAL HOSPITAL;651 ROYAL OTTAWA HEALTH CARE GROUP;463 CANADIAN MENTAL HEALTH ASSOCIATION, THUNDER BAY;345 ALPHA COURT NON-PROFIT HOUSING CORPORATION
userRoles	Uploader;Central Admin;Central Privacy Officer;Privacy Officer;User Manager;Viewer;

Close

**Privacy  
Review**

# Privacy Review

# Privacy Operations Review

- Privacy review is defined in the Data Sharing Agreement
- All HSPs should conduct privacy and security self-assessment on a regular basis, which will assess the effectiveness and efficiency of the privacy operations to ensure continued compliance with the DSA
- The self-assessment should be conducted based on a checklist agreed by all HSPs, to ensure consistency and comparability of the result
- The results of the self-assessment shall be signed off by the HSP's senior management and submitted to the Privacy and Security Committee for review
- Privacy and Security Sub-Committee reviews gaps and mitigation plans from HSPs
- HINP follows up on progress of mitigation plans from HSPs

# Self-Assessment Checklists

## Sections

1. General Questions
2. Consent Management
3. Audit Log Review
4. Client Privacy Right Support
5. Integrated Incident Management
6. User Account Management

## 4 Client Privacy Right Supporting Process

No.	Category	Question	Yes or No	Comments
CP1	<b>Clients Requesting Access to Their Assessment Data</b>	Does a process exist to handle a client requesting a copy of their assessments?		
CP2		Does this process include steps to handle a request involving assessment data under the custody of other HSPs?		
CP3	<b>Clients Requesting Change to Their Assessment Data</b>	Does a process exist to handle a client requesting a change to his/her assessments?		
CP4		Does this process include steps to handle requests involving assessment data under the custody of other HSPs? (e.g. a process for the clients to contact the other HSPs)		
CP5	<b>Client Complaint About HSP Privacy Practices</b>	Does a process exist to handle a client complaint about the privacy practices of your HSP?		
CP6		Does this process include steps to handle a client privacy complaint that involves other HSPs?		



# Integration Points

- Identify who is accountable for acknowledging on the self-assessment report
- Identify who is responsible for performing the self-assessment and conducting the review
- Identify if there is a need to involve different individuals when conducting the different area or section of the review

**Enterprise  
Master  
Patient  
Index**

# **Enterprise Master Patient Index (EMPI)**

# EMPI Overview

- EMPI is an Enterprise Master Person Index that uniquely identifies a person across multiple sources (HSPs)
- EMPI creates a unique enterprise identifier (EID) for any single client
  - EMPI establishes and maintains a mapping between the EID and the client's identifier used inside each of the participating HSPs
- EMPI operations ensure the accuracy, completeness and “up-to-date-ness” of a client's demographics to uniquely identify a person across multiple sources (HSPs)
- Define the processes to identify, escalate, resolve issues related to client's demographic information

# How Matching Is Done

- The EMPI compares demographic data from each assessment and creates matches based on an algorithm and established thresholds
- Demographic information used includes:
  - First Name
  - Last Name
  - Date of Birth
  - Gender
  - Telephone Number
  - Address
  - Health Card Number
- Better matches are reached when using a Health Card Number

# Health Records Lead Role

- Designated by the Executive Lead
- Helps resolve EMPI data element issues:
  - Potential duplicate
  - Potential overlay
- Interacts with the EMPI Data Steward (EDS) at Transformed Shared Services Organization (TSSO) – the EMPI HINP
- Liaises with clinicians, health record personnel, and/or Privacy Officer and facilitates resolution to data element issues

# Typical EMPI Questions

- **Potential Duplicate** – duplicate record for same person in same source
- **Potential Overlay** – same record with different person

*(NOTE: no records can be viewed from IAR until an overlay issue is resolved)*

# EMPI Process Summary

- EMPI Data Steward notifies HSP of data quality issues or errors identified from EMPI regarding client demographic information
- HSPs evaluate, investigate and resolve the identified data quality issues or data errors
- HSPs resubmit assessments if issues are identified and corrected
- EMPI Data Steward and CCIM Support to work with HSPs to resolve major demographic data quality issues or data errors

# **Communication Awareness and Training Next Steps**



# Communication

- HSPs need to raise key stakeholders' awareness and support of the privacy and security of IAR
- HSPs need to obtain the support for the privacy and security implementation
- HSPs need to ensure timely, consistent, clear and coordinated messages
- CCIM will support the HSPs in their communication activities through the development of tools and materials

# Awareness and Training

- HSPs need to raise the staff's awareness of the privacy and security of IAR
- HSPs need to provide training on the privacy processes to the staff who participate in the privacy management activities, such as consent management, breach management, etc.
- CCIM will support HSPs in their awareness and training activities through the development of training tools and materials
  - [https://www.ccim.on.ca/Pages/sp\\_elearning.aspx](https://www.ccim.on.ca/Pages/sp_elearning.aspx)

# Next Steps

- Review and implement privacy and security processes to support IAR
- Complete the required forms and send to CCIM
- Check out the Common Privacy Framework

[https://www.ccim.on.ca/IAR/Private/Document/IAR%20Privacy%20and%20Security/Common%20Privacy%20Framework/Consent Management Implementation guide v1.1 20110602 CPF.pdf](https://www.ccim.on.ca/IAR/Private/Document/IAR%20Privacy%20and%20Security/Common%20Privacy%20Framework/Consent%20Management%20Implementation%20guide%20v1.1%2020110602%20CPF.pdf)

# Thank You!

## Integrated Assessment Record **SUPPORT CENTRE**



Monday to  
Friday

8:30 am — 5.00 pm

1.866.909.5600 option 8

Email

[iar@ccim.on.ca](mailto:iar@ccim.on.ca)