Integrated Assessment Record (IAR)

Privacy, Security and Consent Management Training

Version 4.0

CCIM Community Care Information Management

ACCESS TO INFORMATION

Privacy, Security and Consent Management Training Table of Contents

CCIM Community Care Information Management
ACCESS TO INFORMATION

Community Care Information Management

Privacy, Security and Consent Management Training

Agenda

	Item
1.	Introduction
2.	Data Sharing Agreement
3.	Privacy and Security Processes: Incident Management
4.	Privacy and Security Processes: Consent Management
5.	Privacy and Security Processes: Client Privacy Rights Support
6.	Privacy and Security Processes: User Account Management
7.	Privacy and Security Processes: Audit Log Review
8.	Privacy and Security Processes: Privacy Review
9.	Privacy and Security Processes: Enterprise Management Patient Index (EMPI)
10.	Communications
11.	Awareness and Training (including IAR Privacy and Security Training for Users)
12.	Q & A / Next Steps / Reminders / Wrap-up

CCIM Community Care Information Management

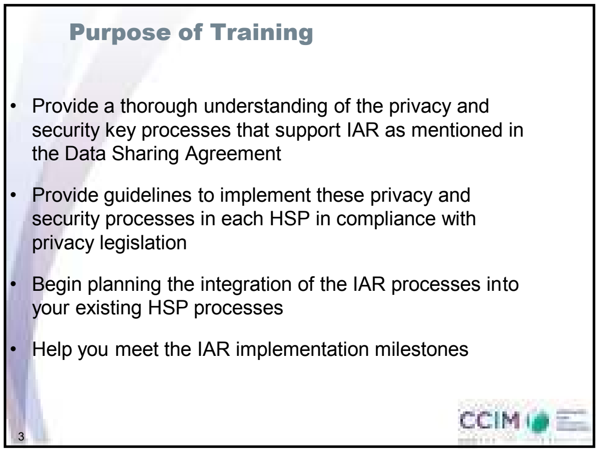
ACCESS TO INFORMATION

Integrated Assessment Record

Consolidated DSA, Privacy, Security and Consent Management Training

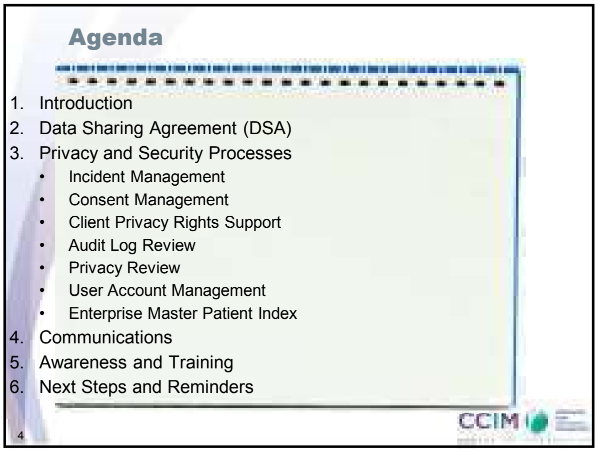
November 2016

Introduction



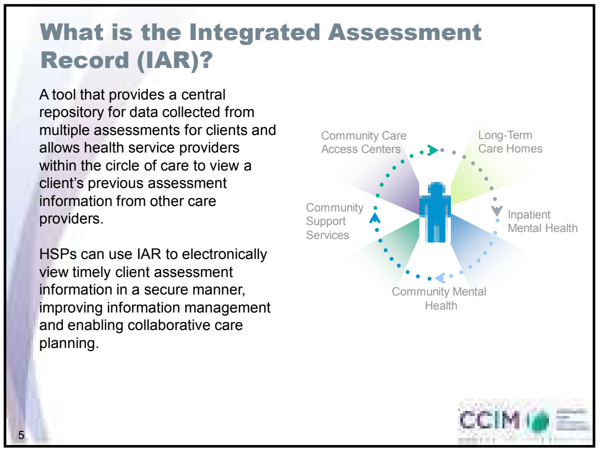
Purpose of Training

- 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

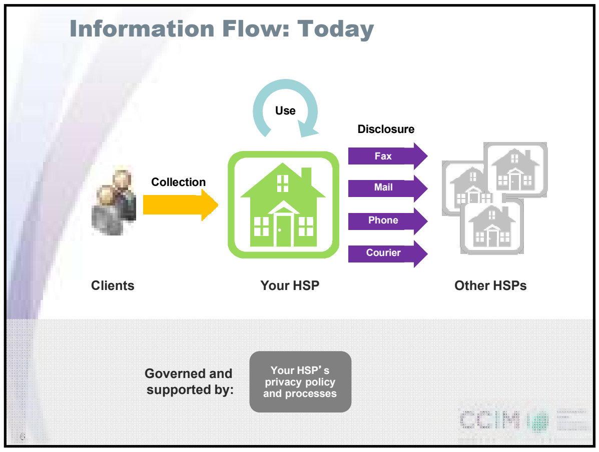
1. Introduction
2. Data Sharing Agreement (DSA)
3. Privacy and Security Processes
   - Incident Management
   - Consent Management
   - Client Privacy Rights Support
   - Audit Log Review
   - Privacy Review
   - User Account Management
   - Enterprise Master Patient Index
4. Communications
5. Awareness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



What is the Integrated Assessment Record (IAR)?

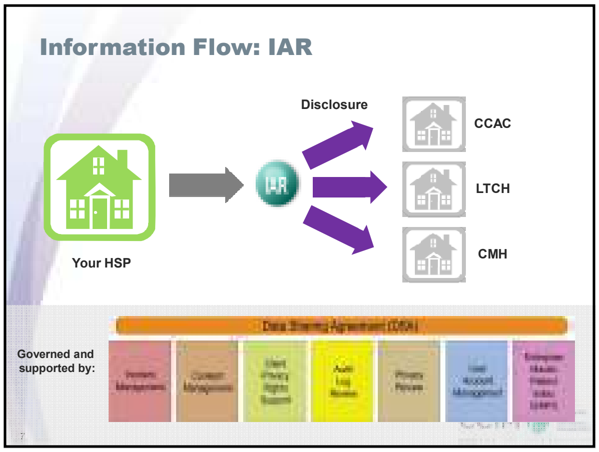
A tool that provides a central repository for data collected from multiple assessments for clients and allows health service providers within the circle of care to view a client's previous assessment information from other care providers.

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

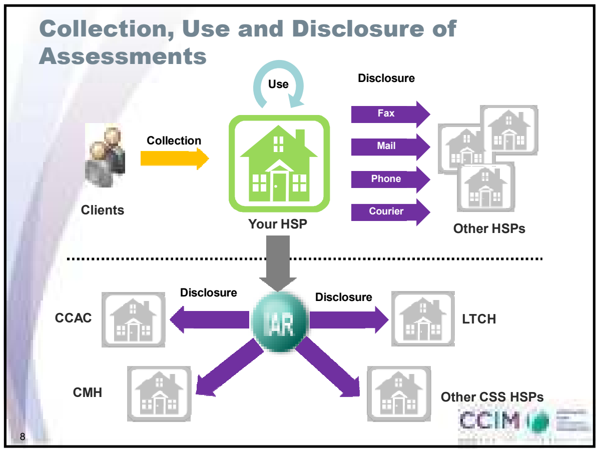


Information Flow: Today

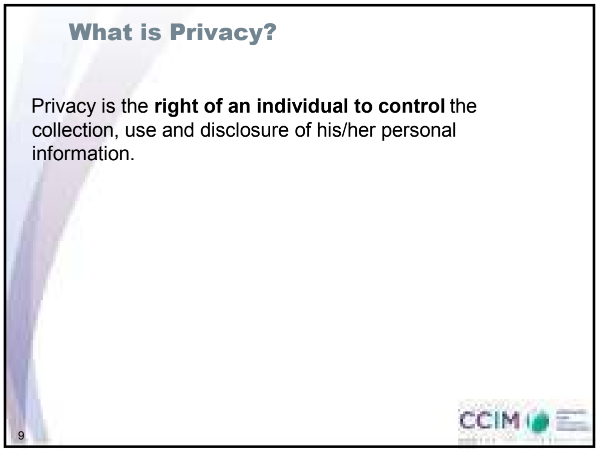
Governed and supported by: Your HSP's privacy policy and processes



Information Flow: IAR



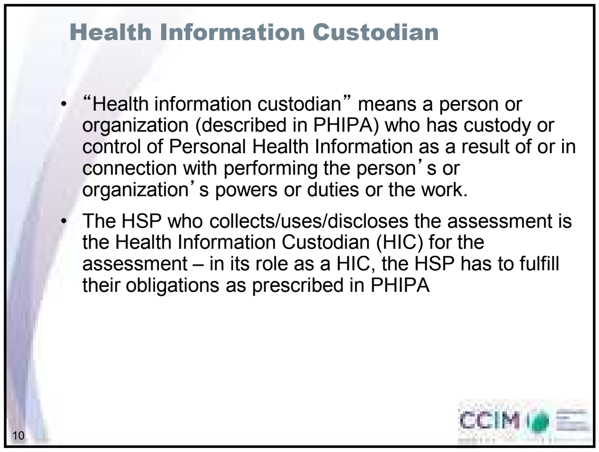
Collection, Use and Disclosure of Assessments



What is Privacy?

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

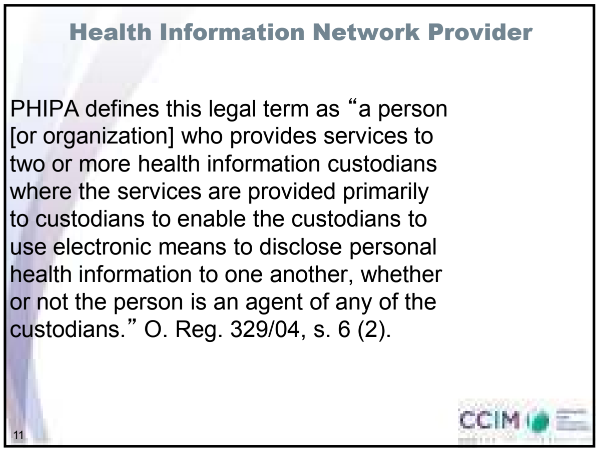
9



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

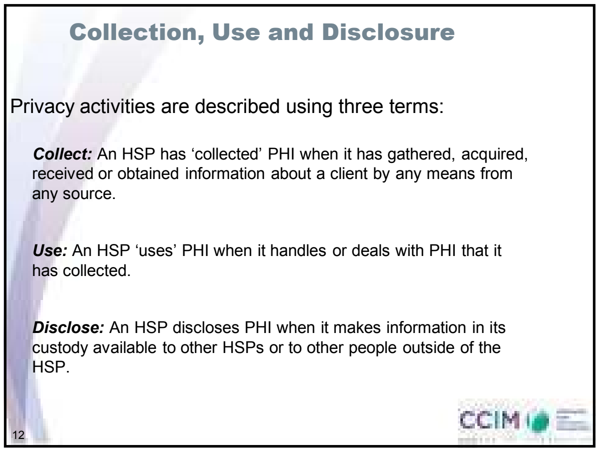
10



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).

11



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.

12

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).

13

IAR
HINP and HIC
Privacy Obligations

14

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

15

HIC/HSP Privacy and Security Obligations

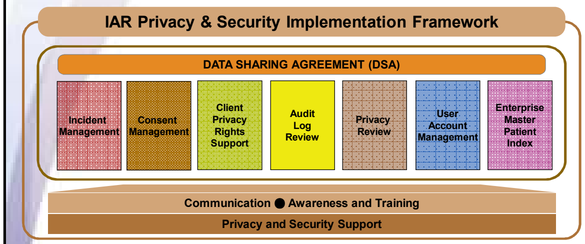
- Designate a privacy contact person (HSP Privacy Officer)
- Sign the Data Sharing Agreement (DSA)
- Manage client's consent and consent directive
- Manage privacy incidents
- Support client's privacy rights
- Manage user accounts
- Review logs
- Manage client's demographics in Enterprise Master Patient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

16

IAR Privacy and Security Implementation Framework

17

Privacy and Security Key Processes



IAR Privacy & Security Implementation Framework

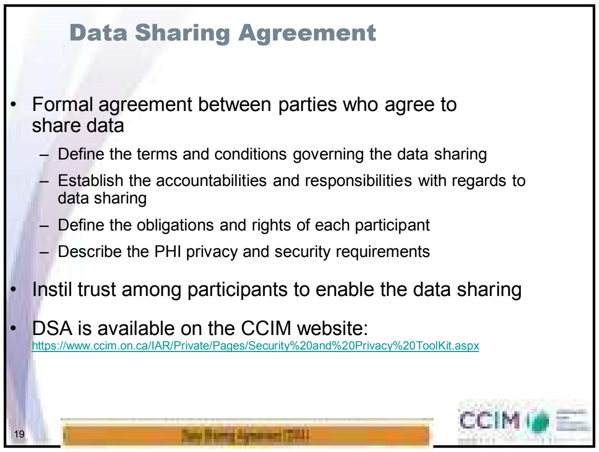
DATA SHARING AGREEMENT (DSA)

Incident Management | Consent Management | Client Privacy Rights Support | Audit Log Review | Privacy Review | User Account Management | Enterprise Master Patient Index

Communication ● Awareness and Training

Privacy and Security Support

18

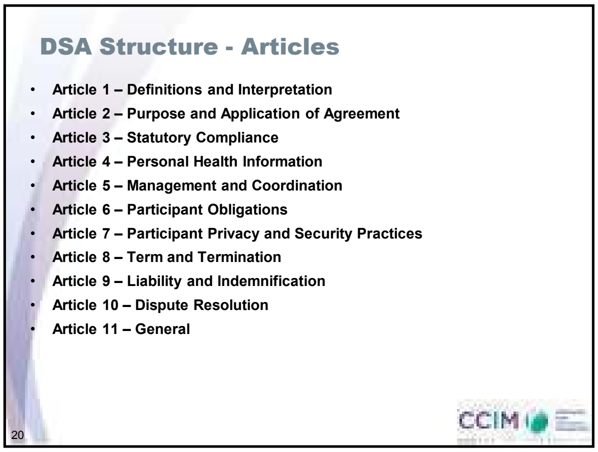


Data Sharing Agreement

- 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

Data Sharing Agreement (DSA)

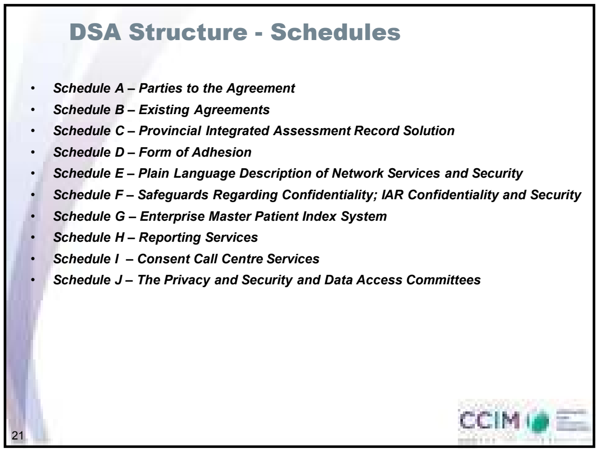
19



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**

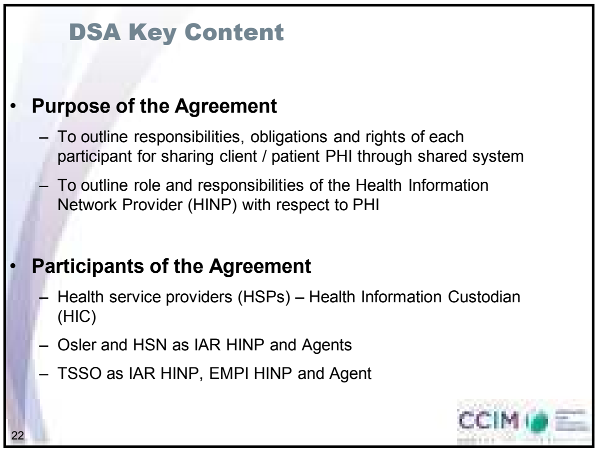
20



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***

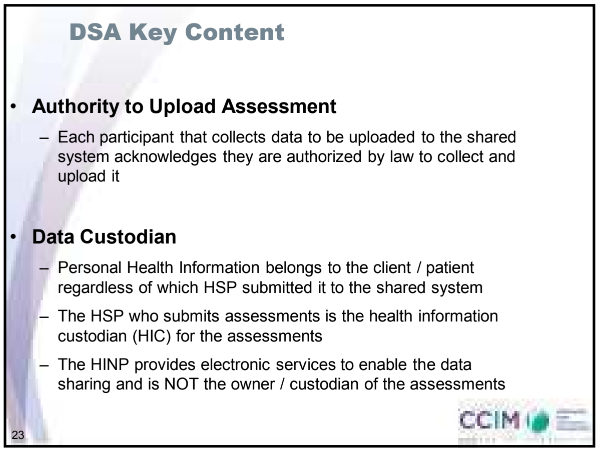
21



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

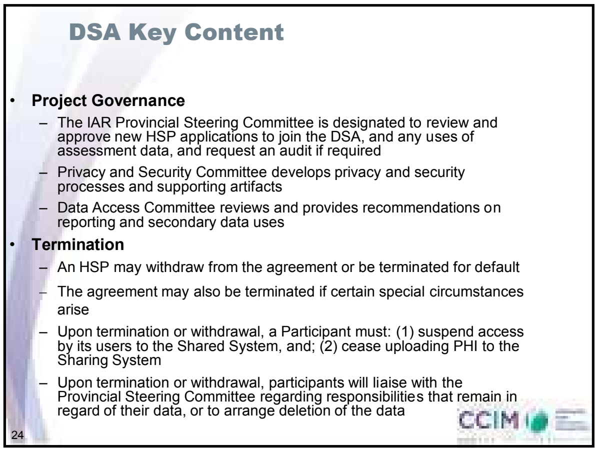
22



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

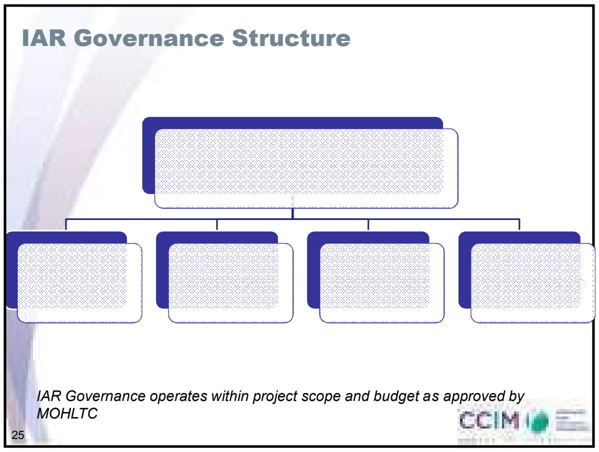
23



DSA Key Content

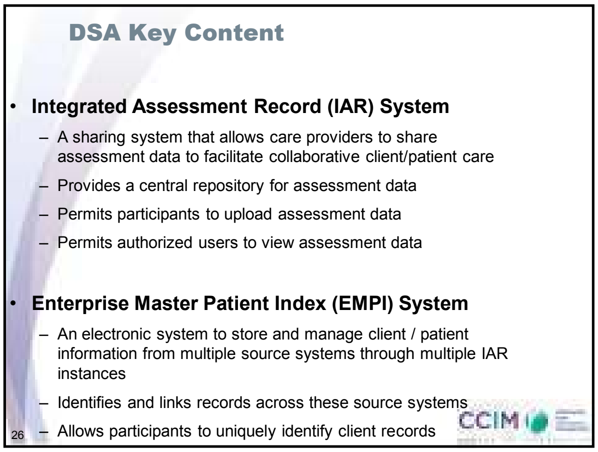
- **Project Governance**
  - The IAR Provincial Steering Committee is designated to review and approve new HSP applications to join the DSA, and any uses of assessment data, and request an audit if required
  - Privacy and Security Committee develops privacy and security processes and supporting artifacts
  - 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

24



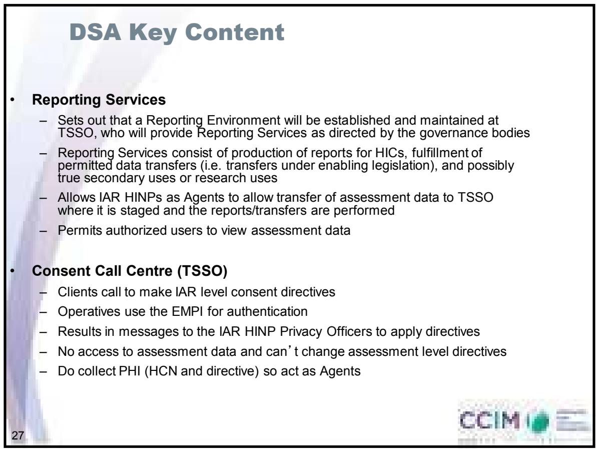
IAR Governance Structure

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



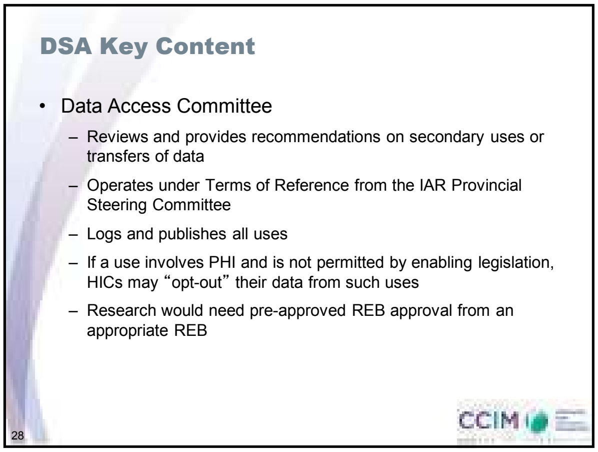
DSA Key Content

- **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



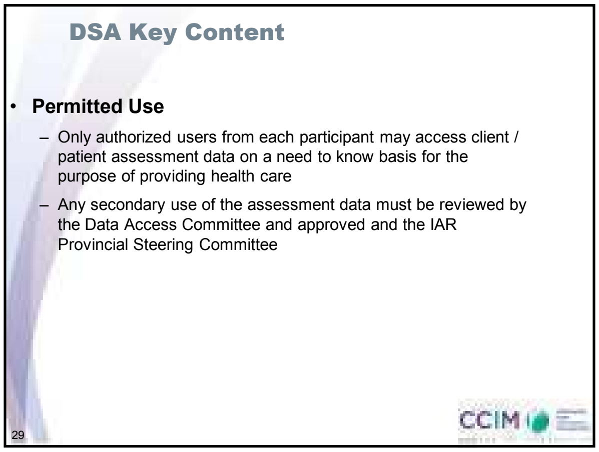
DSA Key Content

- **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



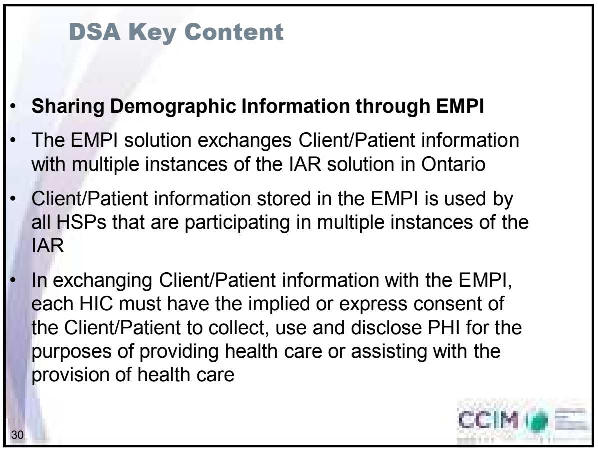
DSA Key Content

- 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



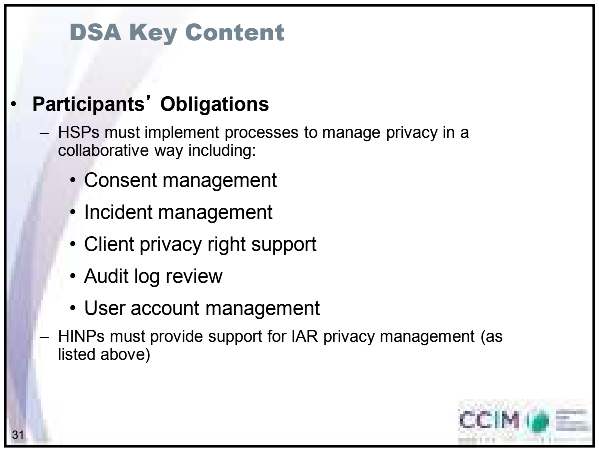
DSA Key Content

- **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



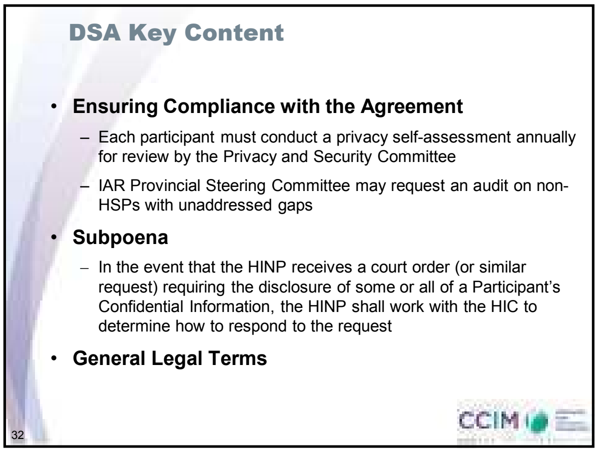
DSA Key Content

- **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



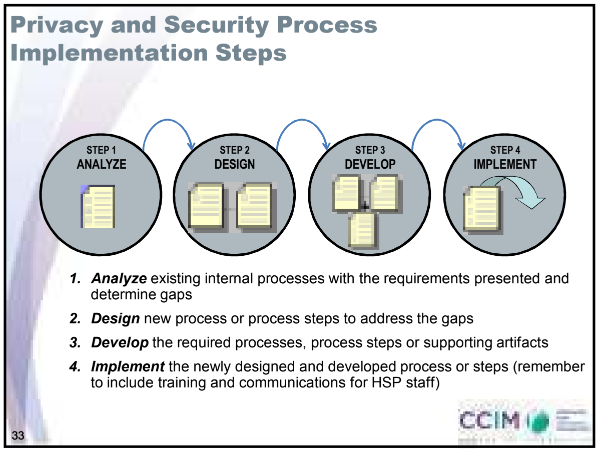
DSA Key Content

- **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**



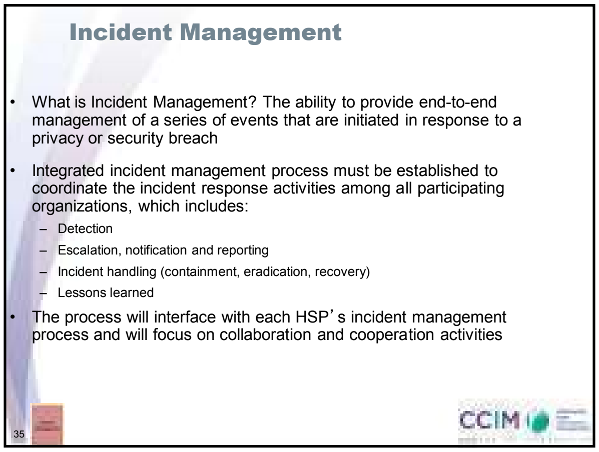
Privacy and Security Process Implementation Steps

STEP 1
ANALYZE
STEP 2
DESIGN
STEP 3
DEVELOP
STEP 4
IMPLEMENT

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)

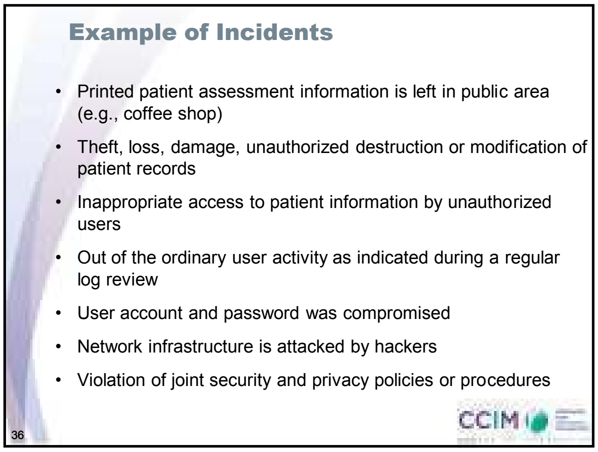
Incident Management

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

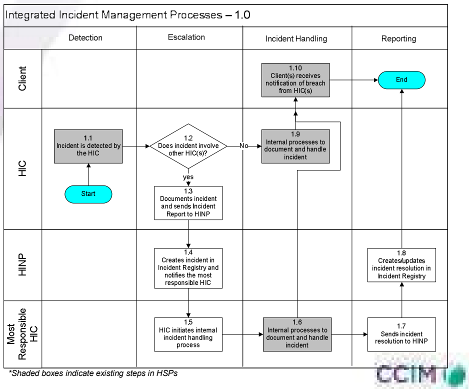
- Incidents can be detected or reported from the following parties:
  1. HIC
  2. Client or third party of the HIC
  3. HINP
  4. Third parties (e.g., agents or service providers) of HINP
- Processes are developed based on the four parties defined above

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



Integrated Incident Management Processes – 1.0

Detection

Escalation

Incident Handling

Reporting

Client

HIC

HINP

Most Responsible HIC

Start

1.1 Incident is detected by the HIC

1.2 Does incident involve other HIC(s)?

No

yes

1.3 Documents incident and sends Incident Report to HINP

1.4 Creates incident in Incident Registry and notifies the most responsible HIC

1.5 HIC initiates internal incident handling process

1.6 Internal processes to document and handle incident

1.7 Sends incident resolution to HINP

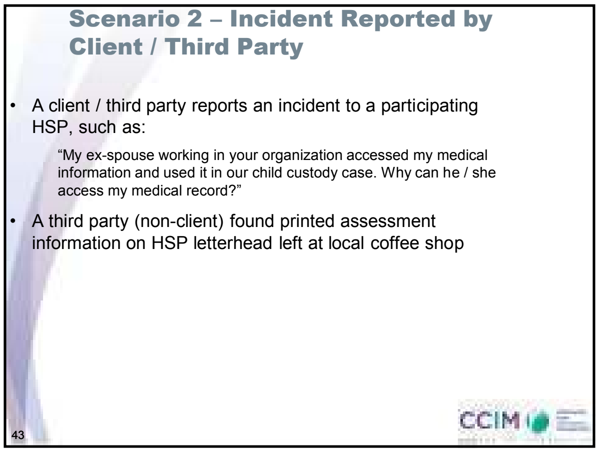
1.8 Creates/updates incident resolution in Incident Registry

1.9 Internal processes to document and handle incident

1.10 Client(s) receives notification of breach from HIC(s)

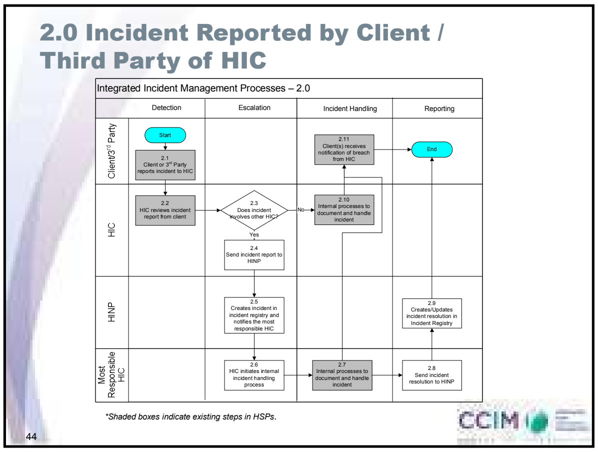
End

*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

Integrated Incident Management Processes – 2.0

Detection | Escalation | Incident Handling | Reporting

Client/3rd Party

Start

2.1 Client or 3rd Party reports incident to HIC

2.11 Client(s) receives notification of breach from HIC

End

HIC

2.2 HIC reviews incident report from client

2.3 Does incident involves other HIC?

No

2.10 Internal processes to document and handle incident

Yes

2.4 Send incident report to HINP

HINP

2.5 Creates incident in incident registry and notifies the most responsible HIC

2.9 Creates/Updates incident resolution in Incident Registry

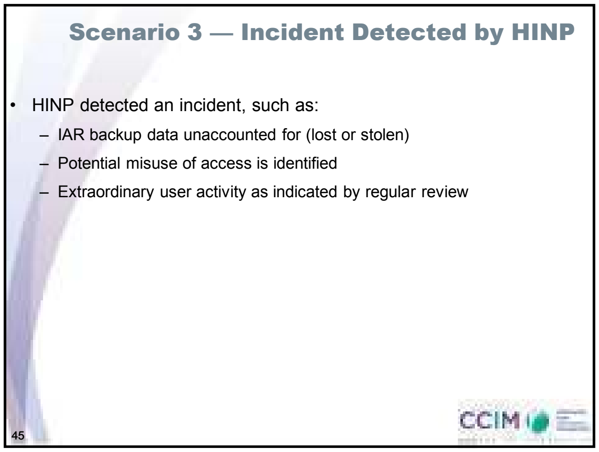
Most Responsible HIC

2.6 HIC initiates internal incident handling process

2.7 Internal processes to document and handle incident

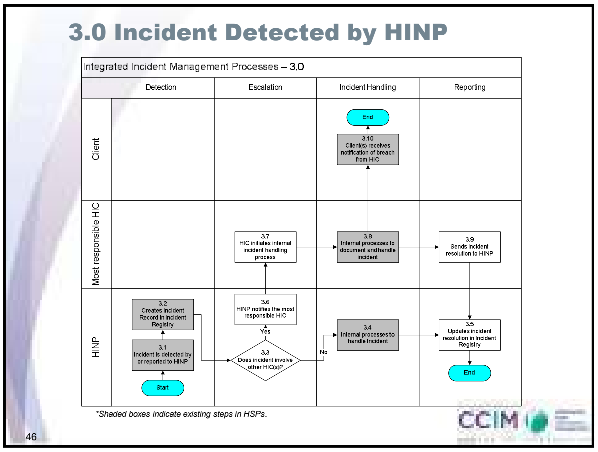
2.8 Send incident resolution to HINP

*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

Integrated Incident Management Processes – 3.0

Detection | Escalation | Incident Handling | Reporting

Client

End

3.10 Client(s) receives notification of breach from HIC

Most responsible HIC

3.7 HIC initiates internal incident handling process

3.8 Internal processes to document and handle incident

3.9 Sends incident resolution to HINP

HINP

3.2 Creates Incident Record in Incident Registry

3.1 Incident is detected by or reported to HINP

Start

3.6 HINP notifies the most responsible HIC

Yes

3.3 Does incident involve other HIC(s)?

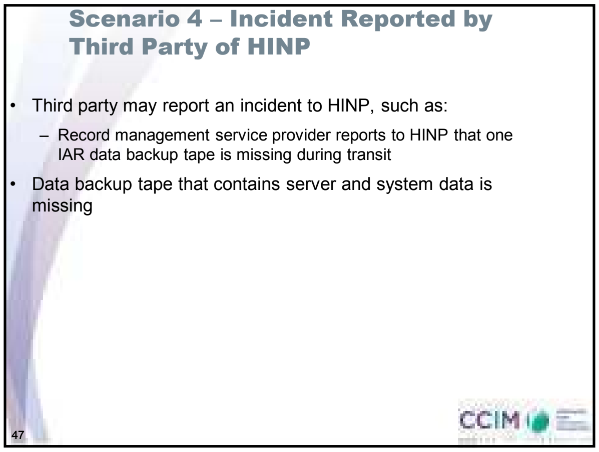
No

3.4 Internal processes to handle Incident

3.5 Updates incident resolution in Incident Registry

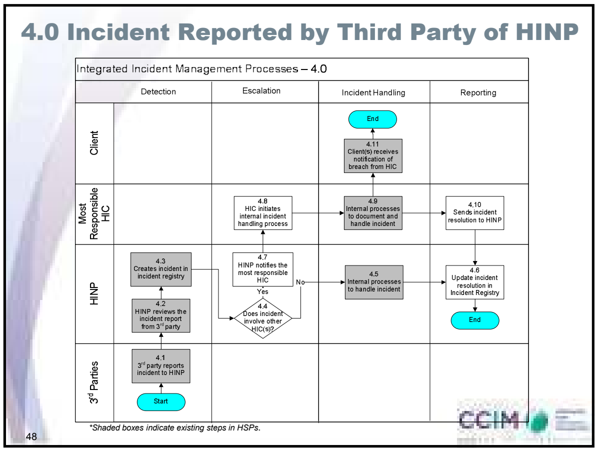
End

*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

Integrated Incident Management Processes – 4.0

Detection | Escalation | Incident Handling | Reporting

Client

End

4.11 Client(s) receives notification of breach from HIC

Most Responsible HIC

4.8 HIC initiates internal incident handling process

4.9 Internal processes to document and handle incident

4.10 Sends incident resolution to HINP

HINP

4.3 Creates incident in incident registry

4.2 HINP reviews the incident report from 3rd party

4.7 HINP notifies the most responsible HIC

Yes

4.4 Does incident involve other HIC(s)?

No

4.5 Internal processes to handle incident

4.6 Update incident resolution in Incident Registry

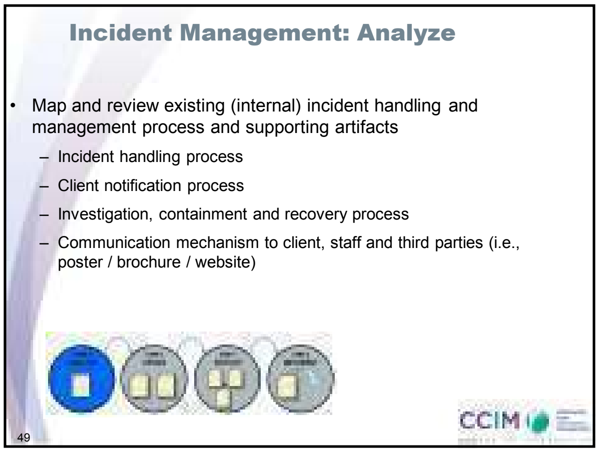
End

3rd Parties

4.1 3rd party reports incident to HINP

Start

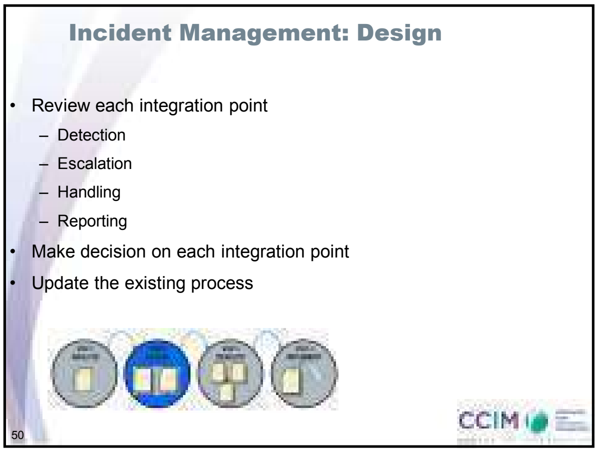
*Shaded boxes indicate existing steps in HSPs.



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)

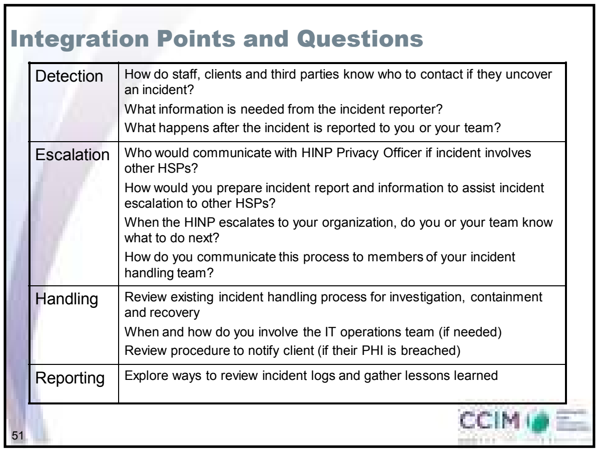
49



Incident Management: Design

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

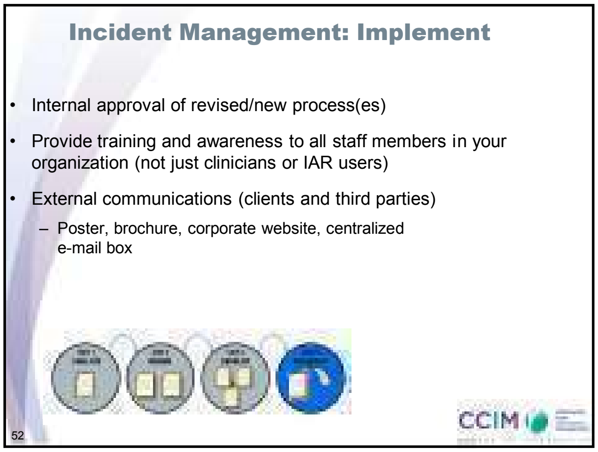
50



Integration Points and Questions

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

51



Incident Management: Implement

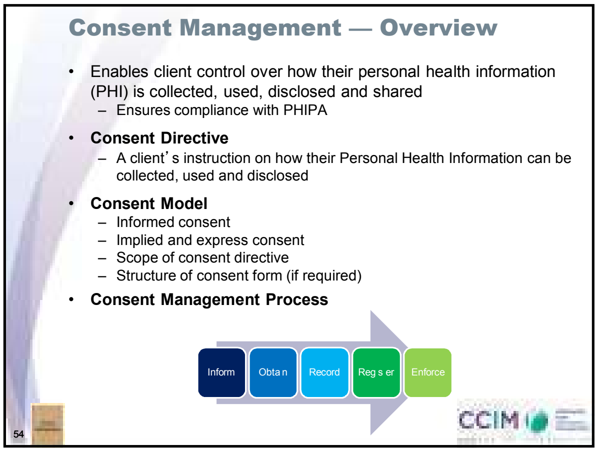
- Internal approval of revised/new process(es)
- Provide training and awareness to all staff members in your organization (not just clinicians or IAR users)
- External communications (clients and third parties)
  - Poster, brochure, corporate website, centralized e-mail box

52

Consent Management

Consent Management
CCIM

53



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**

54

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 not 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 not 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)

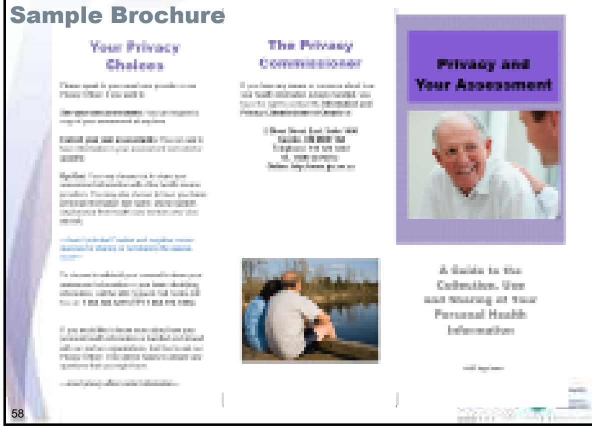
Telephone No: ______________________ Address: ______________________

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

The Privacy Commissioner

Privacy and Your Assessment

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

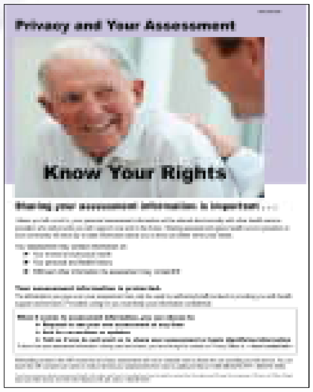
Sample Brochure

Your Personal Health Information

Sharing Your PHI

Privacy and Security of Your Information

Sample Poster

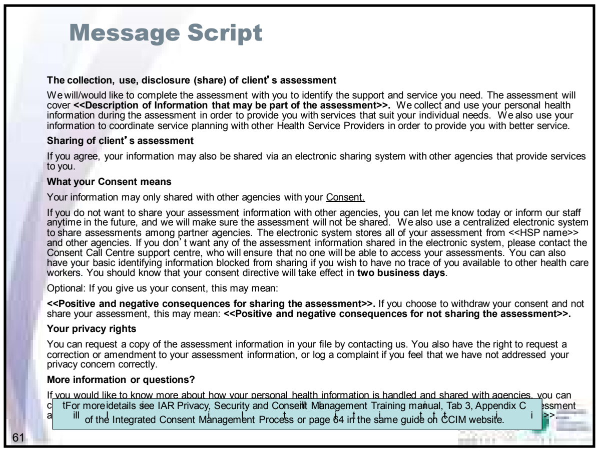


Privacy and Your Assessment

Know Your Rights

Sharing your assessment information is important...

Your assessment information is protected.



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 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

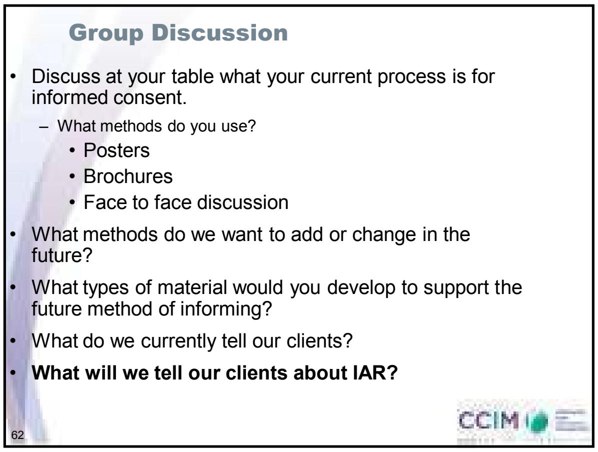
You can request a copy of the assessment information in your file by contacting us. You also have the right to request a correction or amendment to your assessment information, or log a complaint if you feel that we have not addressed your privacy concern correctly.

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 c essment a >>.

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.

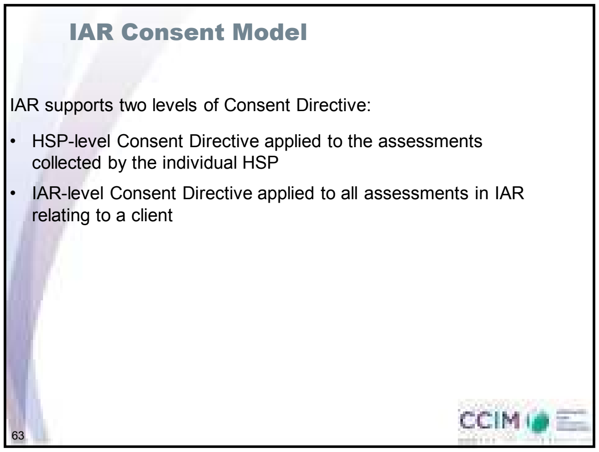
61



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?**

62

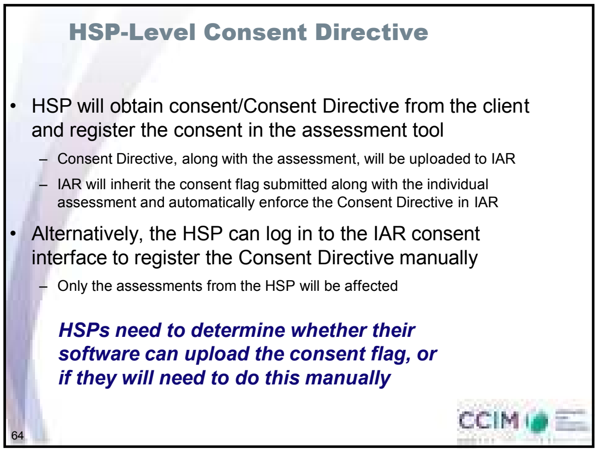


IAR Consent Model

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

63

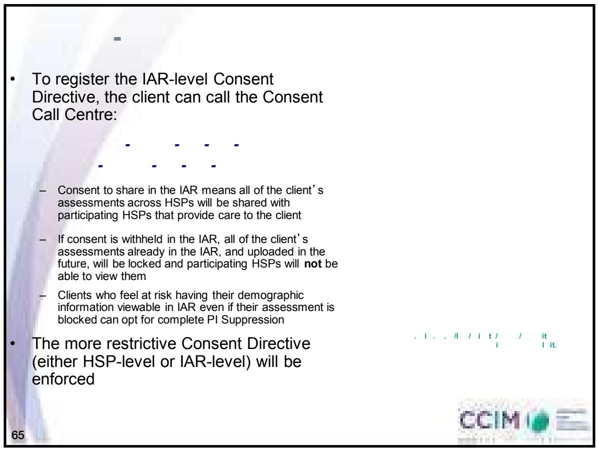


HSP-Level Consent Directive

- 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

64



-

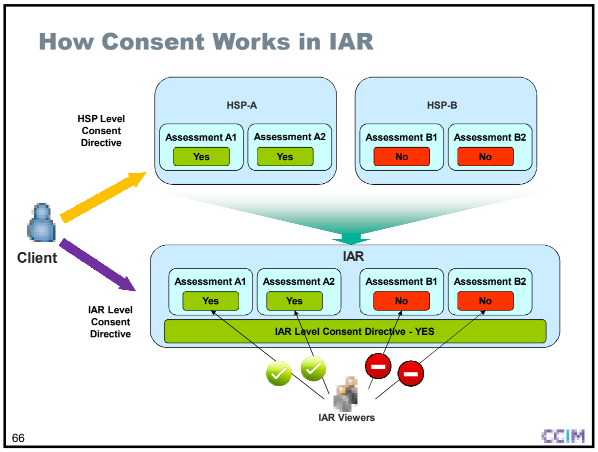
- To register the IAR-level Consent Directive, the client can call the Consent Call Centre:

- - - -

- - - -

  - 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

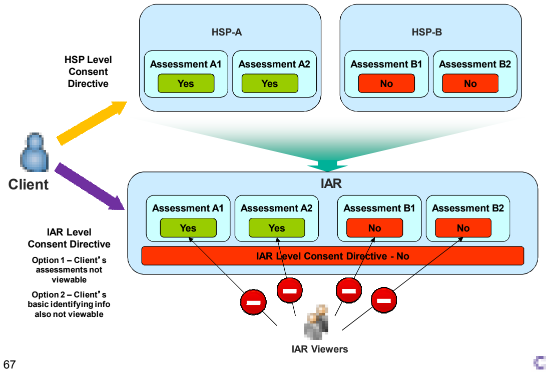
65



How Consent Works in IAR

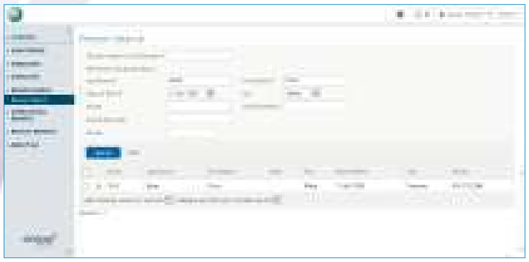
66

How Consent Works in IAR (Cont'd)



67

IAR Consent Directive in Effect



68

IAR Consent Directive with PI Suppression in effect

69

HSP Assessment Consent Directive in Effect

70

Scenarios: Client Needs HSP Help

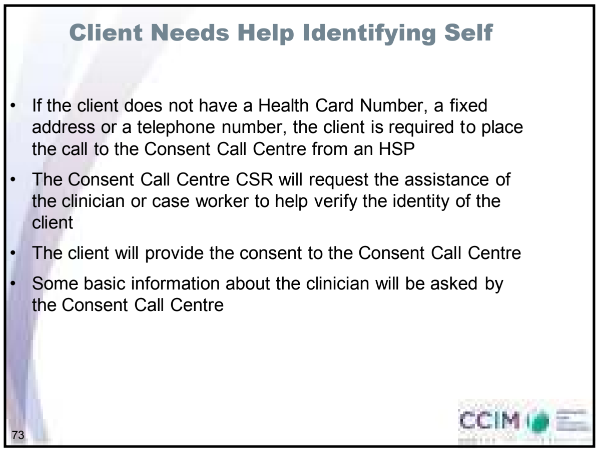
1. Client is not comfortable or not able to call the Consent Call Centre by himself / herself
2. Client does not have enough information to identify himself / herself
3. Client has a substitute decision maker (SDM) who wants to provide a Consent Directive on his / her behalf

71

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

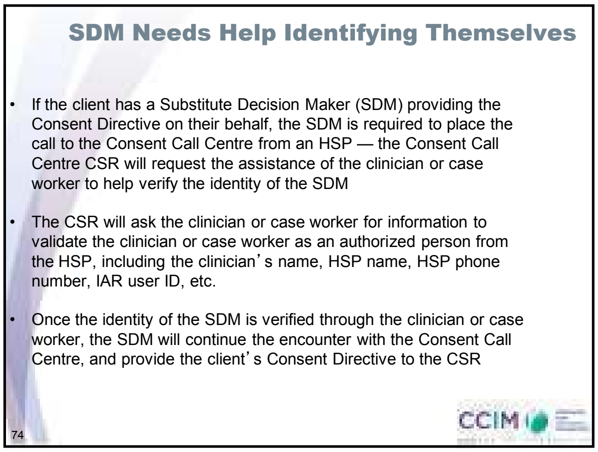
72



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

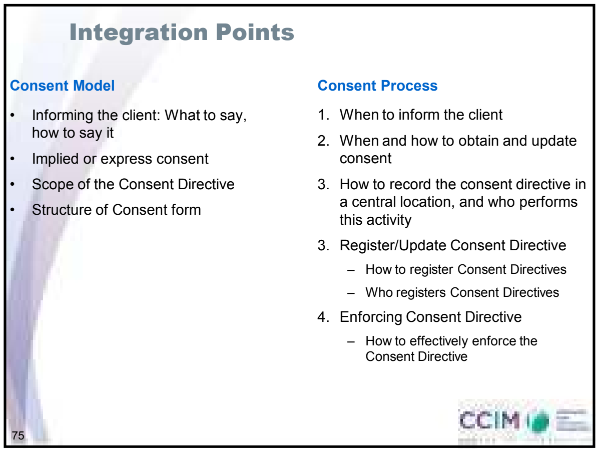
73



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

74



Integration Points

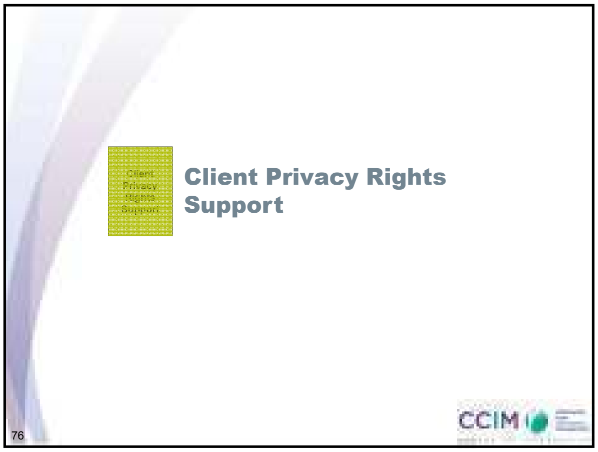
Consent Model

- 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

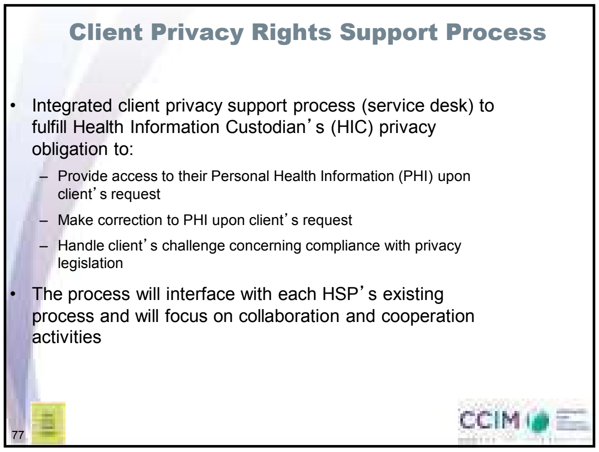
75



Client Privacy Rights Support

Client Privacy Rights Support

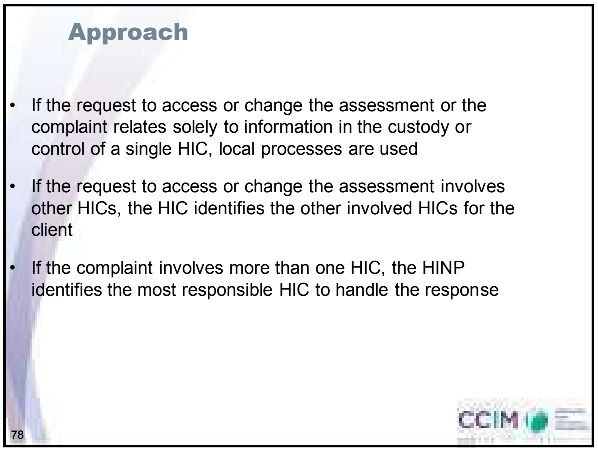
76



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

77



Approach

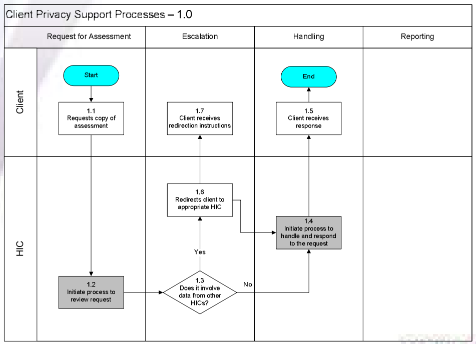
- If the request to access or change the assessment or the complaint relates solely to information in the custody or control of a single HIC, local processes are used
- If the request to access or change the assessment involves other HICs, the HIC identifies the other involved HICs for the client
- If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

78

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



Client Privacy Support Processes – 1.0

Request for Assessment | Escalation | Handling | Reporting

Client | HIC

Start

1.1 Requests copy of assessment

1.2 Initiate process to review request

1.3 Does it involve data from other HICs?

Yes

No

1.4 Initiate process to handle and respond to the request

1.5 Client receives response

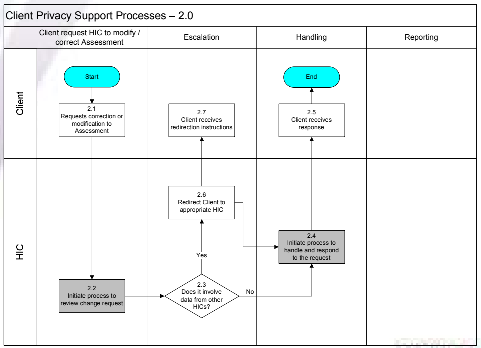
End

1.6 Redirects client to appropriate HIC

1.7 Client receives redirection instructions

Shaded boxes indicate existing steps in HSPs.

2.0 – Request a Correction to Assessment



Client Privacy Support Processes – 2.0

Client request HIC to modify / correct Assessment | Escalation | Handling | Reporting

Client | HIC

Start

2.1 Requests correction or modification to Assessment

2.2 Initiate process to review change request

2.3 Does it involve data from other HICs?

Yes

No

2.4 Initiate process to handle and respond to the request

2.5 Client receives response

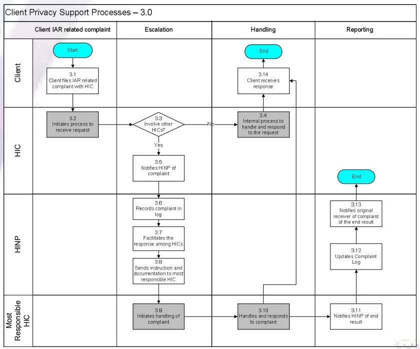
End

2.6 Redirect Client to appropriate HIC

2.7 Client receives redirection instructions

Shaded boxes indicate existing steps in HSPs.

3.0 – File a Complaint With the HIC



Client Privacy Support Processes – 3.0

Client IAR related complaint | Escalation | Handling | Reporting

Client | HIC | HINP | Most Responsible HIC

Start

3.1 Client files IAR related complaint with HIC

3.2 Initiates process to receive request

3.3 Involve other HICs?

No

3.4 Internal process to handle and respond to the request

Yes

3.5 Notifies HINP of complaint

3.6 Records complaint in log

3.7 Facilitates the response among HICs

3.8 Sends instruction and documentation to most responsible HIC

3.9 Initiates handling of complaint

3.10 Handles and responds to complaint

3.14 Client receives response

End

3.11 Notifies HINP of end result

3.12 Updates Complaint Log

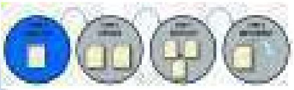
3.13 Notifies original receiver of complaint of the end result

End

Shaded boxes indicate existing steps in HSPs.

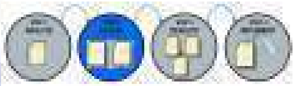
Client Privacy Rights Support: Analyze

- 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

85

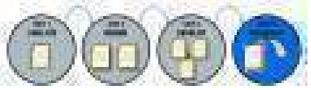
Client Privacy Rights Support: Develop

- 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

86

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)



87

User Account Management

User Account Management

88

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

89

IAR Business Roles and User Accounts: Approach

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

90

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

91

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

92

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

93

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

94

IAR User Account Management Process Maps

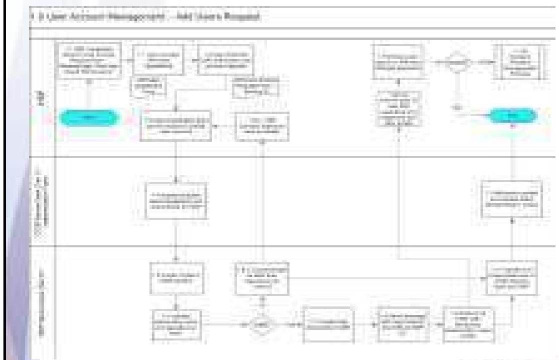
HSP can:

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

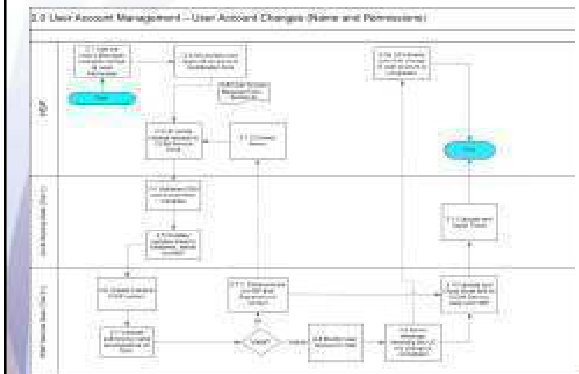
95

1.0 Creation of New Users

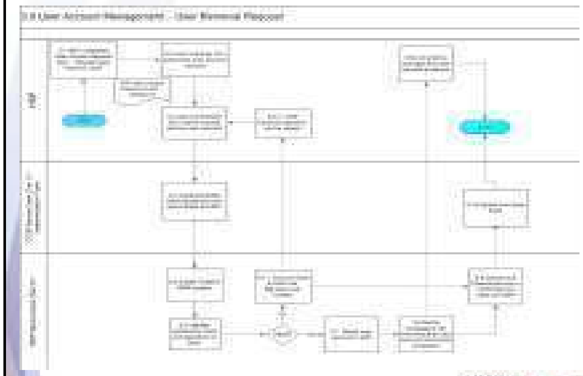


96

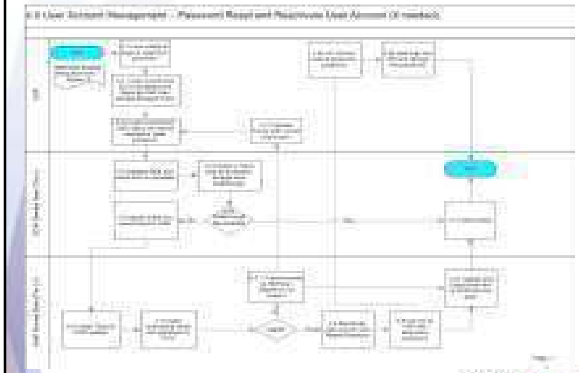
2.0 Request to Change


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

3.0 Removal of Users



4.0 – Password Reset and Reactivate User Account


4.0 User Account Management – Password Reset and Reactivate User Account (if needed)
HSP

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

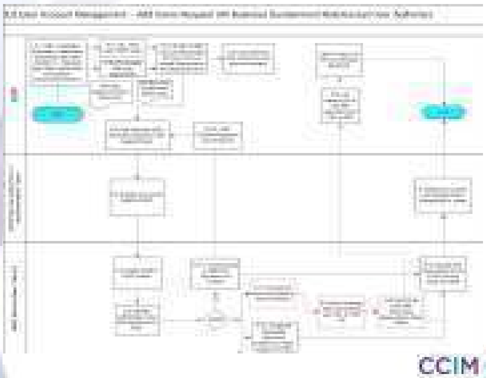
- Each participating organization has to identify the users for each Business Sustainment Role.
  - A UA should be someone in management or someone who has knowledge of who should use IAR
  - PO will be responsible for all Privacy issues (including privacy Complaints) and privacy log Reviews
  - A UC 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

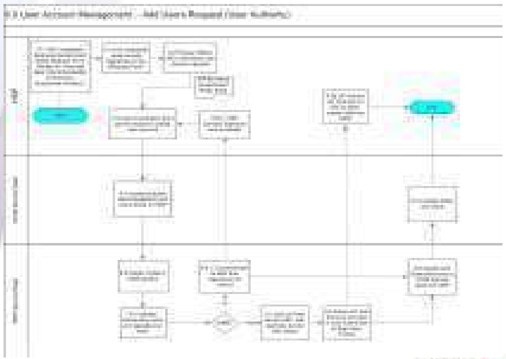
1. Add a user for any of the Business Sustainment Role except UA (e.g. PO, UC, Technical Lead, EMPI Lead)
2. Add a user for UA Role
3. Change or update of user information (e.g., phone number, location, email, etc.) for any of the Business Sustainment Role except UA
4. Change or update of user information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

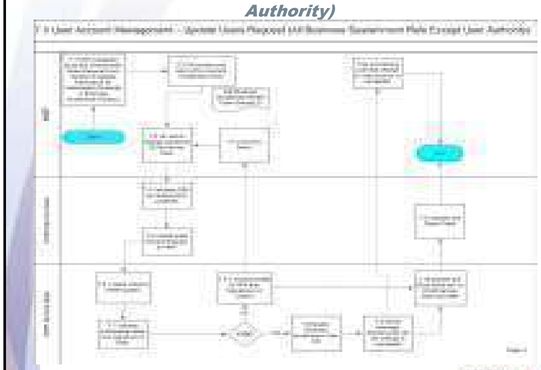
5.0 *Create (or Add) All Business Sustainment Role Users (Except User Authority)*



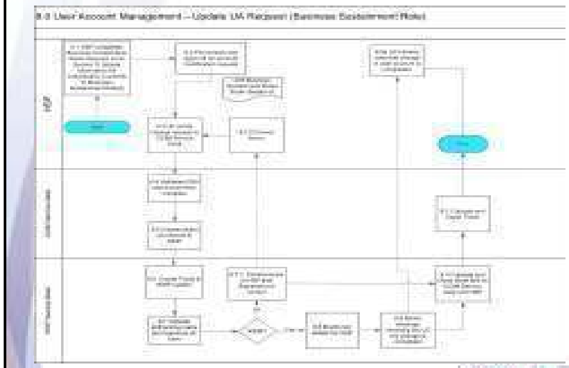
6.0 – Create User Authority Role User



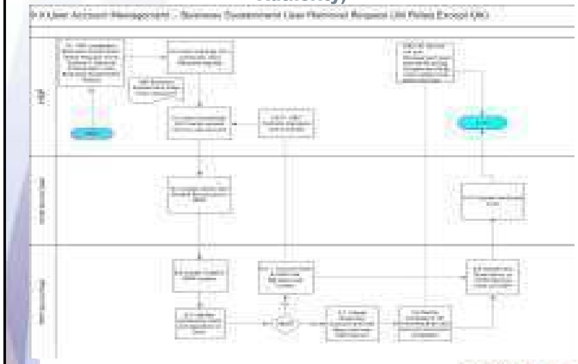
7 .0– Update All Business Sustainment Role (Except User Authority)

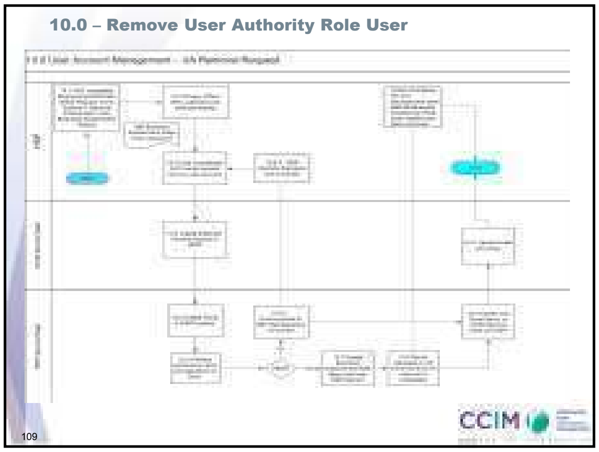


8.0 – Update (or Change) User Authority Role User

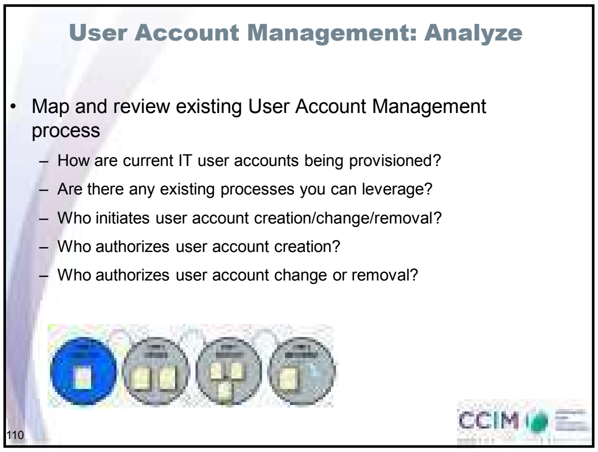


9.0 – Remove All Business Sustainment Role (Except User Authority)



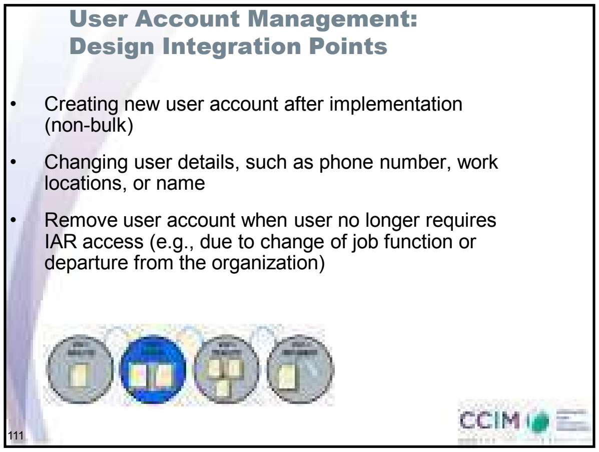


10.0 – Remove User Authority Role User



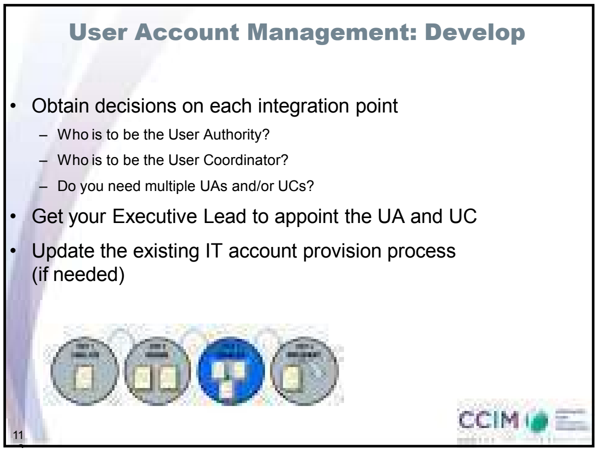
User Account Management: Analyze

- 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?



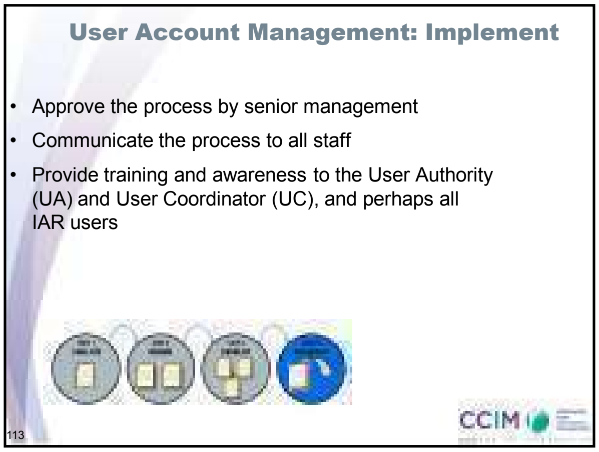
User Account Management: Design Integration Points

- 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)



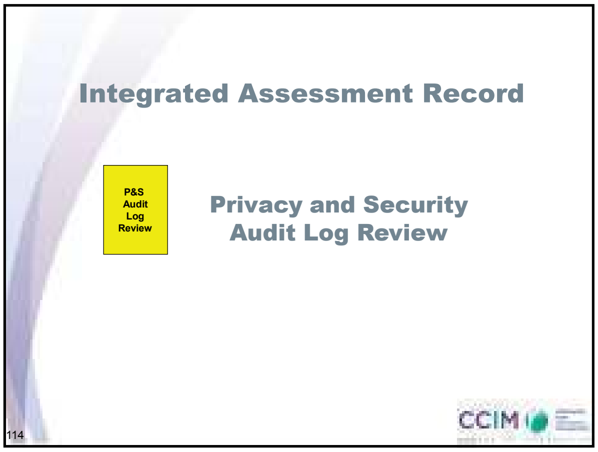
User Account Management: Develop

- 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

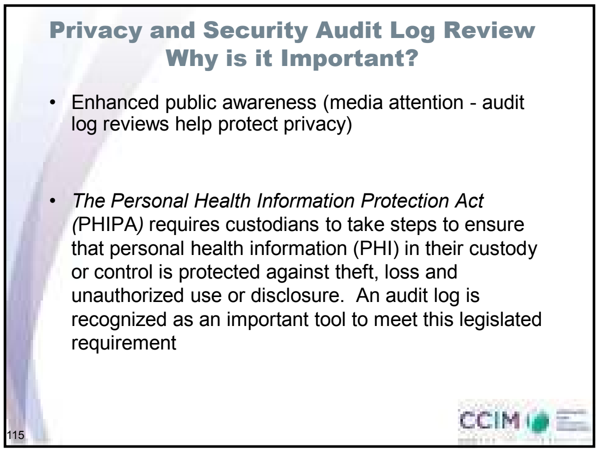
- Approve the process by senior management
- Communicate the process to all staff
- Provide training and awareness to the User Authority (UA) and User Coordinator (UC), and perhaps all IAR users



Integrated Assessment Record

P&S Audit Log Review

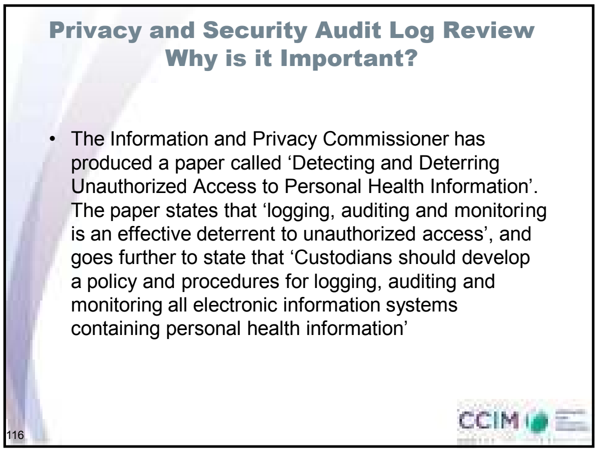
Privacy and Security Audit Log Review



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

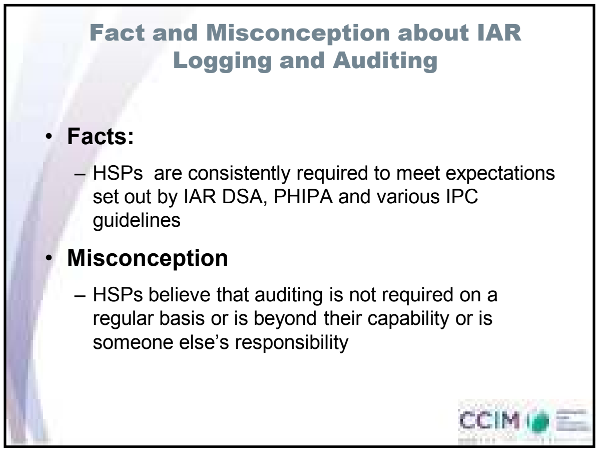
115



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'

116



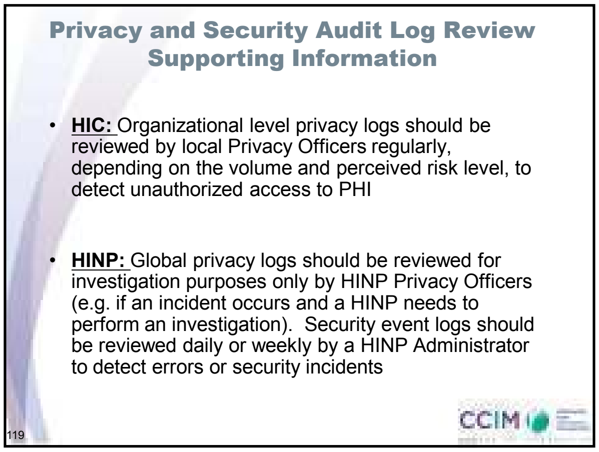
Fact and Misconception about IAR Logging and Auditing

- **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

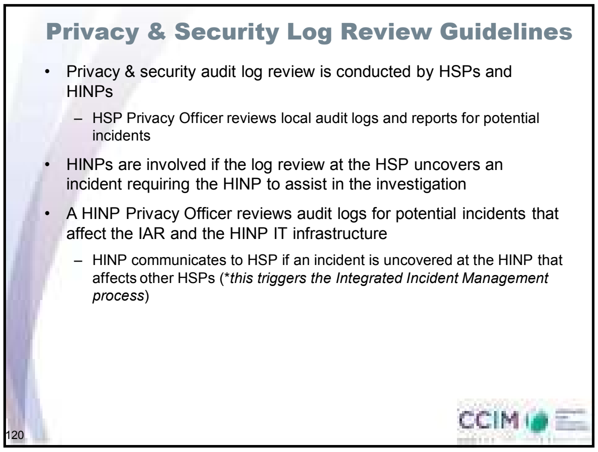
118



Privacy and Security Audit Log Review Supporting Information

- **<u>HIC:</u>** 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
- **<u>HINP:</u>** 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

119



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*)

120

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

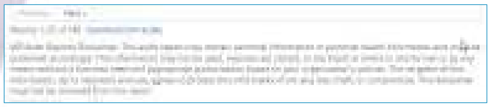
- Advanced log review activities
  - Review privacy logs
  - Review clinical logs
  - Review logins by users who have not logged in for over 90 days
  - Review PS5 report with users to validate they only accessed PHI in the course of providing healthcare to clients

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



Classification: Medium

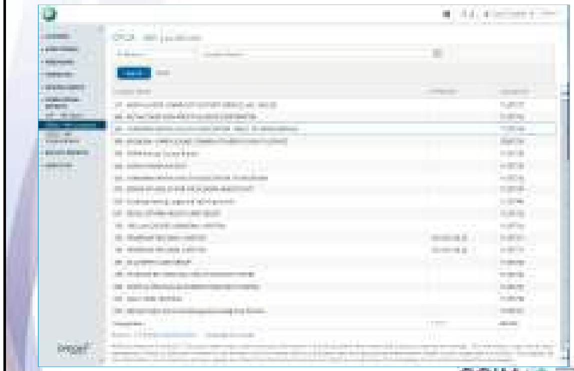
Operational Reports

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

OP1 – List of IAR Users

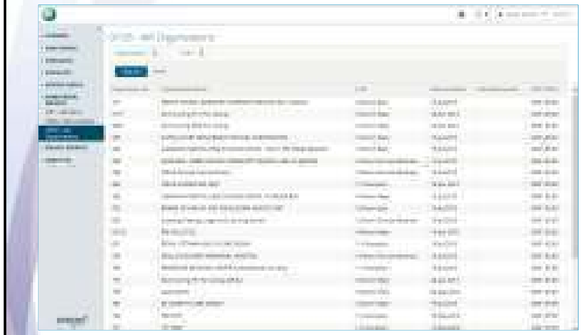
127

OP2A — List of IAR Locations



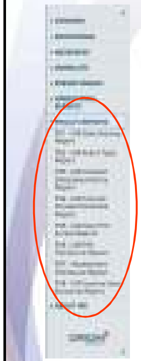
128

OP2B — List of IAR Organizations



129

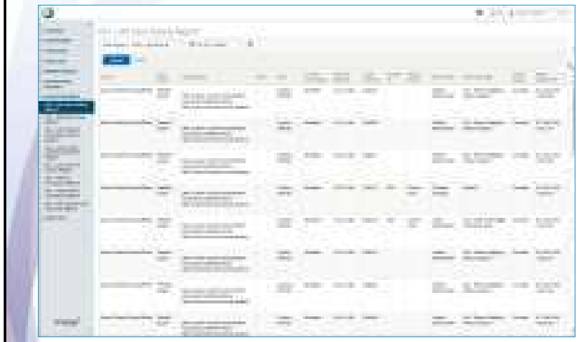
Privacy Reports



- 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

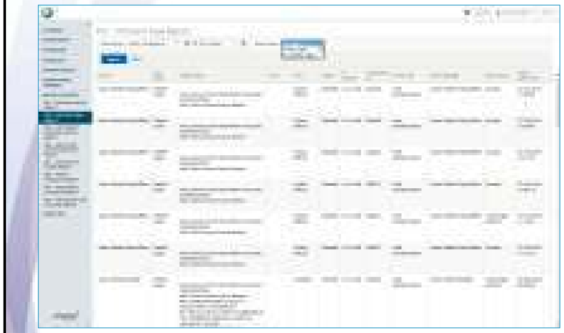
130

PS1 – User Activity Report



131

PS2 – Event Type Report



132

PS3 – IAR Consent Directives History Report

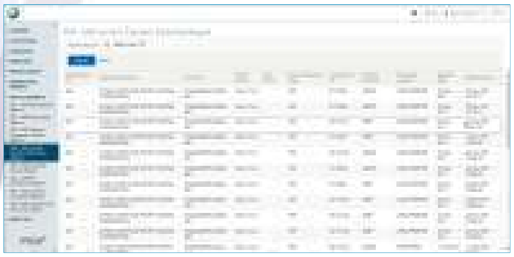
133

PS3 – IAR Consent Directives History Report

Search Criteria Options

134

PS4 – IAR Current Consent Directive Report



135

PS4 – IAR Current Consent Directive Report

Search Criteria Options

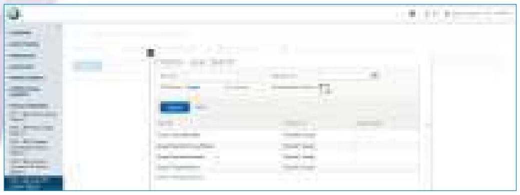
136

PS5 – User PHI Access Report

137

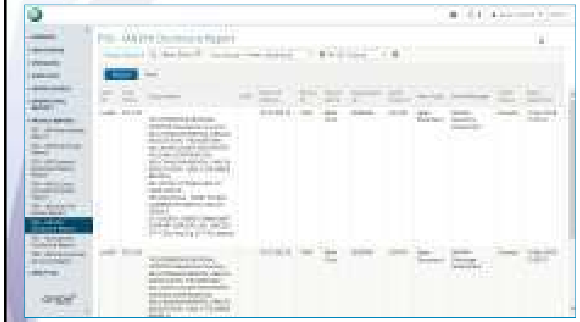
PS5 – User PHI Access Report

Search Criteria Options



138

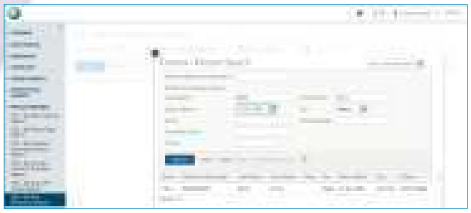
PS6 – IAR PHI Disclosure Report



139

PS6 – IAR PHI Disclosure Report

Search Criteria Options

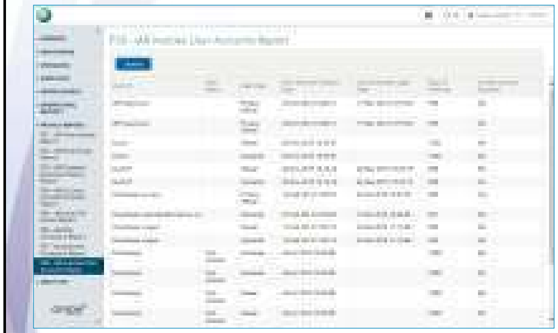


140

PS7 – Assessment Disclosure Report

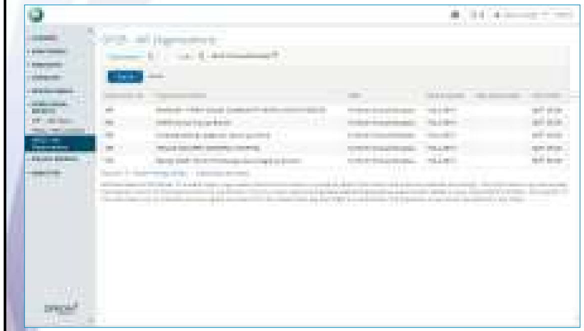
141

PS8 – Inactive Users Report



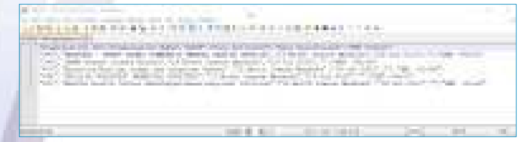
142

Report Format



143

Report in CSV Format



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

144

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

145

Clinical Log

- Fields available to refine search

146

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

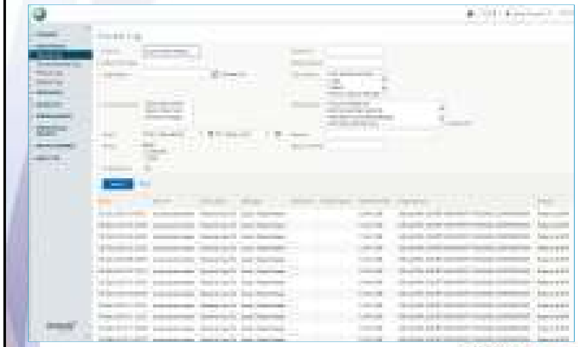
– Account Validation
– Add Group Membership
– Add Role Group Membership
– Add Role Membership
– Add mapping agent
– Assign Privacy Policy
– Authenticated Login
– Background Task
– Configuration
– Configure CCOW context manager
– Copy Entry Point to Application
–Create Custom Privacy Policy
–Create Entry 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

147

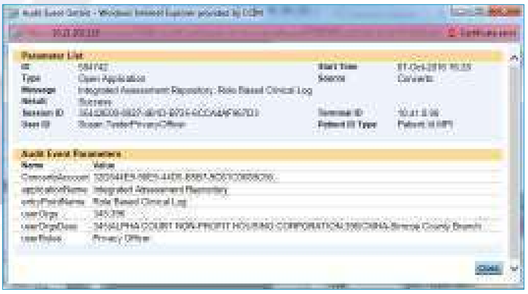
Clinical Log – Search Results



148

Clinical Log

- Search Criteria



Parameter List

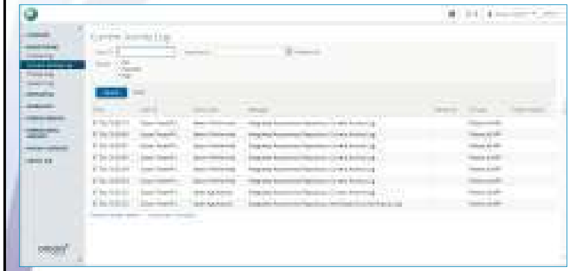
ID 584742 Start Time 01-Oct-2016 15:23
Type Open Application Source Consents
Message Integrated Assessment Repository: Role Based Clinical Log
Result Success
Session ID [illegible] Terminal ID [illegible]
User ID Susan.Tester/PrivacyOfficer Patient ID Type Patient [illegible]

Audit Event Parameters

Name Value
ConnexionAccount [illegible]
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

149

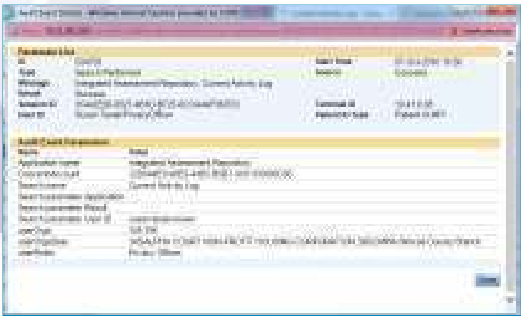
Current Activity Log



150

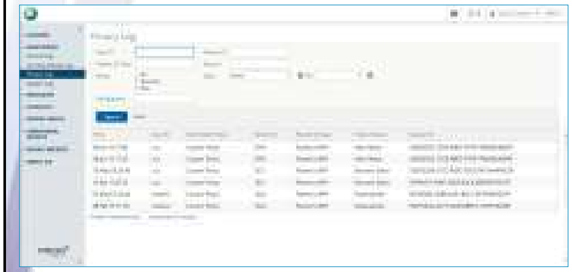
Classification: Medium

Current Activity Log



Privacy Log

- Search Criteria



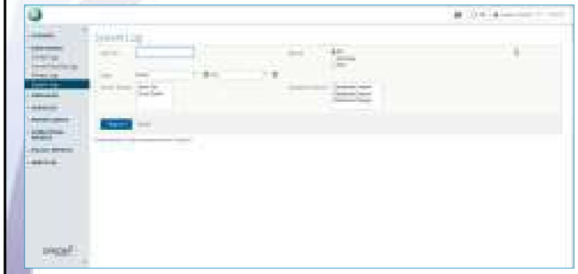
Privacy Log

- **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

- Search Criteria

System Log

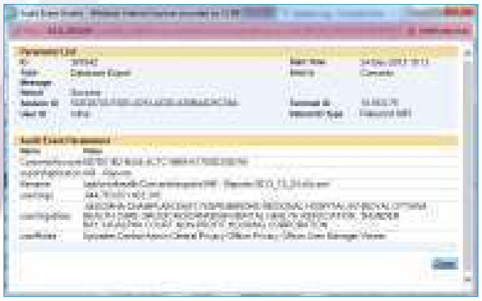


System Log – Search Results

Date Range

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

System Log – Log Entry Details



Parameter List

Audit Event Parameters

Name	Value
[illegible]	[illegible]

Classification: Medium

Privacy Review

Privacy Review

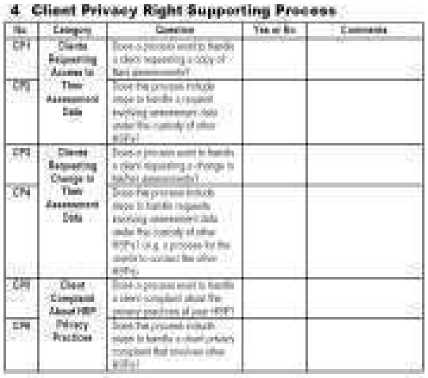
Privacy Operations Review

- 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

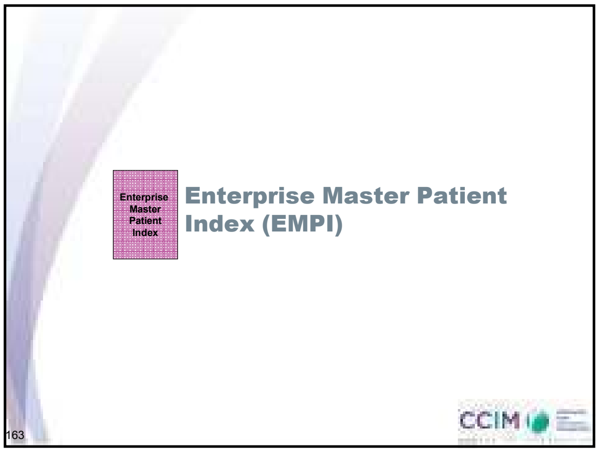


4 Client Privacy Right Supporting Process

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

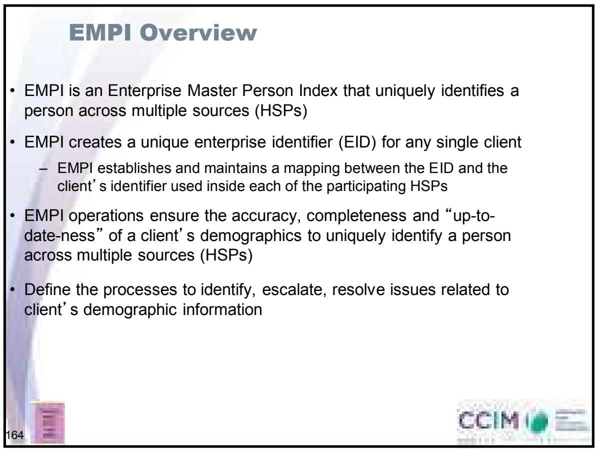
Integration Points

- 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)

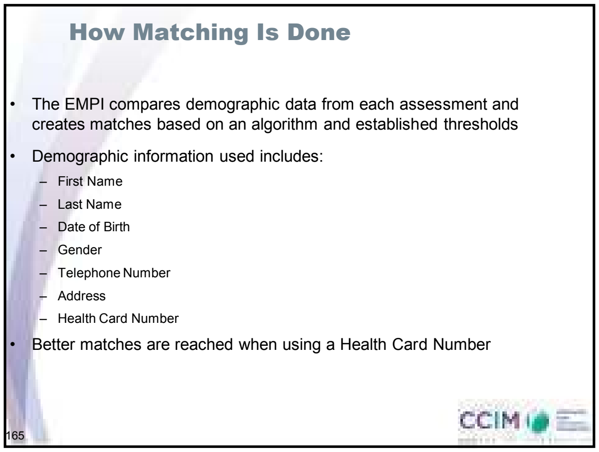
163



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

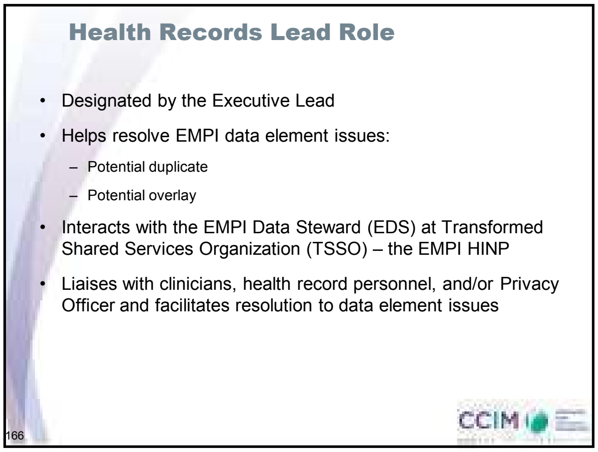
164



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

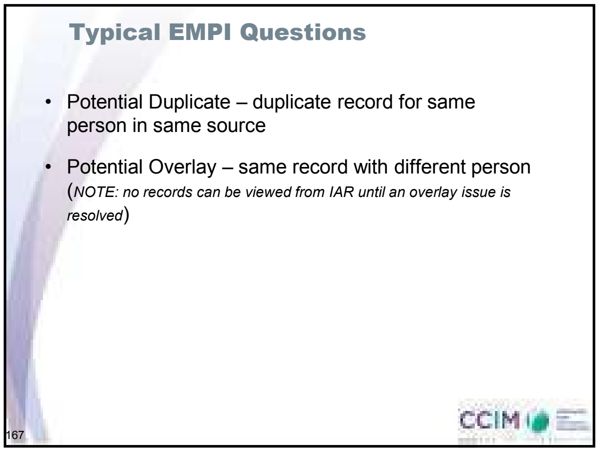
165



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

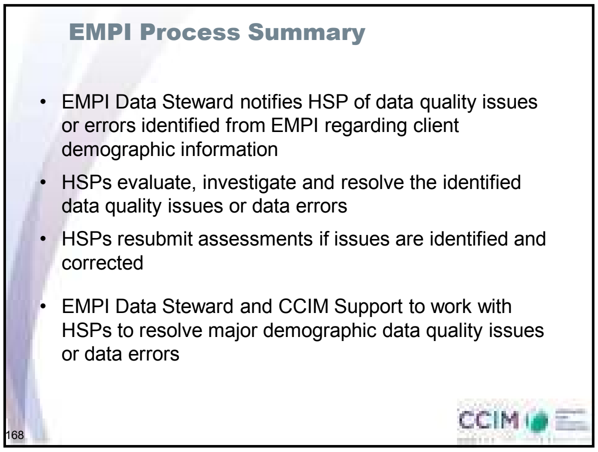
166



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*)

167



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

168

Communication

Awareness and Training

Next Steps

CCIM

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

CCIM

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

CCIM

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

CCIM

Thank You!

Integrated Assessment Record
SUPPORT CENTRE

Monday to Friday	8:30 a.m. – 4:30 p.m. 4:30 p.m. – midnight 8:30 am – 5.00 pm To leave a message	[illegible] [illegible] 1.866.909.5600 option 8 [illegible]
Email	iar@ccim.on.ca	

CCIM

GTA HINP Contact Information

Issues	Contact	Phone & Email
• Report an IAR incident • Escalate an IAR privacy complaint from client • Require audit log investigation support • General IAR privacy and security inquiries	William Osler Health Systems (WOHS) Privacy Officer: Jennifer Beaumont	Tel: 905-494-2120 x59102 Fax: 905-494-6866 IARPrivacy@williamoslerhs.ca

Northern HINP Contact Information

Issues	Contact	Phone & Email
• Report an IAR incident • Escalate an IAR privacy complaint from client • Require audit log investigation support • General IAR privacy and security inquiries	Health Sciences North (previously known as Sudbury Regional Hospital) Privacy Officer: Nancy Andrews	Tel: 705-523-7100 x3982 Fax: 705-523-7075 HINPPrivacyOfficer@hsnsudbury.ca

South West HINP Contact Information

Issues	Contact	Phone & Email
• Report an IAR incident • Escalate an IAR privacy complaint from client • Require audit log investigation support • General IAR privacy and security inquiries	TransForm Shared Service Organization (TSSO) Privacy Officer: Mark Loffhagen	Tel: 519-464-4400 x 8488 Fax: 519-464-4450 privacy@transformsso.ca

Health Service Provider (HSP) Privacy and Security Implementation Checklist

Group	Section	Questions	Yes	No	Action Plan
DSA	**DSA**	Did the HSP sign the Data Sharing Agreement (DSA)?			
General	**Governance**	Has the HSP designated a person responsible for the protection of personal health information (PHI) in the Integrated Assessment Record (IAR) and the privacy of clients/patients?			
		Does the HSP publish/announce the contact details for the HSP's IAR privacy contact person?			
	Privacy Operation	Does the HSP have information practices in place that comply with PHIPA and that describe its practices relating to the collection, use, disclosure, retention and disposal of PHI?			
		Does the HSP have an established consent management process that meets PHIPA requirements?			
		Does the HSP have an established breach management process?			
		Does the HSP have an established client privacy right support process?			
		Does the HSP have an established user account management process?			
		Does the HSP have an established log review process?			
Consent Management	**Consent Model**	Has the HSP determined the consent model – implied, express consent or combination?			
		Does the consent model cover all PHI usage scenarios?			
		Is the scope of the consent directive clearly defined?			
		Does the HSP define the supported "break-the-glass" approach and mechanism?			
	Informing the Client/Patient	Does the HSP define the approach to informing the client/patient for consent?			
		Has the HSP developed the material used to inform the client/patient?			
		Does the material cover the following topics: -What data is being collected, used, disclosed -How the data is collected, used, disclosured and with whom -The purpose for which the data is collected, used and disclosed -Consequences of giving or withholding consent -Client/patient's privacy rights			
	Recording the Consent Directive	Does the HSP archive the consent form and/or log all consent directives requested by clients centrally?			
	Registering (or Updating) the Consent Directive	Has the HSP established the process to register or update the consent directives requested by the clients in the assessment tool or IAR system?			
	Enforcing the Consent Directive	Are consent directives requested by clients enforced by technology and/or the administrative process?			
Log Review	**Log Review Plan**	Has a person from the HSP been assigned to regularly review the IAR audit log?			
		Has the HSP developed an IAR audit log review plan that defines the how frequent the log should be reviewed?			
		Does the IAR audit log review plan describe the type of events and patterns that must be reviewed?			
Client Privacy Right Support Process	**Clients Requesting Access to Their Assessment Data**	Does a process exist to handle a client request for a copy of their assessments?			
		Does this process include steps to handle a request involving assessment data under the custody of another HSP?			
	Clients Requesting Change to Their Assessment Data	Does a process exist to handle a client request for a change to their assessment?			
		Does this process include steps to handle requests involving assessment data under the custody of another HSP? (i.e., a processs to contact the other HSPs)			
	Client Complaint About Organization Privacy Practices	Does a process exist to handle a client complaint about the privacy practices of your organization?			
		Does a process exist to escalate a privacy complaint to the Health Information Network Provider (HINP) Privacy Officer?			
Incident Management	**Incident Management Process**	Does an incident management process exist to handle potential privacy and security incidents in IAR?			
		Has the internal incident coordinator and/or privacy breach coordinator been identified for the IAR project within your organization?			
		Has the internal incident coordinator and/or privacy breach coordinator been made known to your staff so they know who to contact for an incident or breach? If not, please provide plans as to when that will be accomplished			
	Escalation	Is there a process in place for incident coordinator and/or privacy breach coordinator to contact the HINP Privacy Officer, who is responsible for facilitating collaboration among HSPs that are affected?			
	Investigation	Does your HSP establish the incident investigation processes?			
	Notification	Does your HSP have a standard procedure, as required by PHIPA, to notify the IPC if there is a privacy breach that involves a client's personal health information?			
		Does your HSP have a standard procedure to notify clients if a privacy breach involves their personal health information?			
User Account Management	**New User Account Request**	Does your organization designate a person for the role of User Authority (UA) to authorize user access to IAR?			
		Does the designated User Authority (UA) sign the User Account Request form to authorize new IAR user accounts?			
		Are new users required to read and sign the IAR User Agreement?			
	User Account Information Change	Does your organization have a designated person for the role of user authority to authorise the change and a User Coordinator (UC) for liaising on day-to-day user account management activities?			
		Does the Organization use the updated "IAR HSP and User Access Form" to initiate user account information changes?			
	User Account Removal	Does your organization have a designated person for the role of User Authority to authorise removal of the accounts. Does the organization use the "Updated IAR HSP and User Access Form" to initiate user account removals?			
Awareness and Training	**Training**	Is privacy and security training provided to the HSP staff participating the IAR project?			
	Privacy Officer	Do the Privacy Officer reponsible for the IAR privacy and security, understand their roles and responsibilities including all the privacy and security processes?			
	IAR Users	Do all IAR users understand IAR privacy and security requirements and their responsibilities ?			
	HSP Staff	Is HSP staff aware of IAR privacy and security requirements and able to communicate it to the clients?			

Integrated Incident Management Process

Integrated Assessment Record (IAR)

Version 4.0

January, 2016

Table of Contents

Introduction

Incident Management is the ability to provide end to end management of a series of events that are initiated in response to a Privacy or Security breach.

The Integrated Assessment Record (IAR) integrated incident management process deals with IAR-related privacy and security incidents in a coordinated fashion. Incidents that affect multiple participating organizations will involve both the Health Information Network Provider (HINP) and the affected Health Information Custodians (HICs); as well as the privacy officers at the HINP and the participating organizations.

An **incident** is the contravention of a policy, procedure, duty or contract, or a situation of interest that results in the potential exposure of sensitive information to unauthorized parties. Each participating organization will use its existing incident management processes to handle incidents.

The following is a sample of privacy and security incidents that may occur in IAR:

- Printed patient assessment information is left in a public area (e.g. Tim Horton)
- Theft, loss, damage, unauthorized destruction or modification of patient records
- Inappropriate access of patient information by unauthorized users
- Large amount of IAR records were accessed by a single individual in a short period of time (out of the ordinary)
- User account and password was compromised
- Network infrastructure is attacked by hackers
- Violation of joint security and privacy policies or procedures

The Information & Privacy Commissioner (IPC) recommends that the HINP develops a privacy breach protocol to handle any potential privacy breach incident. The protocol enables the HINP and participating organizations to respond quickly and in a coordinated way during a privacy breach. The protocol also defines the roles and responsibilities of each party in this integrated environment, to ensure that investigation and containment are more effective and efficient, and remediation easier to implement.

Incidents can originate from the HIC or the HINP. An incident can also be reported by the clients or a 3rd party of a HIC, or a 3rd party to the HINP.

Following are the four scenarios described in this document.

Scenario 1 – Incident detected by the HIC

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

Scenario 2 – Incident reported by client or 3rd party to the HIC

- Client reports: "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 records?"
- Someone (non-patient) found printed patient assessment information on HIC letterhead left at Tim Hortons

Scenario 3 – Incident detected by the HINP

- IAR backup data unaccounted for (loss or stolen)
- IAR database hacked into by hackers
- Large amount of IAR records were accessed by a single individual in a short period of time (out of the ordinary)
- Missing data backup tape that contains server and system data, but no personal health information (PHI)

Scenario 4 – Incident reported by 3rd party to the HINP

- Record management service provider reports to HINP that one IAR data backup tape went missing during transit
- Missing data backup tape that contains server and system data, but no PHI

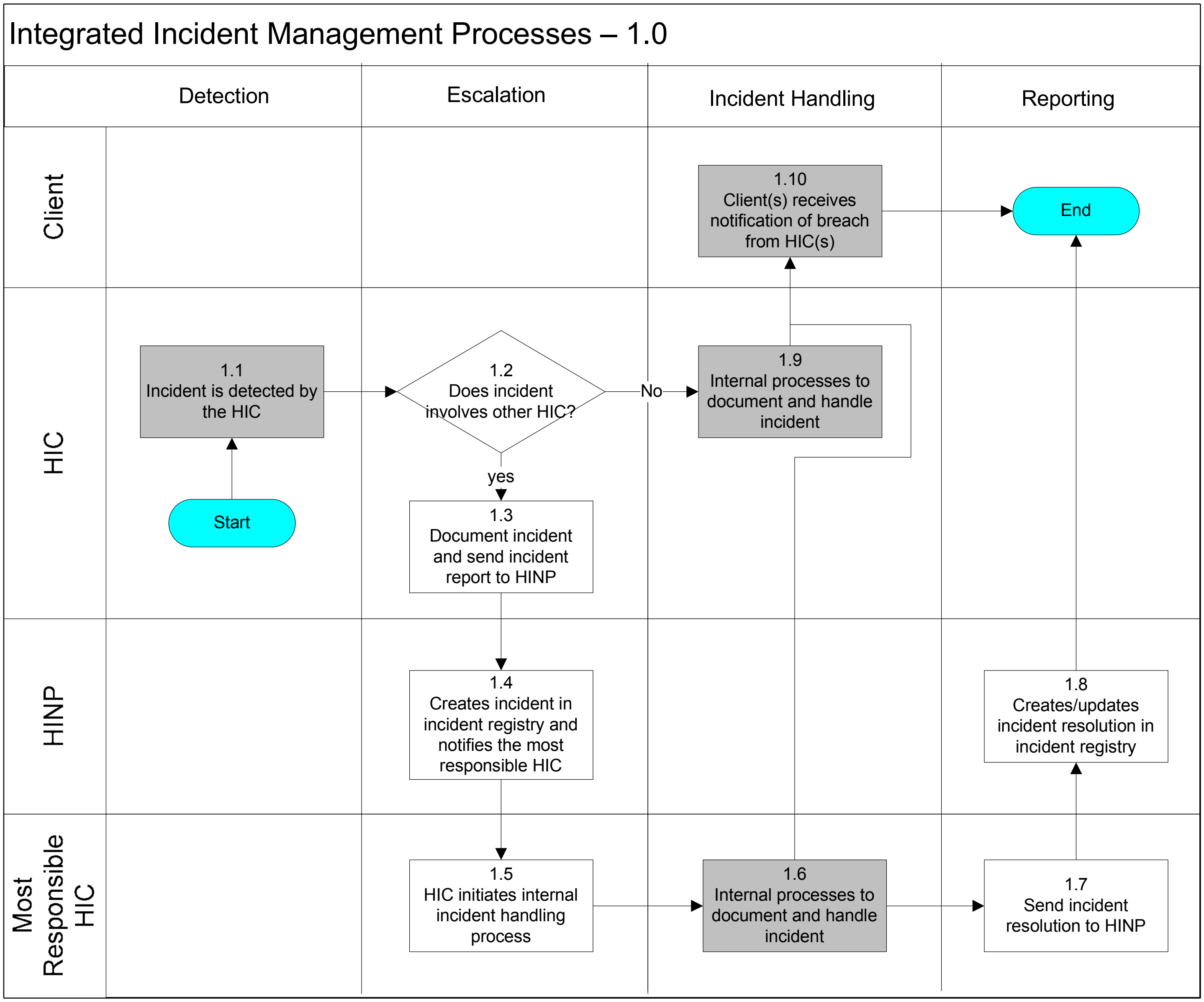
Notification of Clients

PHIPA requires the Health Information Custodian to notify the clients if there is a privacy breach that involves their personal health information. In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach concerning his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in developing the best notification approach to the client. This notification can be in the form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

This document translates the above scenarios into defined processes and steps as it relates to the Integrated Assessment Record. It identifies responsibilities and delineates between those tasks which should already be in place within any given Health Information Custodian and those tasks which are introduced with the IAR.

Processes

Scenario 1 – Incident Detected by HIC



Integrated Incident Management Processes – 1.0
Detection
Escalation
Incident Handling
Reporting
Client
HIC
HINP
Most Responsible HIC
1.10 Client(s) receives notification of breach from HIC(s)
End
1.1 Incident is detected by the HIC
1.2 Does incident involves other HIC?
No
1.9 Internal processes to document and handle incident
yes
Start
1.3 Document incident and send incident report to HINP
1.4 Creates incident in incident registry and notifies the most responsible HIC
1.8 Creates/updates incident resolution in incident registry
1.5 HIC initiates internal incident handling process
1.6 Internal processes to document and handle incident
1.7 Send incident resolution to HINP

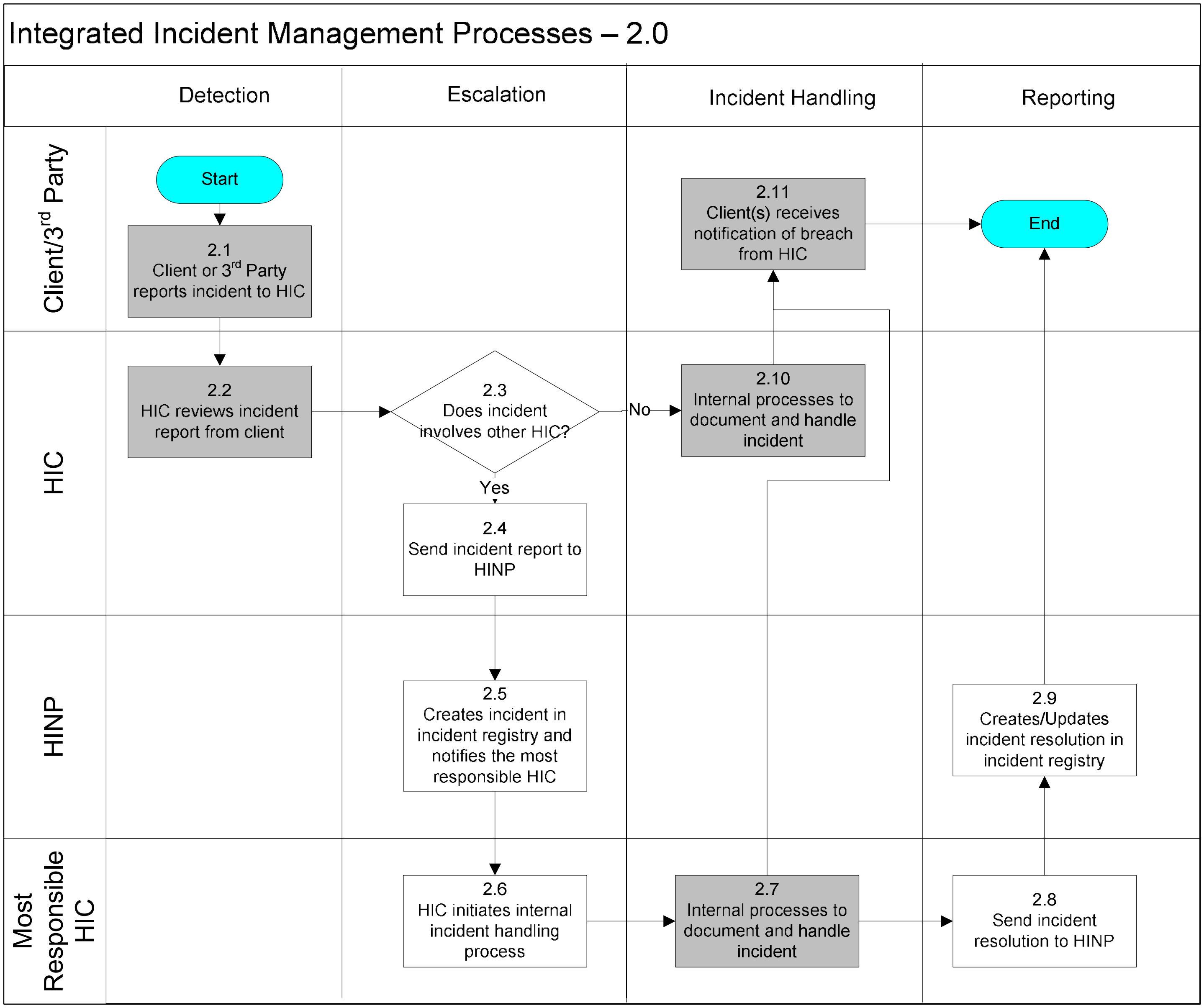
*Note: *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 1 **Incident detected by HIC** Sample scenarios: • Printed patient assessment records were lost • User account and password were compromised • IAR upload files have been compromised possibly by hackers breaking in to network at participating organization (HIC)		
1.1	The incident is detected by the normal incident detection and monitoring process at the HIC or staff at HIC reports incident internally to HIC privacy officer.	Health Information Custodians	Incident Report
1.2	HIC privacy officer triages the reported/detected incident - containment is the first priority - and determines if the incident involves other participating organizations/HICs. • If incident involves other HICs, then the HIC sends the Incident Report to the HINP. (Ref 1.3) • If incident involves only the local HIC, then the HIC initiates internal incident management process. (Ref 1.9) *The HIC has to notify the HINP within 24 hours of receiving the Incident Report if the incident is determined to affect other HICs in accordance with the Data Sharing Agreement*	Health Information Custodians	
1.3	HIC privacy officer documents the incident and sends the Incident Report to the HINP.	Health Information Custodians	Incident Report
1.4	HINP creates incident in the Incident Registry and notifies the most responsible HIC about the incident.	Health Information Network Provider	Incident Report and Incident Registry
1.5	The most responsible HIC initiates internal processes to handle the reported/detected incident.	Health Information Custodians	
1.6	HIC executes the internal incident handling process and documents the incident.	Health Information Custodians	
1.7	HIC sends the incident resolution detail to the HINP.	Health Information Custodians	Updated Incident Report
1.8	HINP creates or updates Incident Record with the resolutions in the	Health Information	Incident Registry

	Incident Registry.	Network Provider	
1.9	HIC initiates internal processes to document and handle the reported/detected incident.	Health Information Custodians	
1.10*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach concerning his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Scenario 2 – Incident Detected by Client or 3rd Party of HIC


Integrated Incident Management Processes – 2.0
Detection
Escalation
Incident Handling
Reporting
Client/3rd Party
HIC
HINP
Most Responsible HIC
Start
2.1 Client or 3rd Party reports incident to HIC
2.2 HIC reviews incident report from client
2.3 Does incident involves other HIC?
No
Yes
2.4 Send incident report to HINP
2.5 Creates incident in incident registry and notifies the most responsible HIC
2.6 HIC initiates internal incident handling process
2.7 Internal processes to document and handle incident
2.8 Send incident resolution to HINP
2.9 Creates/Updates incident resolution in incident registry
2.10 Internal processes to document and handle incident
2.11 Client(s) receives notification of breach from HIC
End

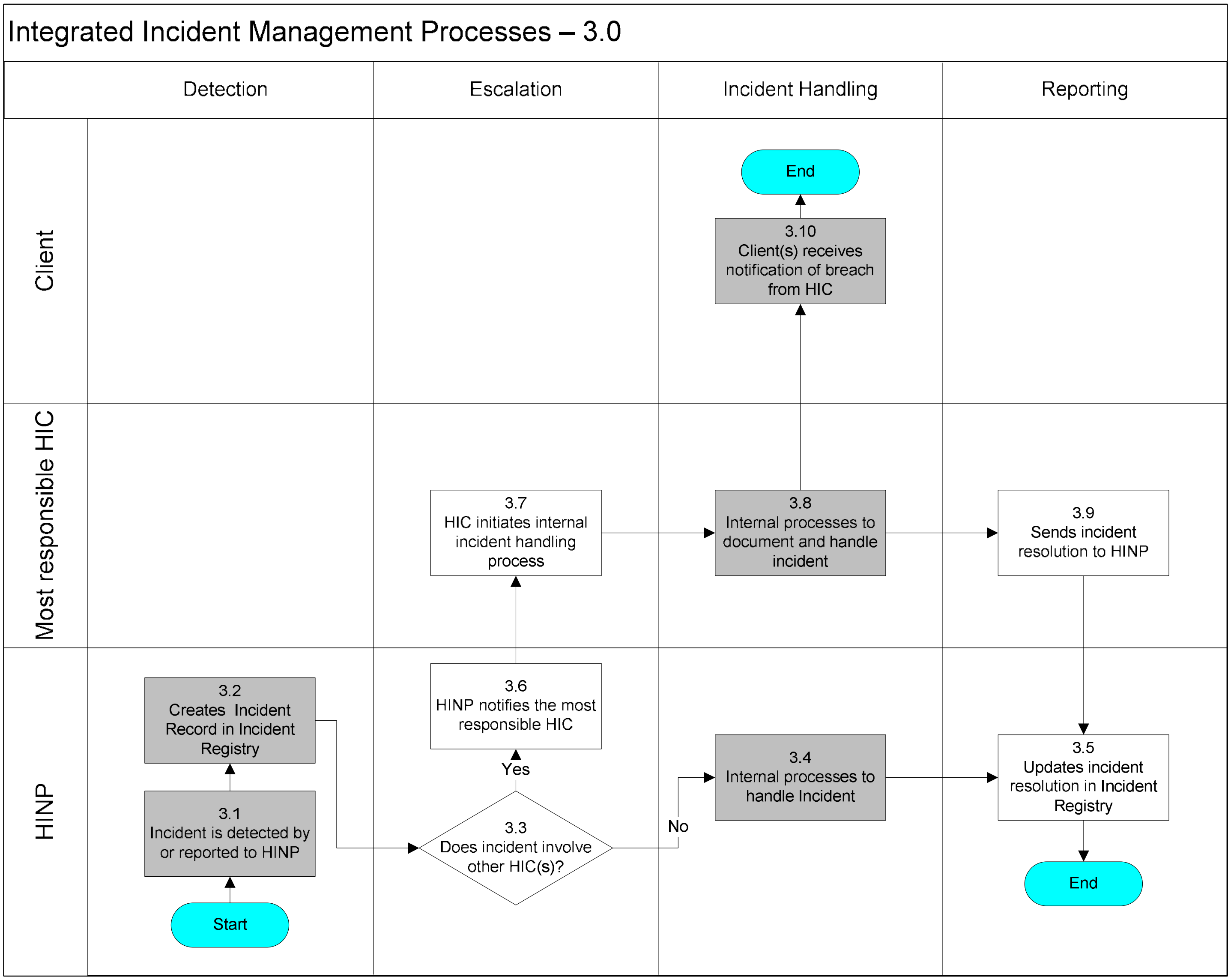
*Note: *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 2 **Incident reported by client** Sample scenarios: • A client of a HIC finds out his/her ex-spouse working at the HIC accessed his/her medical information and used it in his/her child custody case. He/she is wondering why ex-spouse can access his/her medical record for such a purpose.		
2.1	Clients or 3rd party contacts HIC privacy officer, or other HIC staff, to report the incident.	Health Information Custodian	Incident report
2.2	HIC Privacy Officer reviews the Incident Report received (containment is the first priority) from client or internal staff.	Health Information Custodian	Incident report
2.3	HIC Privacy Officer triages the reported incident, and determines if the incident involves any other participating organizations/HICs. • If incident involves other HICs, then the HIC sends the incident report to the HINP. (Ref 2.7) • If incident involves only the local HIC, then the HIC initiates the internal incident management process. (Ref 2.4) *The HIC has to inform the HINP within 24 hours of receiving the Incident Report if the incident is determined to affect other HICs in accordance with the Data Sharing Agreement*	Health Information Custodians	
2.4	HIC sends Incident Report to HINP	Health Information Custodians	Incident Report
2.5	HINP creates incident in the Incident Registry and notifies the most responsible HIC about the incident.	Health Information Network Provider	Incident report
2.6	The most responsible HIC initiates internal processes to handle the reported/detected incident.	Health Information Custodians	
2.7	HIC executes the internal incident handling processes and documents the incident.	Health Information Custodians	
2.8	HIC sends the incident resolution detail to the HINP.	Health Information	Updated incident

		Custodians	report
2.9	HINP creates or updates Incident Registry with details of incident resolution.	Health Information Network Provider	Incident Registry
2.10	HIC initiates internal processes to document and handle the incident.	Health Information Custodians	
2.11*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach of his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in developing the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Scenario 3 – Incident Reported by the HINP


Integrated Incident Management Processes – 3.0
Detection
Escalation
Incident Handling
Reporting
Client
Most responsible HIC
HINP
End
3.10 Client(s) receives notification of breach from HIC
3.7 HIC initiates internal incident handling process
3.8 Internal processes to document and handle incident
3.9 Sends incident resolution to HINP
3.2 Creates Incident Record in Incident Registry
3.6 HINP notifies the most responsible HIC
Yes
3.4 Internal processes to handle Incident
3.5 Updates incident resolution in Incident Registry
3.1 Incident is detected by or reported to HINP
3.3 Does incident involve other HIC(s)?
No
End
Start

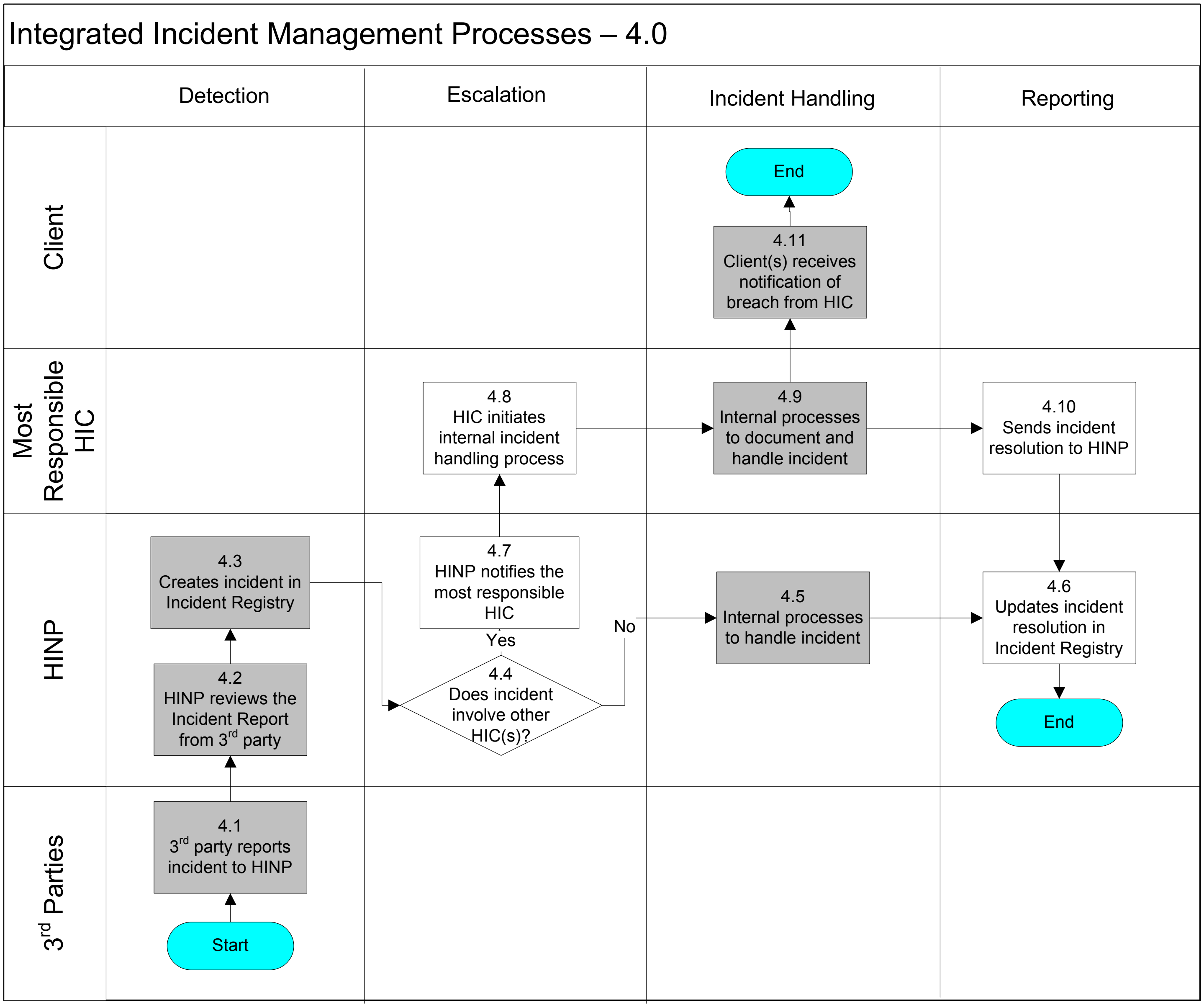
*Note: *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 3 **Incident detected by HINP** Sample scenarios: • IAR backup data unaccounted for (lost or stolen) • IAR database was hacked into by hackers • Large amount of IAR records were accessed by a single individual in a short period of time (duration out of the ordinary) • Missing data backup tape contains server and systems information only (no PHI)		
3.1	The incident is detected by the normal incident detection and monitoring process at the HINP, or staff at HINP reported incident internally to HINP privacy officer.	Health Information Network Provider	Incident Report
3.2	HINP keeps track of incidents by creating a record in the Incident Registry.	Health Information Network Provider	Incident Registry
3.3	HINP Privacy Officer triages the reported/detected incident, and determines if the incident involves other participating organizations/HICs. • If incident involves other HICs, then the privacy officer notifies the most responsible HIC. (Ref 3.6) • If incident involves only the HINP, then the privacy officer initiates the internal incident management process. (Ref 3.4) *The HINP has to inform the affected HIC within 24 hours of receiving the Incident Report in accordance with the Data Sharing Agreement.*	Health Information Network Provider	
3.4	HINP executes internal processes to handle the reported/detected incident.	Health Information Network Provider	
3.5	HINP updates Incident Registry with details of incident resolution.	Health Information Network Provider	Incident Registry
3.6	HINP notifies the most responsible HIC about the incident. If applicable, the HINP continues to investigate and contain the incident, and provides all supporting information to assist the internal incident handling at the HIC.	Health Information Network Provider	Incident Report

3.7	The most responsible HIC initiates the internal incident handling process.	Health Information Custodians	
3.8	The HIC executes internal processes to document and handle the reported/detected incident.	Health Information Custodians	
3.9	The HIC sends incident resolution details to the HINP.	Health Information Custodians	Updated incident report
3.10*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach of his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Scenario 4 – Incident Reported by 3rd Party to HINP


Integrated Incident Management Processes – 4.0
Detection
Escalation
Incident Handling
Reporting
Client
Most Responsible HIC
HINP
3rd Parties
Start
4.1 3rd party reports incident to HINP
4.2 HINP reviews the Incident Report from 3rd party
4.3 Creates incident in Incident Registry
4.4 Does incident involve other HIC(s)?
Yes
No
4.7 HINP notifies the most responsible HIC
4.8 HIC initiates internal incident handling process
4.9 Internal processes to document and handle incident
4.11 Client(s) receives notification of breach from HIC
End
4.5 Internal processes to handle incident
4.10 Sends incident resolution to HINP
4.6 Updates incident resolution in Incident Registry
End

*Note: *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 4 **Incident reported by 3rd party of HINP** Sample scenarios: • Record management service provider reports to HINP that one IAR backup data tape went missing during transit • Missing data backup tape contains server and systems information only (with no PHI)		
4.1	3rd party reports incident to HINP.	Health Information Network Provider	Incident report form
4.2	HINP Privacy Officer reviews the received Incident Report from 3rd party.	Health Information Network Provider	
4.3	HINP creates incident in incident registry.	Health Information Network Provider	Incident Registry
4.4	HINP Privacy Officer triages the reported incident, and determines if the incident involves other participating organizations/HICs. • If incident involves other HICs, then the HINP privacy officer notifies the most responsible HIC about the incident. (Ref 4.7) • If incident involves only the HINP, then the HINP initiates the internal incident management process. (Ref 4.5) *The HINP has to inform the other affected HICs within 24 hours of receiving the Incident Report if the incident is determined to affect other HICs in accordance with the Data Sharing Agreement*	Health Information Network Provider	
4.5	HINP initiates internal processes to handle the reported incident.	Health Information Network Provider	
4.6	HINP updates the incident resolution detail in the Incident Registry.	Health Information Network Provider	Incident Registry
4.7	HINP notifies the most responsible HIC.	Health Information Network Provider	Incident report

4.8	The most responsible HIC initiates internal processes to handle the reported/detected incident.	Health Information Custodians	
4.9	The HIC executes the internal processes to document and handle the incident.	Health Information Custodians	
4.10	The HIC sends the incident resolution detail to the HINP.	Health Information Custodians	Updated incident report
4.11*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach of his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Appendix A – Incident Report Template for HIC

Integrated Assessment Record (IAR) System
Incident Report

Fax No:

1. Contact Information *To be completed by the individual submitting this report*

First Name	Last Name	Date (dd/mm/yyyy)
Email	Organization	
Phone No.	Title / Position	
Address (street, city, province, postal code)		

2. Incident Description *Describe the incident below.*

Date of Incident (dd/mm/yyyy)	Involves PHI?	Reported By
Description / Details		
		Date of Incident (dd/mm/yyyy)

3. Incident Management

Incident #	Internal Reference #
Assigned to	Incident Receipt Date (dd/mm/yyyy)
Containment Action	
Follow-up Action	Most Responsible (Primary) Organization
Follow-up Date (dd/mm/yyyy)	Other Organizations (if any)
Resolution Status	
Resolution Date (dd/mm/yyyy)	
Notes	

Appendix B – Incident Update Report Template for HIC

Integrated Assessment Record (IAR) System **Incident Update** **Fax No:**		
1. Contact Information *To be completed by the individual submitting this update*		
First Name	Last Name	Date (dd/mm/yyyy)
Email	Organization	
Phone No.	Title / Position	
2. Incident Information		
Incident #	Internal Reference #	
Client Contacted?	Date of Contact	
Update		
Notes		

Appendix C - IAR Centralized Incident Registry Template

Incident #	Reported By	Incident Date (dd/mm/yyyy)	Most Responsible (Primary) Org	Secondary Orgs	PHI Involved? (Y/N)	Actions Taken	Action Dates (dd/mm/yyyy)	Is client notified of incident? (Y/N)	Incident Resolution Status	Incident Resolution Dates (dd/mm/yyyy)
ABCD-1234	John Smith	13/05/2010	HIC A	HIC C HIC W HIC Z		Notified Secondary Orgs			Rejected/Resolved/Arbitration	

Incident Management Process Implementation Work Sheet

Ref. No.	Integration Point	Analysis	As is Process	To be Process	Actions
2.1	**Incident is detected or reported to HIC *(Example)***	Do client, staff and 3rd parties know who to report incident to? What information channel can be used to publish how the incident can be reported? Is there any existing incident reporting process?	Staff normally report abnormality to their manager. Clients report to the clinicians or case managers. Uncertain about 3rd parties. IT Managers sometimes receive email regarding potential incidents.	Unifies incident reporting inbox, phone number and physical office location. Incident reporting form to be available on company web site.	• Work with corporate web team to develop content. • Work with HR to include incident reporting steps in new employee training program.
2.1	**Incident is detected or reported to the HIC**	Do client, staff and 3rd parties know who to report incident to? What information channel can be used to publish how incident can be reported? Is there any existing incident reporting process?			
2.2	**Does the incident involve other HICs?**	Privacy Officer is to develop simple mechanism to investigate or search IAR if breach or incident involves other participating organizations.			
2.3	**Internal process to handle the incident.**	Review current incident handling process to see if there are any gaps. Review the process for notifying clients.			
2.4	**Send incident report to the HINP.**	Ensure the HINP Privacy Officer contact number and email address is handy and accessible. Have an electronic copy of the incident report handy for use.			

2.8	**Send incident resolution to the HINP.**	Keep the electronic incident update report template handy for use.			
3.1	**Client or 3rd party reports incident to the HIC.**	Does the client or 3rd party know who they should be reporting an incident to if they discover one?			
3.2	**HIC reviews the incident report from the client or 3rd party.**	Develop a checklist of things to look for in an incident report. Prepare to interview (talk to) the person who reported the incident for more details.			

Integrated Consent Management Process

Integrated Assessment Record

Version 4.0

January 2016

CCIM

Community
Care
Information
Management

ACCESS TO INFORMATION

Table of Contents

Introduction

Consent is a critical component of all health care systems. There are two primary options available to health care organizations: implied and express consent. For the purposes of this project, implied consent is the baseline, while organizations are free to practice express consent if they so choose. Whatever the choice, the starting point for documenting this process is that the consent must be **informed** (i.e., informing the client of what information is being collected from them, why that information is required, to whom that information may be disclosed, how to check the accuracy of their information and how to address their complaints).

IAR Consent Model

IAR supports two levels of consent directive: HSP-level (also Known as Assessment level) consent directive and IAR-level consent directive.

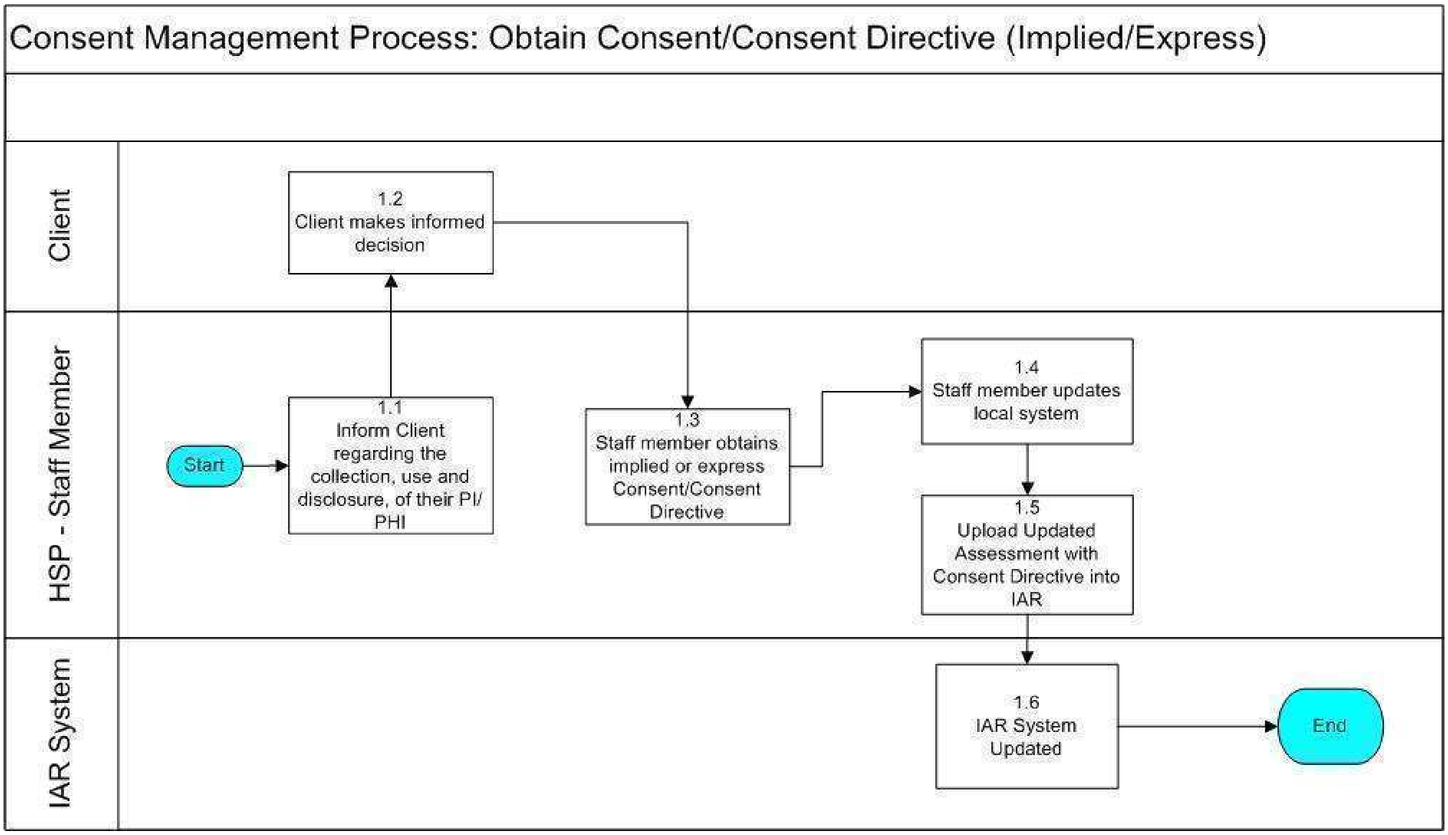
- For the HSP-level consent directive, IAR will inherit the consent flag submitted along with individual assessment and automatically enforce the consent directive in IAR. If the source tool does not support the consent flag, the HSP's Privacy officer will need to login to the IAR HSP consent interface to register the consent directive manually. Only the assessments from the HSP will be affected.
- For the IAR-level consent directive, the client will need to contact the Consent Call Centre to register the consent directive in IAR, which will hide all assessments (across HSPs) relating to the client in IAR.

The more restrictive consent directive (either HSP-level or IAR-level) will take precedence.

The IAR consent model does not provide the ability to override the consent directive feature. Therefore IAR viewers/users cannot override any consent restrictions. The ability to override the consent directive feature will be implemented in a future release of IAR.

1. Consent Management Process

1.1 Consent Management Process: Obtain Consent/ Consent Directive



Consent Management Process: Obtain Consent/Consent Directive (Implied/Express)
Client
HSP - Staff Member
IAR System
Start
1.1 Inform Client regarding the collection, use and disclosure, of their PI/ PHI
1.2 Client makes informed decision
1.3 Staff member obtains implied or express Consent/Consent Directive
1.4 Staff member updates local system
1.5 Upload Updated Assessment with Consent Directive into IAR
1.6 IAR System Updated
End

Table 1: Obtain Consent/ Consent Directive (Implied or Express)

No.	Task / Step	Responsible Person	Supporting Material
1.1	Prior to conducting the assessment, the staff informs client regarding the collection, use and disclosure of their PI/PHI and the client's privacy rights.	Staff Members	Brochure, Poster, Consent Communication Script
1.2	Client makes an informed decision (either to consent or to withhold their consent) initiating a consent directive	Client	
1.3	HSP Staff Member obtains implied or express consent (or consent directive) according to existing HSP consent process	Staff Members	Consent Form Template
1.4	Staff members update local system with the consent directive received according to existing consent process (this should be done as soon as is practical).	Staff Members	
1.5	The assessment with consent directive is uploaded to IAR System		
1.6	The IAR System is updated with the current consent directive	Staff Members	Consent Directive registry template (sect

1.2 Consent Management Process: Update Consent Directive (Withdraw/Reinstate)

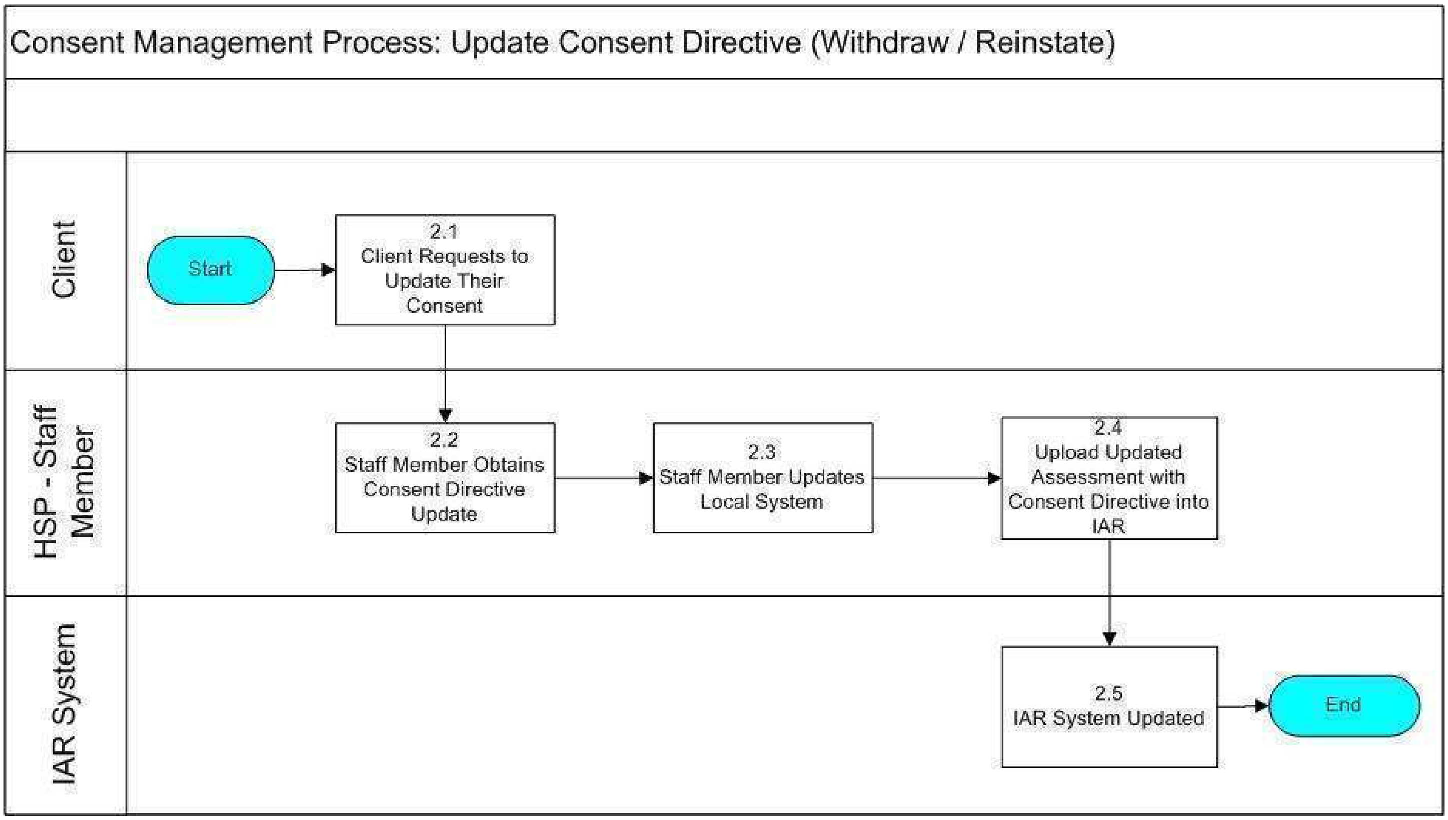

Consent Management Process: Update Consent Directive (Withdraw / Reinstate)
Client
HSP - Staff Member
IAR System
Start
2.1 Client Requests to Update Their Consent
2.2 Staff Member Obtains Consent Directive Update
2.3 Staff Member Updates Local System
2.4 Upload Updated Assessment with Consent Directive into IAR
2.5 IAR System Updated
End

Table 2: Update Consent Directive (Implied or Express)

No.	Task / Step	Responsible Person	Supporting Material
2.1	Client requests to update their consent directive (withdraw or reinstate)	Client	
2.2	Staff obtains verbal or written consent or consent directive according to existing HSP consent process.	Staff Members	Consent Form template
2.3	Staff members update local system with the consent directive received according to existing consent process (this should be done as soon as is practical).	Staff Members	
2..4	The assessment with updated consent directive is uploaded to IAR System		
2.5	The IAR System is updated with the current consent directive		

2. IAR Consent Administration Process

A client can place a call to the centralized Consent Call Centre via a toll free number to register their IAR consent directive. A consent directive to share one's assessment in IAR means all of the client's assessments across HSPs will be shared with participating HSPs that provide care to the client. A consent directive to **not** share assessments, or withdrawal of a previously provided consent directive to share in IAR, means all of the client's assessments in the IAR — both past and any that will be uploaded in the future — will be locked and no participating HSPs will be able to view them.

Apart from the capability to deny sharing Assessment, IAR level consent directive also allows the client to Deny access to their PI, which would mean that IAR users will not be able to search the client in IAR, to an IAR user it would appear as if the client or its assessment do not exist in IAR.

The more restrictive consent directive (either HSP-level or IAR-level) will always be enforced. This means that:

- If the HSP-level consent directive restricts sharing, then the assessment will not be visible through IAR even if the IAR-level consent directive allows sharing.
- Even if the HSP-level consent directive allows sharing, if the IAR-level consent directive is set to restrict sharing, then the assessment will not be visible to any HSP until the IAR-level consent directive is updated to allow sharing of assessments.

Therefore, the client needs to understand that once they call the Consent Call Centre and provide a consent directive to not share assessments — even if they subsequently give consent to share to an HSP — the assessment will not be visible until they call the Consent Call Centre again and update their consent directive to enable sharing.

There are certain scenarios in which a client may seek assistance from the HSP in providing their consent directive to the Consent Call Centre:

1. Client needs help with calling the Consent Call Centre
2. Client does not have enough information to identify themselves
3. Client has a substitute decision maker, and the substitute decision maker wants to provide a consent directive on their behalf

Scenario #1: Client is not comfortable calling the Consent Call Centre by himself/herself

If the client does not feel comfortable calling the Consent Call Centre or speaking with the Consent Call Centre alone, the client can request the clinician or case workers to help place the call to the Consent Call Centre. If the client needs assistance from the clinician or the case worker to navigate through the process during the encounter with the Consent Call Centre customer service representative (CSR), the clinician may help the client by repeating the message from the CSR or explaining what information is required of the client.

Some basic identifying information about the clinician or case worker will be asked by the CSR in order to identify the client and link their consent directive to the correct assessments in IAR.

The client will still need to provide the consent to the Consent Call Centre themselves.

Scenario #2: Client does not have enough information to identify themselves
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; and the Consent Call Centre CSR will request the assistance of the clinician or case worker to help verify the identity of the client.

The CSR will ask the clinician or case worker for information in order to validate the identity of the clinician or case worker as an authorized person from the HSP.

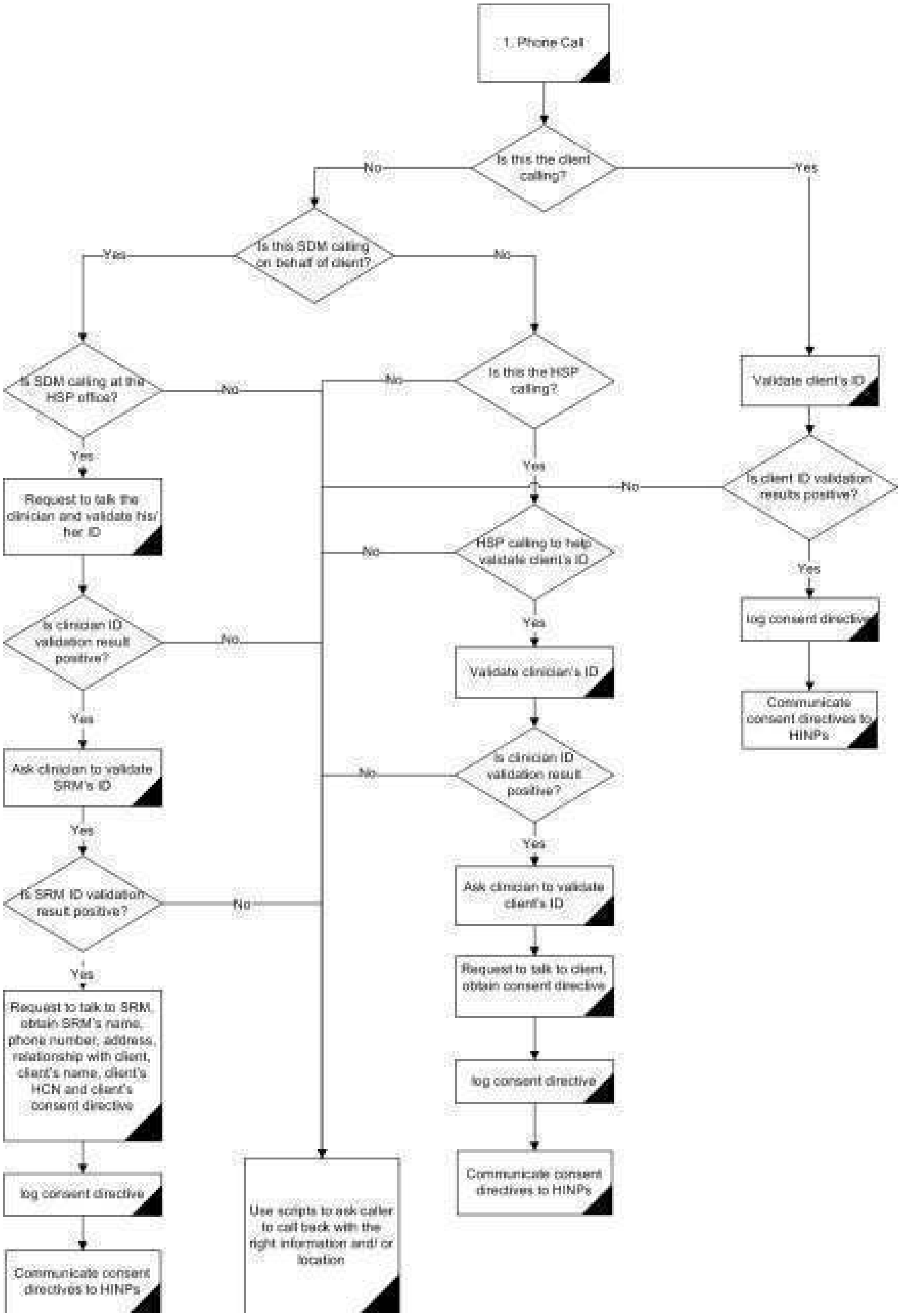
Once the identity of the client is verified through the clinician or case workers, the client will continue the encounter with the Consent Call Centre, and provide his/her consent directive to the CSR.

Scenario #3: Client has a substitute decision maker, and the substitute decision maker wants to provide a consent directive on their behalf
If the client has a substitute decision maker (SDM) who will provide the consent directive on their behalf, the SDM is required to place the call to the Consent Call Centre from an HSP, and the Consent Call Centre CSR will request the assistance of the clinician or case worker to help verify the identity of the SDM.

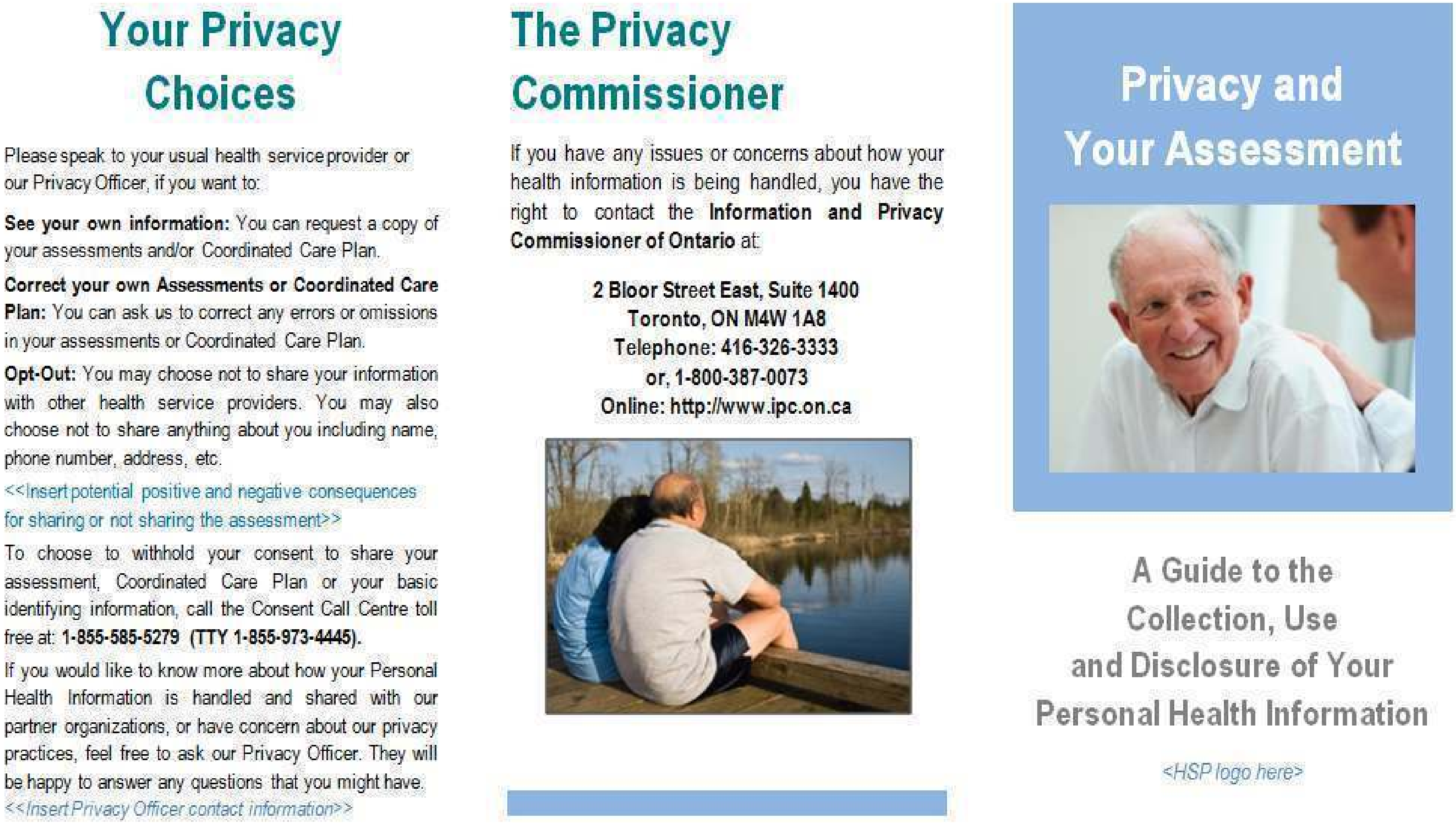
The CSR will ask the clinician or case worker for information in order to validate the clinician or case worker as an authorized person from the HSP.

Once the identity of the SDM is verified through the clinician or case workers, the SDM will continue the encounter with the Consent Call Centre, and provide the client's consent directive to the CSR.

The following is a process flow diagram of the above scenarios:


1. Phone Call
Is this the client calling?
No
Yes
Is this SDM calling on behalf of client?
Yes
No
Is SDM calling at the HSP office?
No
Is this the HSP calling?
No
Validate client's ID
Yes
Request to talk the clinician and validate his/ her ID
Yes
No
Is client ID validation results positive?
HSP calling to help validate client's ID
No
Yes
log consent directive
Is clinician ID validation result positive?
No
Yes
Validate clinician's ID
Communicate consent directives to HINPs
Yes
Ask clinician to validate SRM's ID
No
Is clinician ID validation result positive?
Yes
Yes
Is SRM ID validation result positive?
No
Ask clinician to validate client's ID
Yes
Request to talk to client, obtain consent directive
Request to talk to SRM, obtain SRM's name, phone number, address, relationship with client, client's name, client's HCN and client's consent directive
log consent directive
log consent directive
Communicate consent directives to HINPs
Use scripts to ask caller to call back with the right information and/ or location
Communicate consent directives to HINPs

Appendix A – Brochure



Your Privacy Choices

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

See your own information: You can request a copy of your assessments and/or Coordinated Care Plan.

Correct your own Assessments or Coordinated Care Plan: You can ask us to correct any errors or omissions in your assessments or Coordinated Care Plan.

Opt-Out: You may choose not to share your information with other health service providers. You may also choose not to share anything about you including name, phone number, address, etc.

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

To choose to withhold your consent to share your assessment, Coordinated Care Plan or your basic identifying information, call the 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, or have concern about our privacy practices, 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 Disclosure of Your Personal Health Information

<HSP logo here>

Your Personal Health Information

We use your personal health information (PHI) to provide you with health services. That information is used and sometimes shared with your other providers to determine your health service and support needs and may also be used to coordinate care planning.

Your assessments and Coordinated Care Plan may include information on:

- Your physical and mental health
- Your personal and health history
- <<insert other information that your HSP may collect or use >>

Unless you tell us not to, your personal health information will be shared with other organizations that are providing you with health services, both now and in the future. Sharing assessments, including Coordinated Care Plans, gives health service providers in your community the most complete and up-to-date information about you. Holistic health care depends on a holistic view of your health data to identify and serve your needs.

Sharing your information

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 Personal Health Information, the information in your assessment and Coordinated Care Plan will be used to:

- Provide health support and services based on your needs
- Make sure your health service providers have the most up-to-date and complete record of your health history and needs
- Help us understand your care goals and to provide the services you need
- Make sure everyone is getting the right support and services

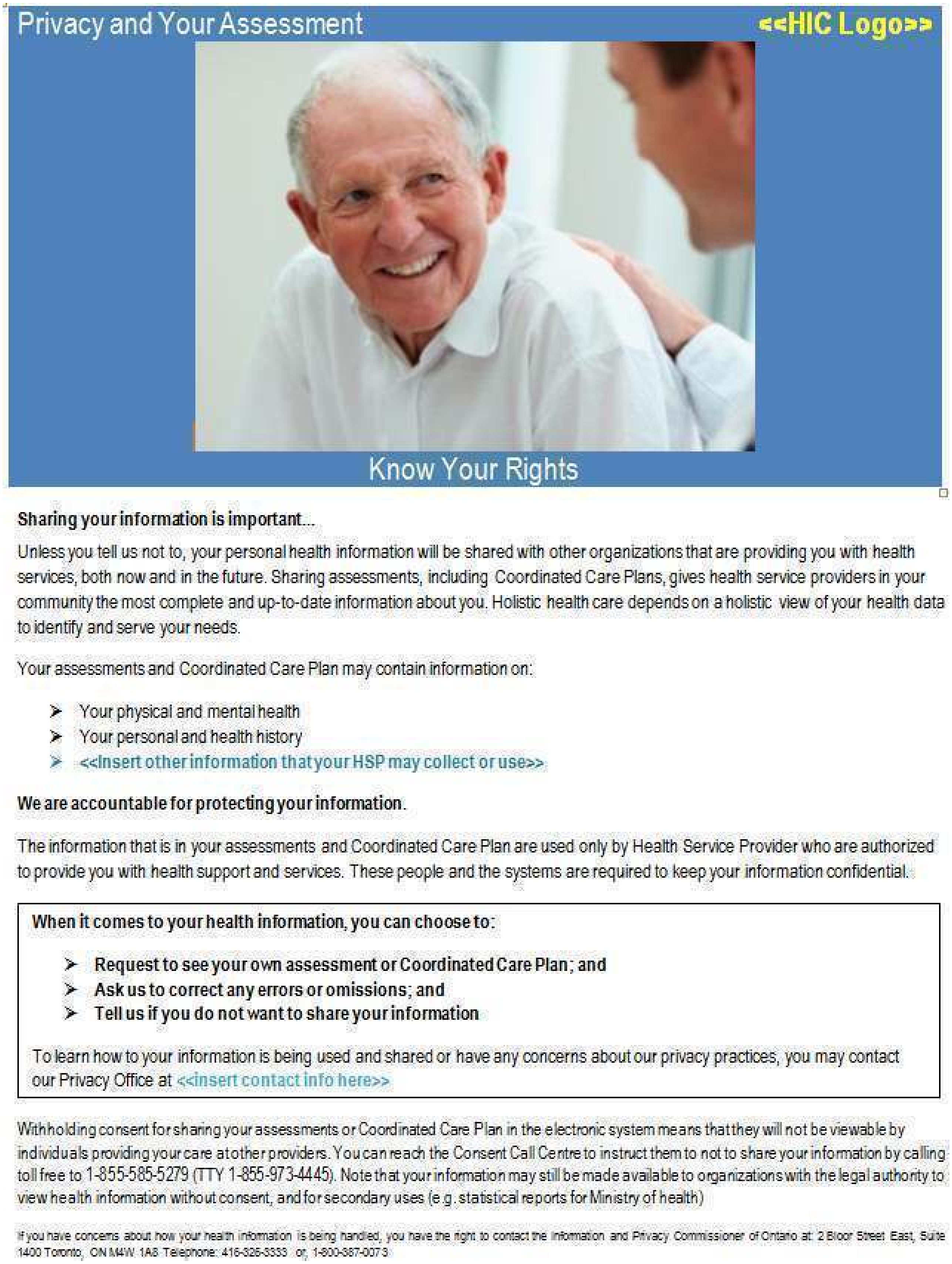
Protecting Your Information

The information in your assessments and Coordinated Care Plan is your information. Our priority is protecting your privacy while delivering high quality care. In the assessment and coordinated care processes, we only collect the information we need to determine your service and support needs. This information cannot be used for any other purposes without your permission unless required by law[1].

- Your health information is kept in a secure place
- Your health information will only be viewed by people we have authorized.
- All health information custodians have confidential legal obligation to protect your privacy.
- When a person views your information, it is recorded in a log. We will review this log regularly to make sure there has been no unauthorized access to your information.
- We will investigate any suspected breach or unauthorized access to, or use of, your Personal Health Information
- Your health information may be used for secondary purposes as authorized by law (e.g. statistical reports for Ministry of Health)

[1] For example, the College of Physicians and Surgeons may need access to information to validate the quality of care you receive from a physician.

Appendix B – Poster



Privacy and Your Assessment

<<HIC Logo>>

Know Your Rights

Sharing your information is important...

Unless you tell us not to, your personal health information will be shared with other organizations that are providing you with health services, both now and in the future. Sharing assessments, including Coordinated Care Plans, gives health service providers in your community the most complete and up-to-date information about you. Holistic health care depends on a holistic view of your health data to identify and serve your needs.

Your assessments and Coordinated Care Plan may contain information on:

- Your physical and mental health
- Your personal and health history
- **<<Insert other information that your HSP may collect or use>>**

We are accountable for protecting your information.

The information that is in your assessments and Coordinated Care Plan are used only by Health Service Provider who are authorized to provide you with health support and services. These people and the systems are required to keep your information confidential.

When it comes to your health information, you can choose to:

- **Request to see your own assessment or Coordinated Care Plan; and**
- **Ask us to correct any errors or omissions; and**
- **Tell us if you do not want to share your information**

To learn how to your information is being used and shared or have any concerns about our privacy practices, you may contact our Privacy Office at **<<insert contact info here>>**

Withholding consent for sharing your assessments or Coordinated Care Plan in the electronic system means that they will not be viewable by individuals providing your care at other providers. You can reach the Consent Call Centre to instruct them to not to share your information by calling toll free to 1-855-585-5279 (TTY 1-855-973-4445). Note that your information may still be made available to organizations with the legal authority to view health information without consent, and for secondary uses (e.g. statistical reports for Ministry of health)

If you have 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

Appendix C – Sample Communication Script for Authorized Users

General Privacy and Consent Communication Sample Script

If your system does not have a way of recoding client/patient consent, you may print this document out and complete it as a form to record consent.

Do not use this with clients/patients until you have reviewed and updated it to match your particular circumstances. The use of << brackets >> indicates text that you must adapt to your HSP.

At a minimum, point #1 and #2 should be covered with the clients/patients either with this script or by a poster/brochure.

1. -The Collection, Use and Disclosure (Sharing) of <<Client/Patient's Assessments and/or Coordinated Care Plans>>: What we collect and why we need it

We would like to complete an **<<Assessment Type or Coordinated Care Plan>>** for you. The **<<Assessment Type or Coordinated Care Plan>>** will include information about you, such as your medical conditions, your goals and other information about you that will help your care team to coordinate and provide care to you.

We collect, use and disclose your personal health information in order to provide you with services, to coordinate your care planning with others and to support those that do provide you with services. We will also use your information for a variety of secondary purposes such as quality control, generating reports required by the Ministry of Health or other purposes that are allowed by law.

The client has heard and understood what we collect and why we need it: □

2. Sharing of Client/Patient's Coordinated Care Plans – what client/patient's consent means

If you give us your consent to share your information, only those health care workers who have been authorized by their organization for this purpose will see your **<<Assessment Type or Coordinated Care Plan>>.** Your **<<Assessment Type or Coordinated Care Plan>>** information will be stored in a security electronic system and will be used by health care workers providing you with service so you don't have to repeat yourself and so that they will have important information about you. Do you give us your consent to share your information?

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

- **<<Positive and negative consequences for sharing the Assessment Type or Coordinated Care Plan>>**

If you choose to withhold your consent and not share your Assessment Type or Coordinated Care Plan, this may mean:

- **<<Positive and negative consequences for not sharing the Assessment Type or Coordinated Care Plan>>**

The client has heard and understood what their consent means: □

3. Future Consent

Would you like to maintain this consent for the future? If you do, this means that each time your **<<Assessment Type or Coordinated Care Plan>>** is updated, the consent that you provide today will automatically be applied to those updates and we will not ask you these consent questions each time your Coordinated Care Plan is updated, otherwise, we will ask you for your consent each time the **<<Assessment Type or Coordinated Care Plan>>** is updated.

The client has agreed to future consent for this assessment: □

(If the client/patient gives consent, skip to #5. If the client/patient wants to withdraw consent, please go to point #4a)

4. Consent Withdrawal Options

a) **HSP specific withdrawal of consent --** If you do not want to share this **<<Assessment Types or Coordinated Care Plans>>** information with other health care workers, you can let me know today or inform our staff anytime in the future, and we will make sure the **<<Assessment Types or Coordinated Care Plans>>** will not be shared. Do you consent to sharing this **<<Assessment Types or Coordinated Care Plans>>** ?

Consent Granted: □ **Consent Denied:** □

Do you have concerns about sharing other **<<Assessment Types or Coordinated Care Plans>>** that have been completed before now? If client/patient is concerned about all of their Coordinated Care Plans in the secure electronic system go on to point #4b. If not, go to #5.

b) **IAR Consent Directive** – Would you want all of your **<<Assessment Types or Coordinated Care Plans>>** *blocked* -- Or do you want none of your **<<Assessment Types or Coordinated Care Plans>** information shared, even the **<<Assessment Types or Coordinated Care Plans>** information gathered at other Health Service Providers? You can call the Consent Call Centre at 1-855-585-5279 during regular business office hours. This will ensure that no one will be able to access any of your **<<Assessment Types or Coordinated Care Plans>**. Only your basic identifying information, like name, phone number and city will be there. This basic identifying information is used in the event that you change your mind and decide to share your **<<Assessment Types or Coordinated Care Plans>** in the future. Your health service provider will be able to find you as well as your shared Coordinated Care Plans. Is this okay with you?

The client/patient wishes to apply an IAR level consent directive: □ **(Leave blank for no)**

If client/patient is concerned about having basic identifying information (i.e. name, phone number, city, date of birth, gender, etc.) in the IAR, go on to #4c. Otherwise go to #5.

c) **IAR Consent Directive with basic identifying information blocked –** If you do not want to share your basic identifying information, like name, phone number and city, you can have that blocked by calling the Consent Call Centre at 1-855-585-5279 during regular business office hours. By telling them that you do not want to share your personal information; your identifying information will not be visible.

The client/patient also wishes to suppress personal information: □ (Leave blank for no)

For any IAR Level Consent Directive add: We call this instruction a Consent Directive. It will take effect in **<<# number of business days>>** after you inform the Consent Call Centre that you want your assessment/personal information blocked.

The client/patient needs assistance calling the Consent Call Centre: □ (Leave blank for no)

5. Your Privacy Rights

You can request a copy of your **<<Assessment Type or Coordinated Care Plan>>** information in your file by contacting us. You also have the right to request a correction or amendment to your **<<Assessment Type or Coordinated Care Plan>>** information, or log a complaint if you feel that we have not addressed your privacy concerns properly. You should know that you will need to identify yourself to the Privacy Officer (or designated staff) in order to make privacy related requests. You may need to provide the following information **<<Identification Information>>.**

6. Need More Information or Have Questions?

If you would like to know more about how your Personal Health Information is handled and shared with other Health Service Providers or have concerns about your privacy, you can contact the Privacy Officer at **<<HSP name>>**. They will help you understand what it means to share your assessments and/or Coordinated Care Plan and will be able to answer your questions. Please contact our designated Privacy contact at **<<Privacy Contact Information>>**

Name and/or ID of the client patient:	
Name of the person obtaining the consent:	
Date that the consent was obtained:	

Appendix D – Consent Directive Form Template

<<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 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 *not* apply to the copies of my assessments that other HSPs have already received.**
□ **Yes, I consent**	□ **No, I don't consent**	**To the sharing of** all my previous and future 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 not 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) ______________________

Relationship ______________________ ______________________

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: (###) ###-####.

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

<<Contact Information / Website>>

Appendix E – Consent Directive Log Template

HINP Ref. No.	Organization Name	Client/Patient Name and #	Consent Directive Requested	Received By	Received Date	Registered by	Registration Date
H201001	*HSP 1*	*John Smith 54321*	*Lock all assessment and PI Data*	*David Jones*	*13/01/2016*	*Jane Doe*	*15/01/2016*

Consent Management Process

Recording, Registering and Updating Consent Worksheet

	Record	Register	Update
Where ?			
When ?			
Who ?			

Integrated Client Privacy Rights Supporting Process

Integrated Assessment Record (IAR)

Version 4.0

January 2016

CCIM Community Care Information Management

ACCESS TO INFORMATION

Table of Contents

Introduction

Under the Personal Health Information Protection Act, individuals have certain rights to their health care records. Specifically, they have a right to:

1. **Access their record –** Sections 52 through 54 state that an individual has a "right of access" to their record of personal health information. These sections also state that the Health Information Custodian (HIC) must provide a response within 30 days. If the individual believes that the Health Information Custodian has refused or is thought to have refused the request, they have the right to file a complaint with the Privacy Commissioner.
2. **Change/correct information within their record –** Section 55 states that an individual may request that the custodian correct their record, if the individual believes the record is inaccurate or incomplete. In this case as well, the custodian must grant or refuse the request within 30 days. If the individual believes that the Health Information Custodian has refused or is thought to have refused the request, they have the right to file a complaint with the Privacy Commissioner.
3. **File a complaint with the Privacy Commissioner regarding an organization's privacy practices –** Section 56 of PHIPA states that an individual has the right to file a complaint with the Privacy Commissioner if they have "reasonable grounds" to believe that someone has contravened or is about to contravene a provision of the Act. Applying this right to these circumstances, an individual has the right to file a complaint if they believe that the Health Information Custodian has sub-standard privacy practices or they have failed in some way to protect their privacy.
4. **Be notified of a change to an assessment record initiated by the HIC –** This process describes the steps required when the Health Information Custodian initiates a change to a client's assessment record. PHIPA does not require the HIC to notify the client of change in their Personal Health Information. However, the HIC may choose to notify the client if the changed information may have an effect on the provision of care to the client, or if notification of changes is required by other applicable health care legislations.

This document translates these client rights into defined processes and steps as they relate to the Integrated Assessment Record (IAR). It identifies responsibilities and delineates between those tasks which should already be in place within any given Health Information Custodian and those tasks which are introduced with the IAR.

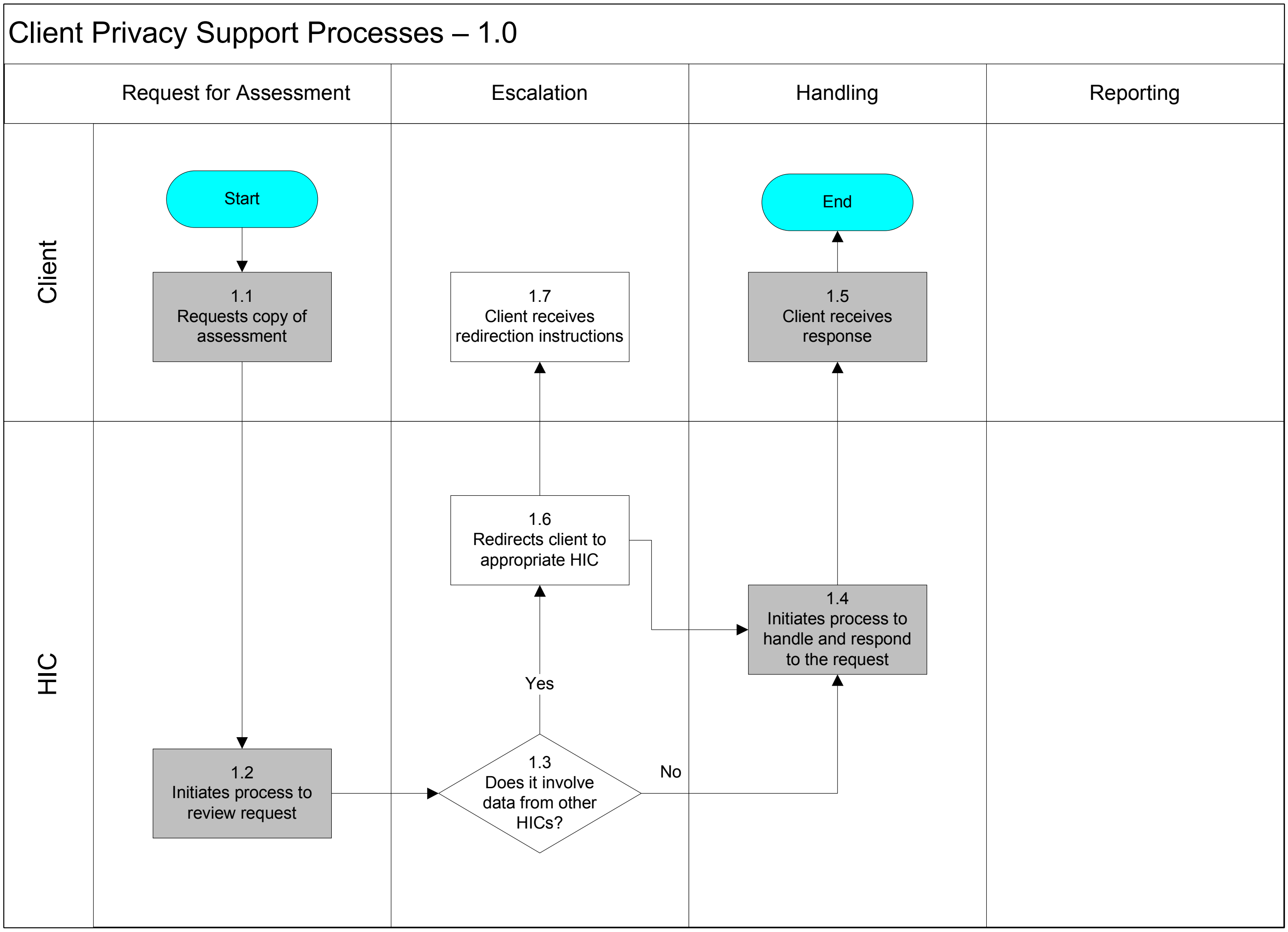
If the request to access or change the assessment, or the complaint relates solely to information in the custody or control of a single HIC, local processes are leveraged. If the request to access or change the assessment involves other HICs, the HIC identifies the other involved HICs for the client to contact and make their request separately.

The HINP will only participate and coordinate the privacy complaint management process. If the complaint involves more than one HIC, the HINP facilitates and communicates among the multiple HICs to respond to the client complaint.

IAR privacy complaints are recorded in a centralized Privacy Complaint Registry by the HINP privacy officer.

Processes

Client Request for Assessment Record

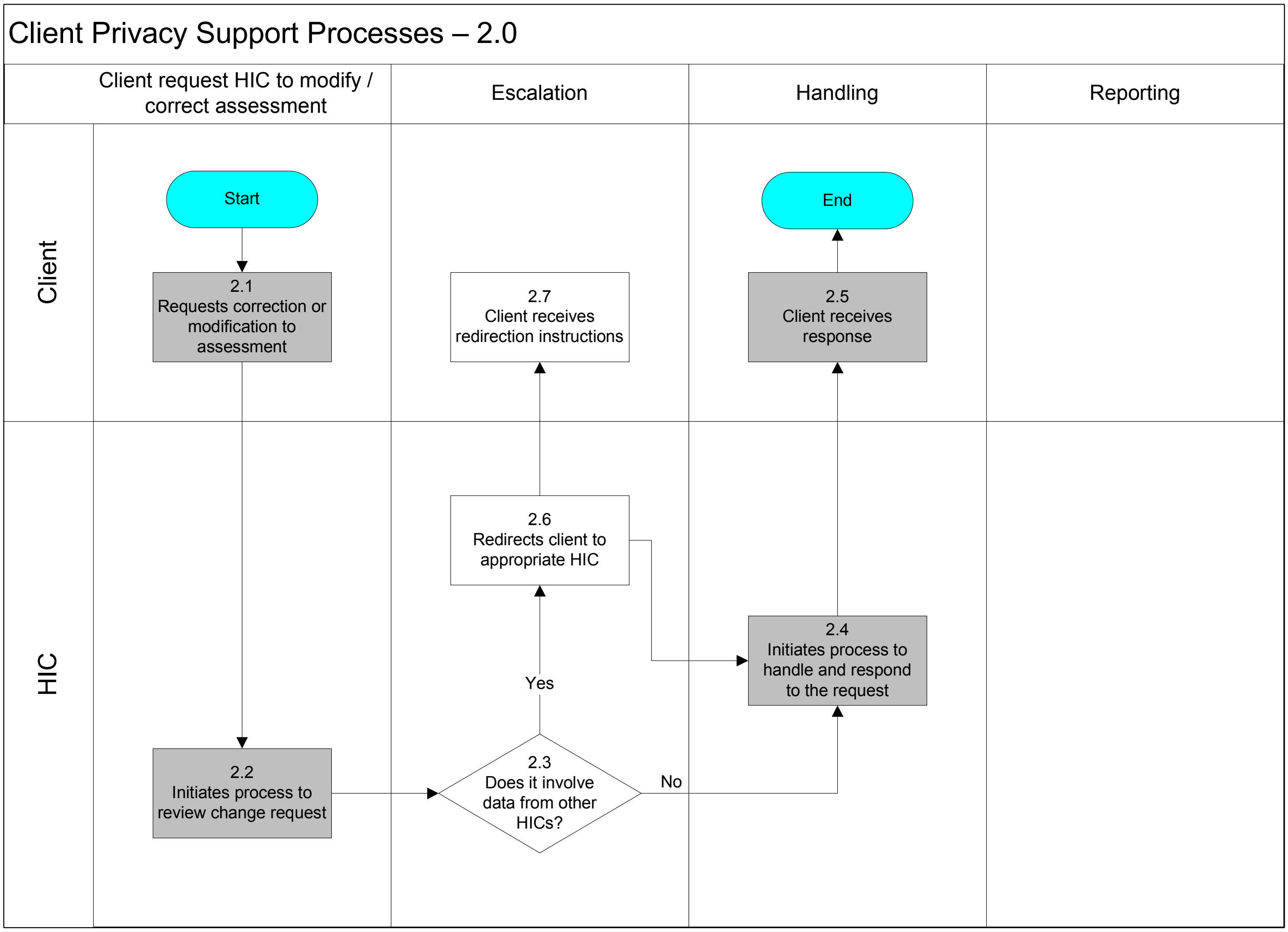

Client Privacy Support Processes – 1.0
Request for Assessment
Escalation
Handling
Reporting
Client
HIC
Start
1.1 Requests copy of assessment
1.7 Client receives redirection instructions
End
1.5 Client receives response
1.6 Redirects client to appropriate HIC
1.4 Initiates process to handle and respond to the request
Yes
1.2 Initiates process to review request
1.3 Does it involve data from other HICs?
No

Note:

- *Grey shaded boxes indicate steps which should currently exist within the Health Information Custodian and Health Information Network Provider*
- *Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR*

Ref No.	Task / Step	Owner	Artifacts
1.1	Request copy of assessment from HIC	Client	Client Request Form
1.2	Initiate process to review the request for a copy of assessment	HIC	
1.3	Determine whether the request for an assessment involves data under the custody or control of any other HICs. If the request does involve data under the custody or control of another HIC, then the process goes to step 1.6. Otherwise the process ends. Handle and respond to the request for a copy of assessment	HIC	
1.4	Initiate internal process to handle and response to the client's request	HIC	
1.5	The client receives the response	Client	
1.6	Re-direct the request - If the client's request involves data under the custody or control of another HIC, the client needs to be redirected to the appropriate body that can respond (Each HIC is only able to release information that is under their custody or control)	HIC	Client Request Response Form
1.7	The client receives the redirection instructions	Client	

Client Request to Modify/Correct Assessment Information

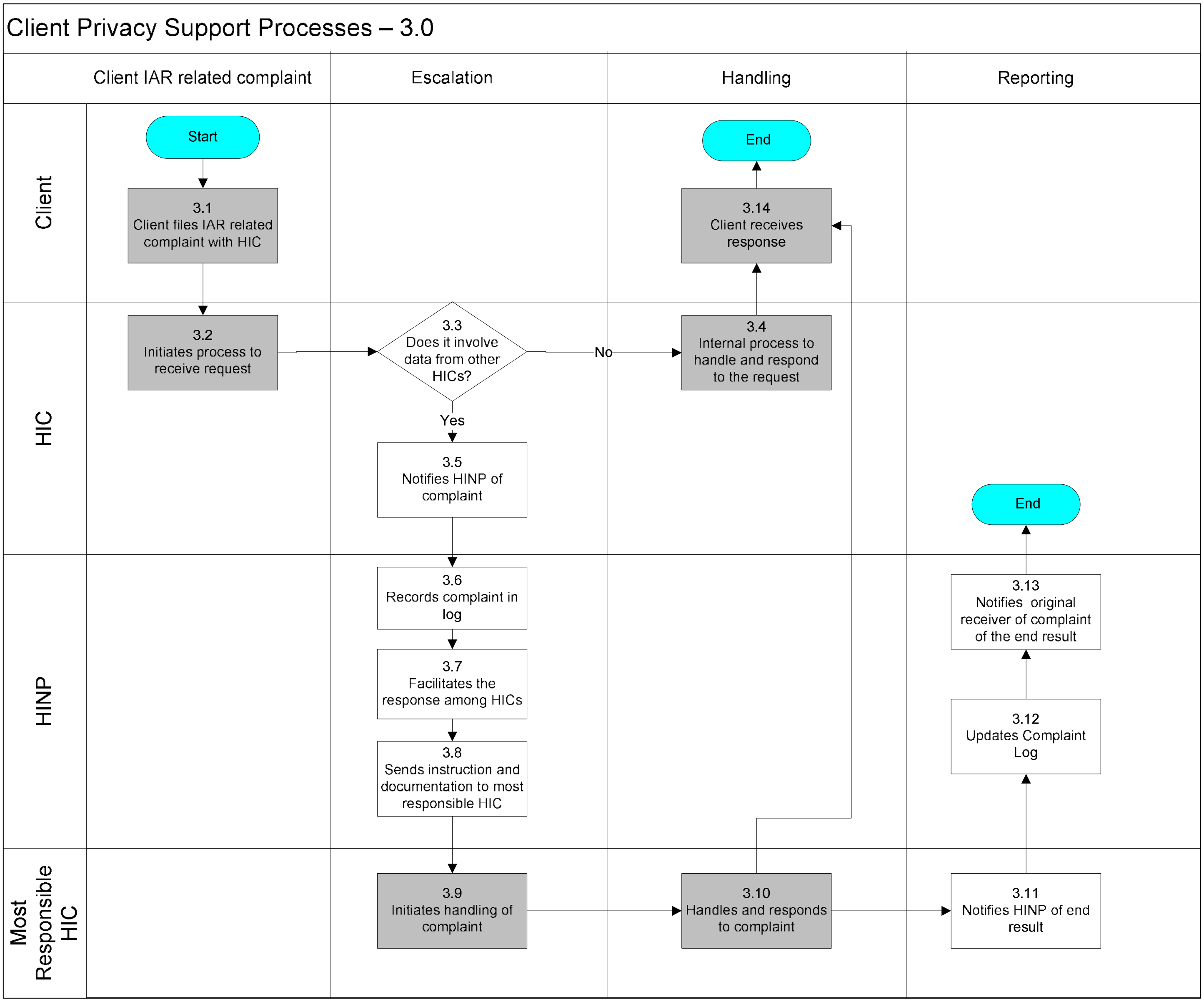

Client Privacy Support Processes – 2.0
Client request HIC to modify / correct assessment
Escalation
Handling
Reporting
Client
HIC
Start
2.1 Requests correction or modification to assessment
2.2 Initiates process to review change request
2.3 Does it involve data from other HICs?
Yes
No
2.6 Redirects client to appropriate HIC
2.7 Client receives redirection instructions
2.4 Initiates process to handle and respond to the request
2.5 Client receives response
End

Note:

- *Grey shaded boxes indicate steps which should currently exist within the Health Information Custodian and Health Information Network Provider*
- *Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR*

Ref No.	Task / Step	Owner	Artifacts
2.1	Request a modification or correction to their assessment information	Client	Client Request Form
2.2	Initiate process to review the modification or correction request	HIC	
2.3	Determine whether the request involves data under the custody or control of any other HICs. If it does, then the process goes to step 2.6. otherwise the process ends.	HIC	
2.4	Initiate internal process to handle and respond to the request for modification or correction to the assessment information	HIC	
2.5	The client receives the response from the HIC	Client	
2.6	Re-direct the request - If the Client's request involves data under the custody or control of another HIC, the client needs to be redirected to the appropriate body that can respond to them (Each HIC is only able to change information that is under their custody or control)	HIC	Client Request Response Form
2.7	The client receives the redirection instructions	Client	

Client Complaint about Privacy Practices


Client Privacy Support Processes – 3.0
Client IAR related complaint
Escalation
Handling
Reporting
Client
HIC
HINP
Most Responsible HIC
Start
3.1 Client files IAR related complaint with HIC
3.2 Initiates process to receive request
3.3 Does it involve data from other HICs?
No
Yes
3.4 Internal process to handle and respond to the request
3.5 Notifies HINP of complaint
3.6 Records complaint in log
3.7 Facilitates the response among HICs
3.8 Sends instruction and documentation to most responsible HIC
3.9 Initiates handling of complaint
3.10 Handles and responds to complaint
3.11 Notifies HINP of end result
3.12 Updates Complaint Log
3.13 Notifies original receiver of complaint of the end result
End
3.14 Client receives response
End

Note:

- *Grey shaded boxes indicate steps which should currently exist within the Health Information Custodian and Health Information Network Provider.*
- *Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
3.1	Files IAR related complaint with the HIC	Client	Complaint Form
3.2	Initiate process to receive the complaint form	HIC	
3.3	Decide whether the complaint involves other HICs. If so, then the HINP needs to be notified and this process continues with 3.5. If the complaint is specific to the HIC that received it, internal handling and response steps take place as identified in 3.4.	HIC	
3.4	Internal process to handle and respond to the complaint	HIC	
3.5	Notify HINP of the complaint within 2 business days, as it relates to IAR and other HICs	HIC	
3.6	Record complaint in Complaint Registry	HINP	Complaint Registry
3.7	The HINP facilitates among the different HICs that are involved in the client complaint to determine the most appropriate response to the client, including determining the most responsible HIC	HINP	
3.8	Send applicable instruction and documentation to the most responsible HIC	HINP	
3.9	Initiate the process of handling and responding to the complaint	HIC	
3.10	The most responsible HIC handles and responds to the complaint	HIC	
3.11	The most responsible HIC notifies the HINP of the end result of the complaint	HIC	Complaint Report
3.12	The HINP updates the Complaint Registry	HINP	Complaint Registry
3.13	The HINP notifies the original HIC with the results of the complaint	HINP	
3.14	Client receives the response	Client	

Appendix A – Client Request Form Template

Integrated Assessment Record (IAR) System
Patient Privacy Rights Request Form

1. Requester Information *To be completed by the requester*

First Name	Last Name	Initial
Date of Birth (dd/mm/yyyy)	Email	
Phone No.	Alternate Phone No.	
Street Address (street, city, province, zip)		

2. Request Description *Describe the assessment information that you want to access. Include the type of assessment, and the date (of range of date) of the assessments*

3. Purpose of Use

I understand that my personal information will be used for the purposes of locating the assessment information I request.

Signature_______________________________ Date (dd/mm/yyyy) ______________

For Internal Use Only

Request #	Request Reception Date (dd/mm/yyyy)
Request completed Date (dd/mm/yyyy)	Other Organizations (if any)
Person handled the request	
Status	
Notes	

Appendix B – Client Request Response Form Template

Integrated Assessment Record (IAR) System
Patient Privacy Rights
Client Request Response Form

[Enter Date]

Dear [Enter Requestor's Name],

Thank you for your request for your assessment data. We have provided you with the assessments that were conducted here.

However, your request also includes assessments stored by the following health service provider organizations:

Organization Name	Organization Address	Contact Name	Phone No.	Email Address

Please use the information provided above to contact the privacy officers of these additional health service provider organizations to obtain your assessment collected by them.

Sincerely,

[Insert your Name]
Privacy Officer

Appendix C – Patient Privacy Right Complaint Form Template

Integrated Assessment Record (IAR) System
Patient Privacy Rights Complaint Form

1. Complainant Information *To be completed by the complainant*

First Name	Last Name	Initial
Date of Birth (dd/mm/yyyy)	Email	
Phone No.	Alternate Phone No.	
Street Address (street, city, province, zip)		

2. Complaint Description *In your own words, provide the details of your complaint, the names of any individuals or healthcare organizations involved if you know them, and the date when it happened. Attach additional pages if more space is needed.*

Date of Occurrence (dd/mm/yyyy)

3. Purpose of Use

I understand that my personal information will be used for the purposes of resolving my complaint.

Signature_______________________________ Date (dd/mm/yyyy) ________________

For Internal Use Only

Complaint #	Complaint Reception Date (dd/mm/yyyy)
Follow-up Action	Most Responsible (Primary) Organization
Follow-up Date (dd/mm/yyyy)	Other Organizations (if any)
Resolution Status	
Resolution Date (dd/mm/yyyy)	
Notes	

Appendix D – Patient Privacy Right Complaint Report

Integrated Assessment Record (IAR) System
Patient Privacy Rights Complaint Report

Complaint Number:		
Complainant & Complaint Information		
First Name	Last Name	Initial
Complaint Date (dd/mm/yyyy)	Resolution Due Date (dd/mm/yyyy)	
Most Responsible (Primary) Organization	Secondary Organization(s)	
Action Taken	**Action Dates (dd/mm/yyyy)**	
Complaint Resolution Status (Rejected/Resolved/Arbitration)	**Complaint Resolution Date (dd/mm/yyyy)**	
Notes		

Appendix E – Client Privacy Right Complaint Registry

Complaint #	Complainant Name	Complaint Date (dd/mm/yyyy)	Resolution Due Date (dd/mm/yyyy)	Most Responsible (Primary) Org	Secondary Orgs	Actions Taken	Action Dates (dd/mm/yyyy)	Complaint Resolution Status	Complaint Resolution Dates (dd/mm/yyyy)
QXY-1234	John Smith	13/01/2016	13/01/2016	HIC A	HIC C HIC W HIC Z	Notified Secondary Orgs		Rejected/Resolved/Arbitration	

Client Privacy Right Support Process Implementation Work Sheet

Ref. No.	Integration Point	Analysis	As is Process	To be Process	Actions
1.3, 2.3	**Does the request involve data from other HICs?**	Based on the client request, use the IAR to determine whether the request by client actually involves other HSPs (i.e., data from multiple organizations/HICs).			
1.5, 2.5	**Does a process and template exist to provide Response to the client**	Create a standard response form for replying to the user request			
1.6, 2.6	**Redirect the client to appropriate HSPs.**	Keep a contact list of Privacy Officers from other involved HSPs handy. Keep the response form template handy and available for use.			
1.4, 2,4, 3.4	**Initiate the process to handle and respond to the request.**	Review the current process and determine whether there is any gap in responding to the client's request for their PHI.			

Ref. No.	Integration Point	Analysis	As is Process	To be Process	Actions
3.2	**Initiate the process to receive request/compliant.**	Review whether there are any gaps in existing process to receive client's complaint. Do staff members know if they receive a privacy complaint who they should be directing that complaint to?			
3.3	**Involve other HICs?**	Determine from the client complaint whether the complaint involves other HSP(s) besides yours.			
3.5	**Notify the HINP PO of complaint.**	Keep HINP Privacy Officer contact number and email address handy. Have a cover email template handy to forward complaint to HINP Privacy Officer.			

User Account Management Process

Integrated Assessment Record (IAR)

Version 4.0

January 2016

CCIM Community Care Information Management

ACCESS TO INFORMATION

Table of Contents

Introduction

The IAR User Account Management process creates, modifies and removes user accounts for the participating organizations in the IAR environment. It is a centralized process handled by the CCIM Support Desk and the HINP.

As IAR system matures several role have been identified and grouped as Business Sustainment Roles There roles are as follows:

1. User authority Role
2. User Coordinator Role
3. Privacy Officer
4. EMPI Lead (also Known as Data Quality Lead)
5. Technical Lead / Webservice Contact.

The Users associated with Business Sustainment Roles Can be added, their information updated or removed from the role using the IAR Business Sustainment Roles Form. Add (create), change or remove account requests have to be authorized by the User Authority for all roles except the User Authority role. Add (create), change or remove account requests for User Authority (UA) role has to be authorized by the Privacy Officer (PO). A copy of the IAR Business Sustainment Roles Form is appended to the document as Appendix C.

Each participating organization designates a person to authorize user access to IAR, called the User Authority (UA). The UA approves all new user account creation in IAR for their respective organizations by signing off on the IAR HSP and User Access Form. A copy of the IAR HSP and User Access Form is appended to the document as Appendix B.

Each user is required to read and accept the IAR User Agreement before access is granted. The IAR User Agreement is an agreement between the user and the participating organization. A copy of the IAR User Agreement can be found in the appendix A of this document. Participating organizations should review the user agreement template and modify it accordingly to reflect the organization's name and other references.

The Privacy Officer is expected to be the primary contact for resolving issues arising related to privacy and client (patient) rights. PO is responsible to review Privacy and Security Logs and Reports on a scheduled basis. And therefore need an account in the IAR system with privacy offer permissions.

The Web Services UPLOADER Account is used for auto upload of assessments to IAR. The Technical lead is responsible for the Web Services Uploader account and therefore is required to read and accept the IAR User Agreement before access is granted. The WebService User account addition, change and deletion follow the same process as any other IAR user. The UA has to approve the Web Services Uploader Account request by signing on the IAR HSP and User Access Form.

For each participating organization, there is a designated contact person, called the User Coordinator (UC) for liaising day-to-day user account management activities with the CCIM Support Desk and the HINP User Account Management team (e.g., user account modification and removal). User account management artifacts and templates are included in the appendix of this document.

Each Participating organization are also required to designate a Data Quality Lead also known as EMPI lead. The EMPI lead is responsible for resolving Client (Patient) demographic issues within the EMPI.

The IAR application provides user with the capability to change personal passwords or reset a forgotten password; if the online password change or reset does not work, users can request password reset through the IAR help desk. A password reset process is included in this document.

Because the IAR on boarding has been completed and no new organizations are getting on board to IAR, the process for the initial one-time bulk creation or conversion of user accounts to IAR is not included in this document.

The Privacy officer of all participating organizations can generate the list of active users as well as users not logged in for 90 days. Privacy officers should review and validate these accounts on a frequent basis to confirm the continued validity of these user accounts in their respective organizations.

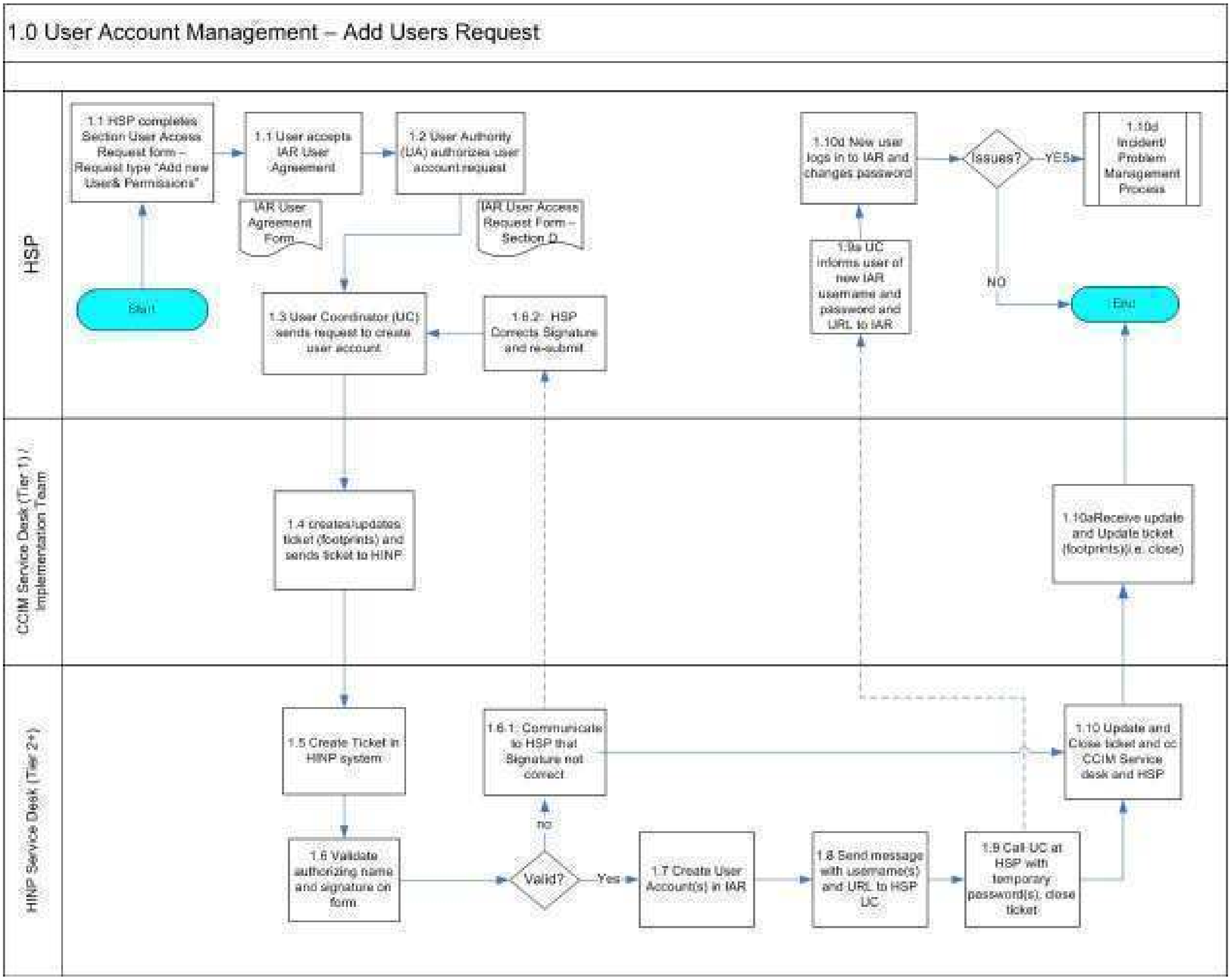
The following process map and process description is developed to illustrate the following three scenarios:
Scenario 1 – Creation of new user accounts
Scenario 2 – Modification of existing user accounts
Scenario 3 – Removal of existing user accounts
Scenario 4 – Password Reset and /or User Account Reactivation
Scenario 5 – Create (or Add) All Business Sustainment Role Users (Except User Authority)
Scenario 6 – Create User Authority Role User
Scenario 7 – Update All Business Sustainment Role (Except User Authority)
Scenario 8 – Update (or Change) User Authority Role User
Scenario 9 – Remove All Business Sustainment Role (Except User Authority)
Scenario 10 – Remove User Authority Role User

All of the Completed User Account Management request forms should be faxed to the CCIM Support Desk at **(416) 314-1585.** Or PDF version of the forms can be sent using email with the approval signatures to IAR@CCIM.ON.CA. Forms without an approval signature will not be processed.

The latest versions of all User Account Management forms can be found on the CCIM portal.

Processes

Scenario 1 – Creation of New User Accounts

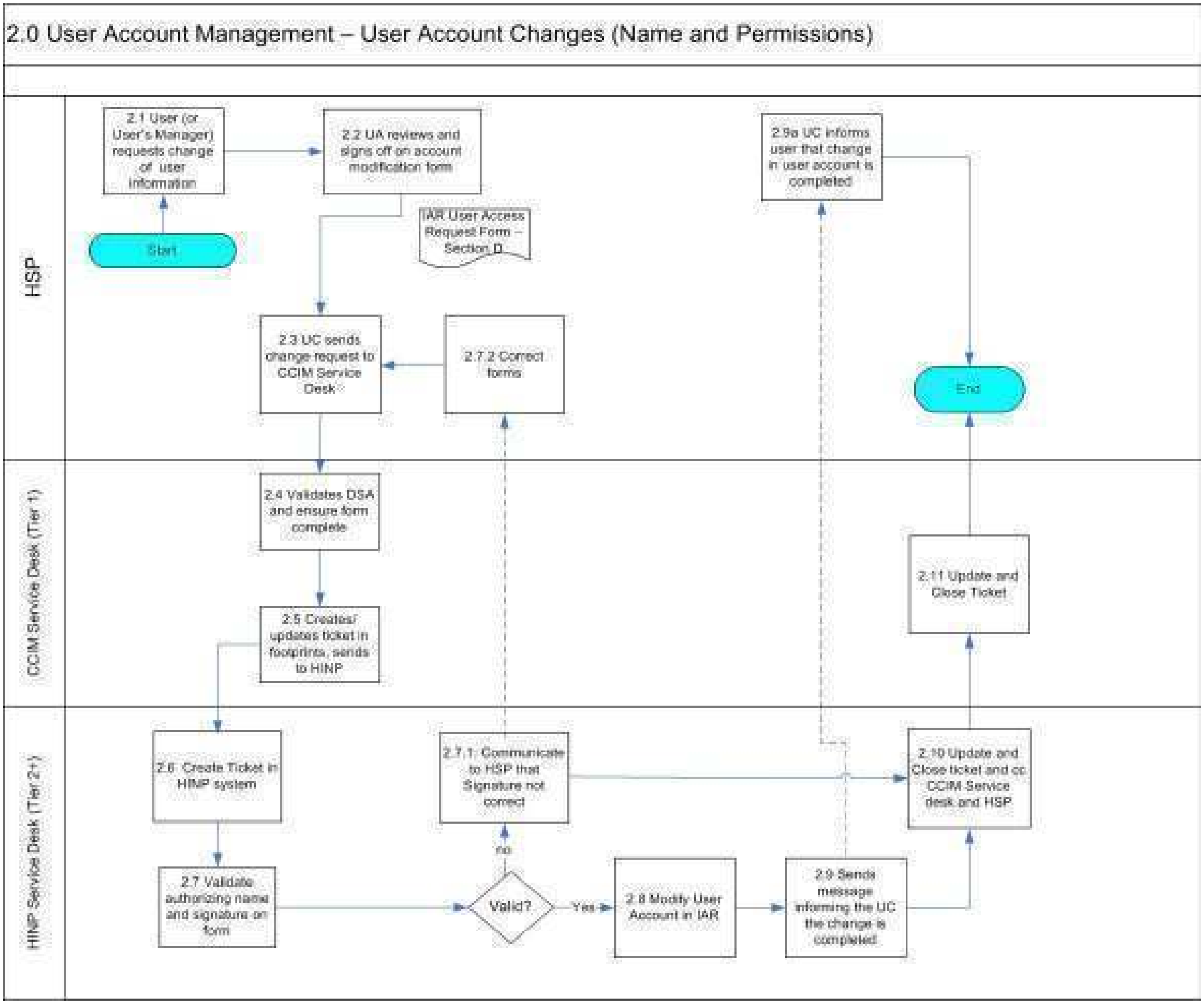

1.0 User Account Management – Add Users Request
HSP
CCIM Service Desk (Tier 1) / Implementation Team
HINP Service Desk (Tier 2+)
Start
1.1 HSP completes Section User Access Request form – Request type "Add new User& Permissions"
1.1 User accepts IAR User Agreement
IAR User Agreement Form
1.2 User Authority (UA) authorizes user account request
IAR User Access Request Form – Section D
1.3 User Coordinator (UC) sends request to create user account
1.6.2: HSP Corrects Signature and re-submit
1.4 creates/updates ticket (footprints) and sends ticket to HINP
1.5 Create Ticket in HINP system
1.6 Validate authorizing name and signature on form
Valid?
no
Yes
1.6.1: Communicate to HSP that Signature not correct
1.7 Create User Account(s) in IAR
1.8 Send message with username(s) and URL to HSP UC
1.9 Call UC at HSP with temporary password(s); close ticket
1.10 Update and Close ticket and cc CCIM Service desk and HSP
1.10aReceive update and Update ticket (footprints)(i.e. close)
1.9a UC informs user of new IAR username and password and URL to IAR
1.10d New user logs in to IAR and changes password
Issues?
YES
NO
1.10d Incident/ Problem Management Process
End

Ref No.	Task / Step	Owner	Artifacts
	User Account Management Process – Creation of new user • Each new user account must be authorized by the User Authority of the respective organization. The User Authority (UA) is a designated person in the participating organization that approves creation of new user accounts in IAR. • Each new user is required to read and accept the IAR User Agreement. • The User Coordinator (UC) is a designated user account contact in the participating organization for day-to-day user account management activities (i.e. modification and removal), and interacts with the centralized User Account Management team.		
1.1	The user's manager completes the User Account Request form with the required user details. If a Web Services Uploader Account is required The person Responsible for the account (Technical Lead) should complete the form	Health Service Providers	IAR HSP and User Access Form
1.2	The user reads and accepts the IAR User Agreement. If the request is for a Web Service Uploader account, the person responsible for the Web Services Uploader Account is required to read and accept the IAR User Agreement.	Health Service Providers	IAR User Agreement IAR HSP and User Access Form
1.3	The User Authority (UA) checks the user Agreement to ensure the user has read and signed it, then authorizes the user access to IAR by signing the User Account Request form and acknowledging the user has read and signed the IAR User Agreement. If a Web Services Uploader account is requested, the UA must ensure that the Technical Lead responsible for the account has read and signed has read and signed the IAR User Agreement.	Health Service Providers	IAR HSP and User Access Form IAR User Agreement
1.4	The User Coordinator (UC) sends the User Account Request form to IAR Support Center located at CCIM.	Health Service Providers	
1.5	The IAR Support Centre reviews the User Account Request form, ensures that the HSP is IAR participant, raises a ticket, and assigns it to the HINP.		
1.6	The HINP User Account Management Team reviews and validates the HSP User Authority If the signature are fine please skip the next two steps and move to	HINP	

	step 1.7		
1.6.1	If the HINP if not satisfied that the Signature on the form belongs to the User authority it has on the record for the organization, HINP would inform the HSP. And close the ticket	HINP	
1.6.2	HSP corrects the form and gets the correct signatures and resubmit the form via a new ticket.	HSP	
1.7	The HINP User Account Management Team Creates the User account in the IAR system	HINP	
1.8	The HINP User Account Management Team sends the newly created IAR username and the URL for the application to the HSP User Coordinator	HINP	
1.9	A member of the HINP User Account Management Team calls the User Coordinator with the password	HINP	
1.9a	The User Coordinator informs the user of the newly created IAR username and password	HSP	
1.9b	The new user logs on to IAR, and changes their password to a new and unique password. The initial user password expires upon user's first logon.	HSP	
1.9c	If there is a problem with the user login or password the HSP will initiate the IAR Integrated Incident management process	HSP	
1.10	The HINP User Account Management Team updates and closes the ticket.	HINP	
1.10a	The IAR Support Centre updates and closes the ticket.	IAR Support Centre	

The privacy officer needs to be appropriately informed of the user account management process (i.e., new user account creation, modification and removal).

Scenario 2 – Update of Existing User Accounts


2.0 User Account Management – User Account Changes (Name and Permissions)
HSP
CCIM Service Desk (Tier 1)
HINP Service Desk (Tier 2+)
2.1 User (or User's Manager) requests change of user information
Start
2.2 UA reviews and signs off on account modification form
IAR User Access Request Form – Section D
2.9a UC informs user that change in user account is completed
2.3 UC sends change request to CCIM Service Desk
2.7.2 Correct forms
End
2.4 Validates DSA and ensure form complete
2.5 Creates/ updates ticket in footprints, sends to HINP
2.11 Update and Close Ticket
2.6 Create Ticket in HINP system
2.7.1: Communicate to HSP that Signature not correct
2.10 Update and Close ticket and cc CCIM Service desk and HSP
no
2.7 Validate authorizing name and signature on form
Valid?
Yes
2.8 Modify User Account in IAR
2.9 Sends message informing the UC the change is completed

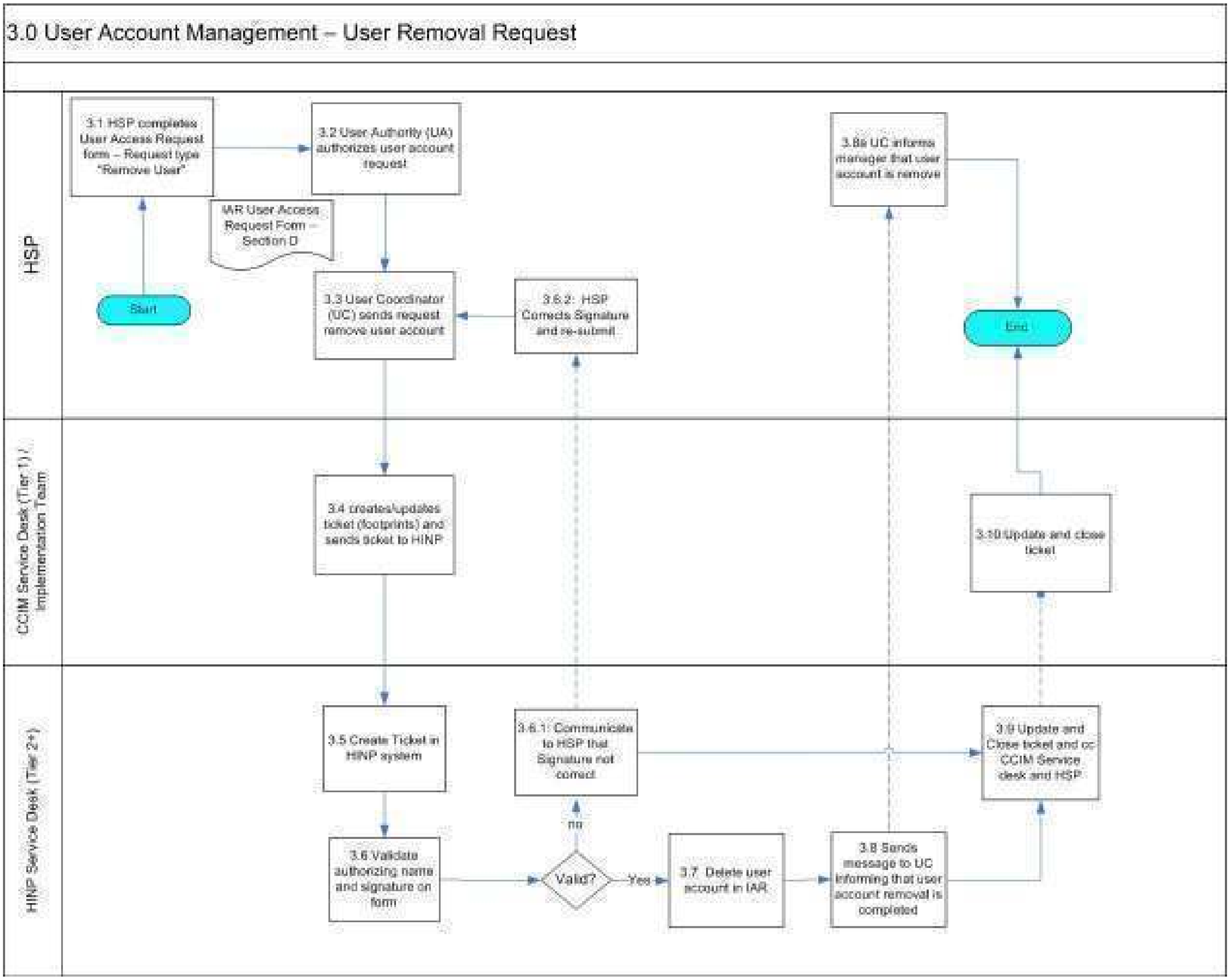
Note: *Forgotten passwords can be reset by the user via the IAR user interface or through the IAR Reset process described elsewhere in this document* Change of password for Uploader account can also be carried out via this process

Ref No.	Task / Step	Owner	Artifacts
	User Account Management Process – Modification of user details, such as: • Change of information such as email address, contact phone numbers, etc. • Changes in permission (e.g. Viewer to Uploader)		
2.1	The user or user's manager completes the IAR User Access Form with the "Change User Information and/or Permissions" checkbox checked in Section D and passes it to the User Authority (UA).	Health Service Providers	IAR HSP and User Access Form
2.2	The User authority at the HSP reviews and signs the IAR User Access Form, authorizing the changes and pass it to the UC at the HSP	Health Service Providers	IAR HSP and User Access Form
2.3	The UC forwards the form to IAR support desk at CCIM.	Health Service Providers	IAR HSP and User Access Form
2.4	IAR support desk validates the HSP is IAR participant by checking the DSA and checks the submitted form is complete	Health Service Providers	IAR HSP and User Access Form
2.5	The IAR Support Center raises a ticket, and forward the Account change request to appropriate HINP	IAR Support Centre	IAR HSP and User Access Form
2.6	The HINP User Account Management Team receives the account change request and creates a ticket in their system	HINP	IAR HSP and User Access Form
2.7	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no. 2.8 otherwise proceed to step no. 2.7.1	HINP	
2.7.1	If the signature is not verified the HINP User Account Management Team informs the HSP accordingly and closes the ticket	HINP	
2.7.2	The HSP Then corrects the signatures on the form and resubmits the request	HSP	
2.8	After the HSP Authorizing signature have been verified the HINP User Account Management Team modifies the user account according to the details provided on the User Account Change form,(including permission changes as requested)	HINP	
2.9	The HINP User Account Management Team sends the information to the UC that the updates have been completed.	HINP	
2.9a	The User Coordinator informs the user (or the user's manager) that the	HSP	

	change requested for the user account is complete		
2.10	The HINP User Account Management Team updates and closes the Ticket as well CC the CCIM desk that the ticket ticket.	HINP	
2.11	The IAR Support Centre updates and closes the ticket.	IAR Support Centre	

Note: The privacy officer needs to be appropriately informed of the user account management process (i.e., new user account creation, modification and removal).

Scenario 3 – Removal of User Accounts

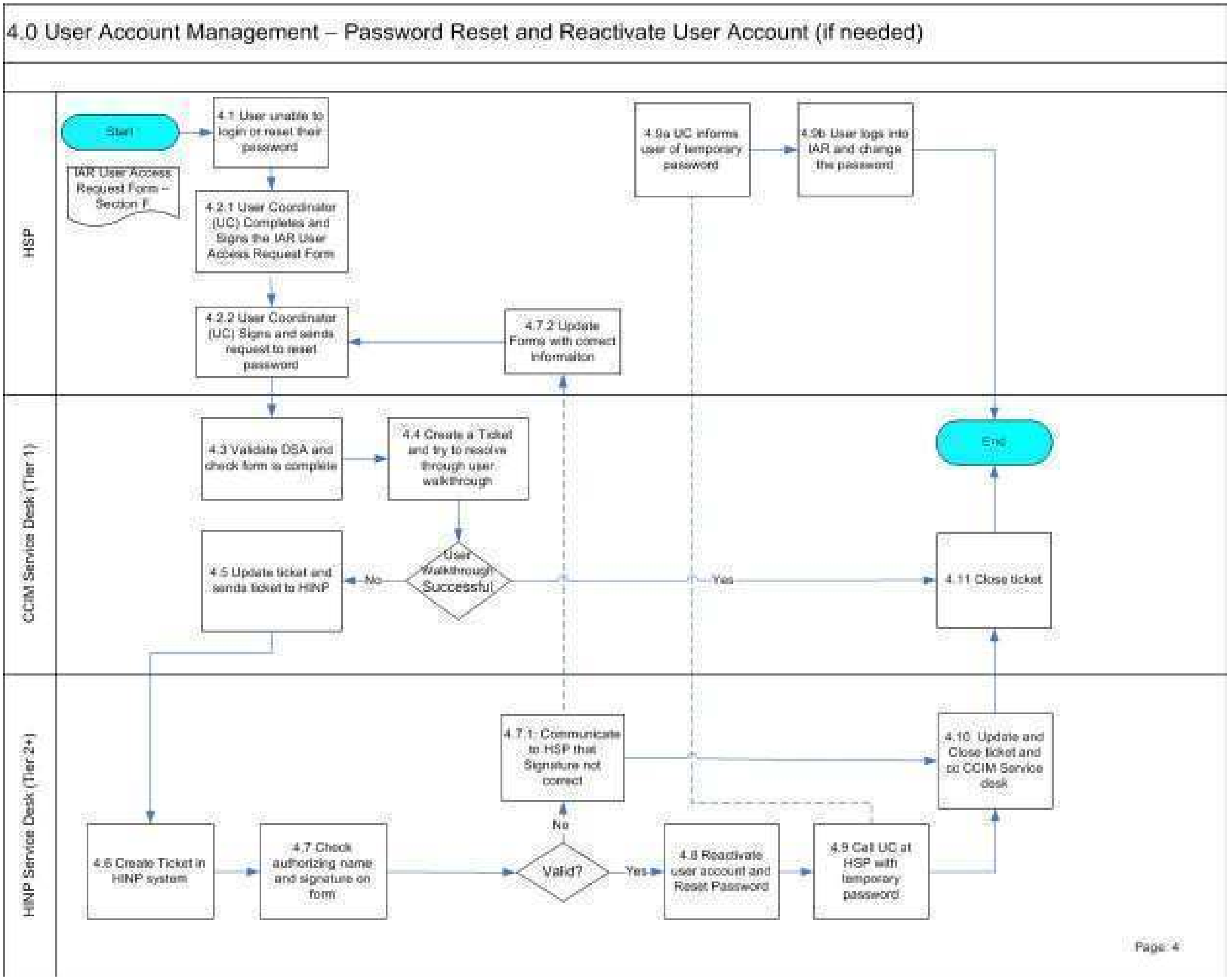

3.0 User Account Management – User Removal Request
HSP
CCIM Service Desk (Tier 1) / Implementation Team
HINP Service Desk (Tier 2+)
Start
3.1 HSP completes User Access Request form – Request type "Remove User"
IAR User Access Request Form – Section D
3.2 User Authority (UA) authorizes user account request
3.3 User Coordinator (UC) sends request remove user account
3.6.2: HSP Corrects Signature and re-submit
3.8a UC informs manager that user account is remove
End
3.4 creates/updates ticket (footprints) and sends ticket to HINP
3.10 Update and close ticket
3.5 Create Ticket in HINP system
3.6.1: Communicate to HSP that Signature not correct
3.9 Update and Close ticket and cc CCIM Service desk and HSP
3.6 Validate authorizing name and signature on form
Valid?
no
Yes
3.7 Delete user account in IAR
3.8 Sends message to UC informing that user account removal is completed

Ref No.	Task / Step	Owner	Artifacts
	User Account Management Process – Removal of user accounts, due to the following reasons: • User is no longer associated with the participating organization • User responsibilities have changed within the organization, and the user no longer need access to IAR system		
3.1	User's manager or HR completes the IAR HSP and User Access Form by clicking the Checkbox beside "Remove User" and providing the Details of the user to be removed. The form is then forwarded to the User Authority within the Organization.	HSP	IAR HSP and User Access Form
3.2	UA checks and signs the request sends it to UC at the Organization.	HSP	IAR HSP and User Access Form
3.3	The User Coordinator forwards the request to CCIM support desk. If the request is urgent, the UC can communicate with the CCIM Support Desk directly, and follow up with the IAR HSP and User Access Form	HSP	IAR HSP and User Access Form
3.4	The IAR Support Centre reviews the IAR User Access Form, raises a ticket, and assigns it to the HINP.	IAR Support Centre	IAR HSP and User Access Form
3.5	The HINP User Account Management Team receives the account removal request and creates a ticket in their system	HINP	IAR HSP and User Access Form
3.6	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no. 3.7 otherwise proceed to step no. 3.6.1	HINP	IAR HSP and User Access Form
3.6.1	If the signature is not verified the HINP User Account Management Team informs the HSP accordingly and closes the ticket	HINP	IAR HSP and User Access Form
3.6.2	The HSP Then corrects the signatures on the form and resubmits the request	HSP	IAR HSP and User Access Form
3.7	The HINP User Account Management team reviews the details on the User Account Removal request. User Account Management team removes the user account.	HINP	IAR HSP and User Access Form

3.8	The User Account Management team informs the UC that the user account is removed.	HINP	
3.8a	The UC informs the user's manager who made the user account removal request that the user account is removed.	HSP	
3.9	The HINP User Account Management Team updates and closes the ticket, while cc'ing IAR support desk (at CCIM) and the HSP	HINP	
3.10	IAR Support Centre updates and closes the ticket.	IAR Support Centre	

Note: The privacy officer needs to be appropriately informed of the user account management process (i.e., new user account creation, modification and removal).

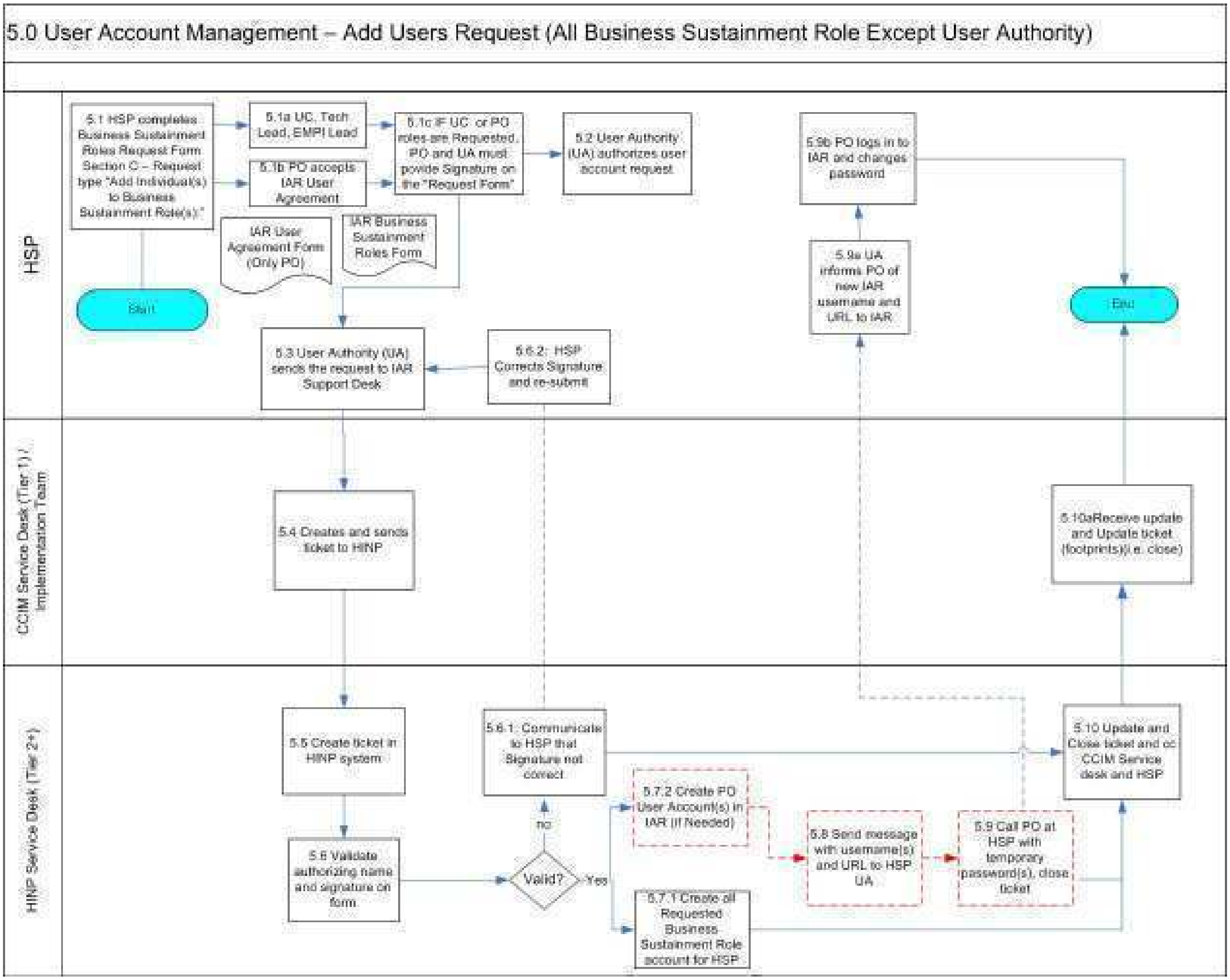
Scenario 4 – Password Reset and Reactivate User Account (if required)


4.0 User Account Management – Password Reset and Reactivate User Account (if needed)
HSP
CCIM Service Desk (Tier 1)
HINP Service Desk (Tier 2+)
Start
4.1 User unable to login or reset their password
IAR User Access Request Form – Section F
4.2.1 User Coordinator (UC) Completes and Signs the IAR User Access Request Form
4.2.2 User Coordinator (UC) Signs and sends request to reset password
4.7.2 Update Forms with correct information
4.9a UC informs user of temporary password
4.9b User logs into IAR and change the password
4.3 Validate DSA and check form is complete
4.4 Create a Ticket and try to resolve through user walkthrough
End
4.5 Update ticket and sends ticket to HINP
No
User Walkthrough Successful
Yes
4.11 Close ticket
4.7.1: Communicate to HSP that Signature not correct
4.10 Update and Close ticket and cc CCIM Service desk
No
4.6 Create Ticket in HINP system
4.7 Check authorizing name and signature on form
Valid?
Yes
4.8 Reactivate user account and Reset Password
4.9 Call UC at HSP with temporary password
Page 4

Ref No.	Task / Step	Owner	Artifacts
	User Account Management Process – Password Reset, due to the following reasons: • User's account is locked and due to inactivity • User is unable to reset the password through the IAR online password change utility		
4.1	IAR user is unable to reset password using the IAR online Password utility and contacts UC for their IAR Password reset	HSP	
4.2.1	User Coordinator (UC) completes the IAR HSP and User Access Form by completing Section F: Manage Password Resets and Reactivations, with the relevant details of the users whose password need to changed or account reactivated.	HSP	IAR HSP and User Access Form
4.2.2	The User Coordinator signs and forwards the request to CCIM support desk.	HSP	IAR HSP and User Access Form
4.3	The IAR Support Centre validates the org status as a participating org and reviews the IAR User Access Form, raises a ticket, and assigns it to the HINP.	IAR Support Centre	IAR HSP and User Access Form
4.4	The IAR Support Center Contact the users and try to resolve the issue by assisting them with the online password change utility. If the Walkthrough is successful The Ticket is closed otherwise proceed to step no. 4.5	IAR Support Centre	
4.5	The IAR support Center updates the ticket and forward the ticket to HINP	IAR Support Centre	IAR HSP and User Access Form
4.6	The HINP User Account Management Team creates a ticket in their System	HINP	IAR HSP and User Access Form
4.7	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no. 4.8 otherwise proceed to step no. 4.7.1	HINP	IAR HSP and User Access Form
4.7.1	If the signature is not verified the HINP User Account Management Team informs the HSP accordingly and closes the ticket	HINP	IAR HSP and User Access Form
4.7.2	The HSP Then corrects the signatures on the form and resubmits the request	HSP	IAR HSP and User Access Form
4.8	The HINP User Account Management team reviews the details on the	HINP	IAR HSP and User

	User Account Password reset or account reactivation request. User Account Management team reactivates the account (if required) and reset the password with a temporary password which is configured to be changed at the first login		Access Form
4.9	The User Account Management team calls the UC and informs them that the user account is reactivated (if required). The temporary password is also communicated to the UC	HINP	
4.9a	The UC informs the user about the account reactivation (if needed) and the temporary password	HSP	
4.9b	The User Logs into the IAR and change the temporary password	HSP	
4.10	The HINP User Account Management Team updates and closes the ticket, while cc'ing IAR support desk (at CCIM) and the HSP	HINP	
4.11	IAR Support Centre updates and closes the ticket.	IAR Support Centre	

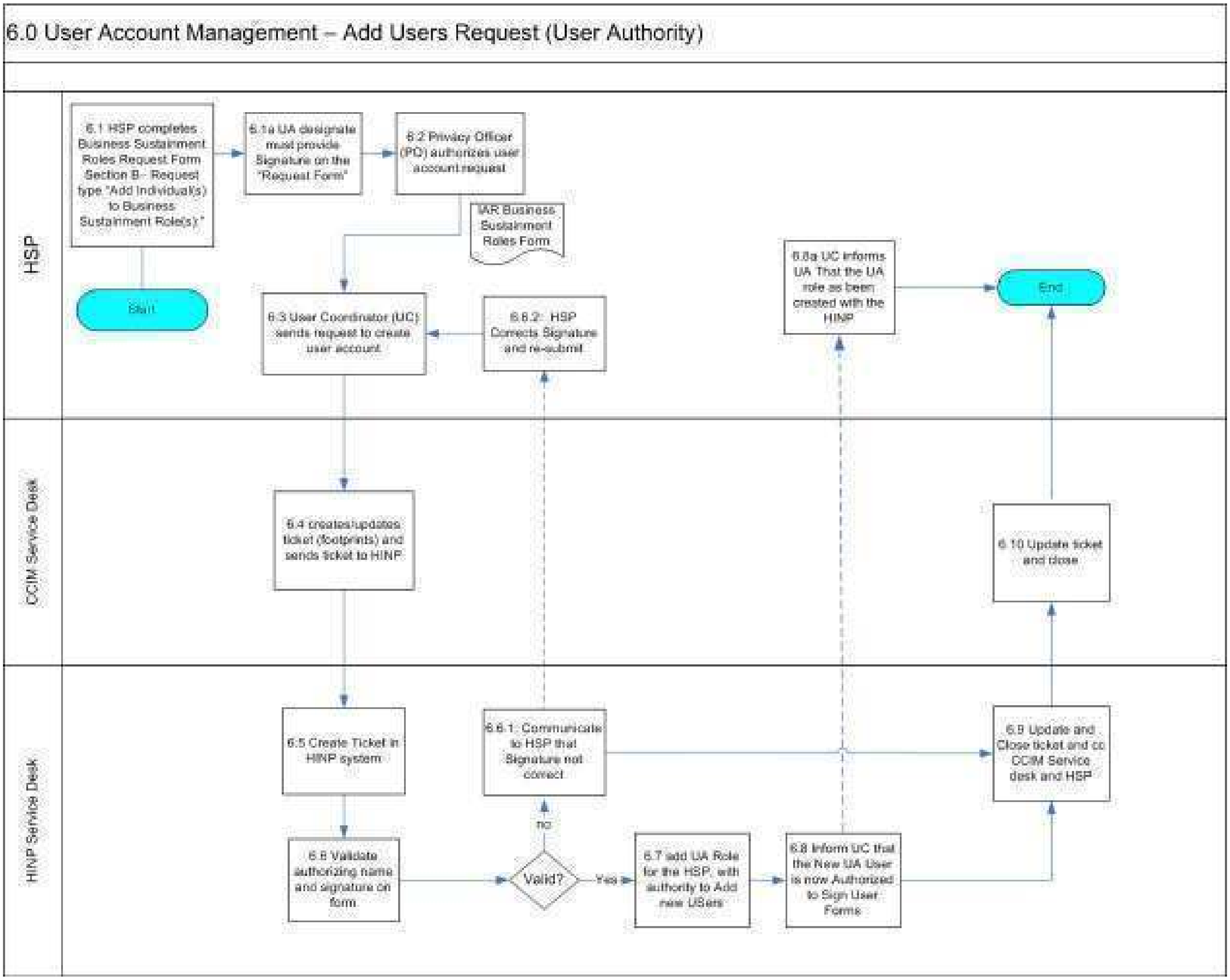
Scenario 5 – Create (or Add) All Business Sustainment Role Users (Except User Authority)


5.0 User Account Management – Add Users Request (All Business Sustainment Role Except User Authority)
HSP
CCIM Service Desk (Tier 1) / Implementation Team
HINP Service Desk (Tier 2+)
5.1 HSP completes Business Sustainment Roles Request Form Section C – Request type "Add Individual(s) to Business Sustainment Role(s)."
Start
5.1a UC, Tech Lead, EMPI Lead
5.1b PO accepts IAR User Agreement
IAR User Agreement Form (Only PO)
IAR Business Sustainment Roles Form
5.1c IF UC or PO roles are Requested, PO and UA must povide Signature on the "Request Form"
5.2 User Authority (UA) authorizes user account request
5.3 User Authority (UA) sends the request to IAR Support Desk
5.6.2: HSP Corrects Signature and re-submit
5.9b PO logs in to IAR and changes password
5.9a UA informs PO of new IAR username and URL to IAR
End
5.4 Creates and sends ticket to HINP
5.10aReceive update and Update ticket (footprints)(i.e. close)
5.5 Create ticket in HINP system
5.6 Validate authorizing name and signature on form
Valid?
no
Yes
5.6.1: Communicate to HSP that Signature not correct
5.7.2 Create PO User Account(s) in IAR (If Needed)
5.7.1 Create all Requested Business Sustainment Role account for HSP
5.8 Send message with username(s) and URL to HSP UA
5.9 Call PO at HSP with temporary password(s), close ticket
5.10 Update and Close ticket and cc CCIM Service desk and HSP

Ref No.	Task / Step	Owner	Artifacts
	User Account Management Process – Creation (or add) New Business Sustainment Role **The Process is used for creating or adding the following Business Sustainment Role Users** • User Coordinator (UC) • Privacy Officer (PO) • Technical Lead/ Webservice Contact • Enterprise Master Patient Index Lead (EMPI Lead) The User Authority and Privacy Officer roles must be held by different individuals • Each new user account must be authorized by the User Authority of the respective organization. The User Authority (UA) is a designated person in the participating organization that approves creation of new user accounts in IAR. • Each new user is required to read and accept the IAR User Agreement.		
5.1	The HSP management team completes the IAR Business Sustainment Roles Form with the required user details.	HSP	IAR Business Sustainment Roles Form
5.1a	For User Coordinator, Technical lead and EMPI lead roles, IAR User Agreement form is not required	HSP	IAR Business Sustainment Roles Form
5.1b	If a Privacy officer Role is requested, The Privacy officer must sign the "IAR User Agreement Form"	HSP	IAR Business Sustainment Roles Form IAR User Agreement
5.1c	If a User Coordinator (UC) and / or a Privacy Officer (PO) roles are requested, both the UC and the PC must provide a sample of their signature by signing the IAR Business Sustainment Roles Forms	HSP	IAR Business Sustainment Roles Form
5.2	The User Authority (UA) checks the user Agreement to ensure the user has read and signed it (if needed), checks the IAR Business Sustainment Roles Form to ensure PO and / or UC have signed it (if UC or PO or both roles are requested) UA then authorizes the user access to IAR by signing the IAR Business Sustainment Roles Form and acknowledging the user has read and signed the IAR User Agreement.	Health Service Providers	IAR Business Sustainment Roles Form

5.3	The User authority (UA) signs and sends the User Account Request form to IAR Support Center located at CCIM.	HSP	IAR Business Sustainment Roles Form
5.4	The IAR Support Centre reviews the IAR Business Sustainment Roles Form, ensures that the HSP is IAR participant, raises a ticket, and assigns it to the HINP.	IAR Support Center	
5.5	The HINP User Account Management Team Creates a ticket in the HINP ticketing system		
5.6	The HINP User Account Management Team reviews and validates the HSP User Authority If the signature are fine please skip the next two steps and move to step 5.7	HINP	
5.6.1	If the HINP if not satisfied that the Signature on the form belongs to the User authority it has on the record for the organization, HINP would inform the HSP. And close the ticket	HINP	
5.6.2	HSP corrects the form and gets the correct signatures and resubmit the form via a new ticket.	HSP	
5.7.1	The HINP User Account Management Team Creates the Business sustainment Users for the HSP	HINP	
5.7.2	The HINP User Account Management Team Creates the Privacy officer account in the IAR		
5.8	The HINP User Account Management Team sends the newly created IAR PO username and the URL for the application to the HSP User authority (if needed)	HINP	
5.9	A member of the HINP User Account Management Team calls the User Authority with the password for PO account (if needed)	HINP	
5.9a	The User authority informs the user of the newly created IAR username and password	HSP	
5.9b	The new PO user logs on to IAR, and changes their password to a new and unique password. The initial user password expires upon user's first logon.	HSP	
5.10	The HINP User Account Management Team updates and closes the ticket.	HINP	
5.10a	The IAR Support Centre updates and closes the ticket.	IAR Support Centre	

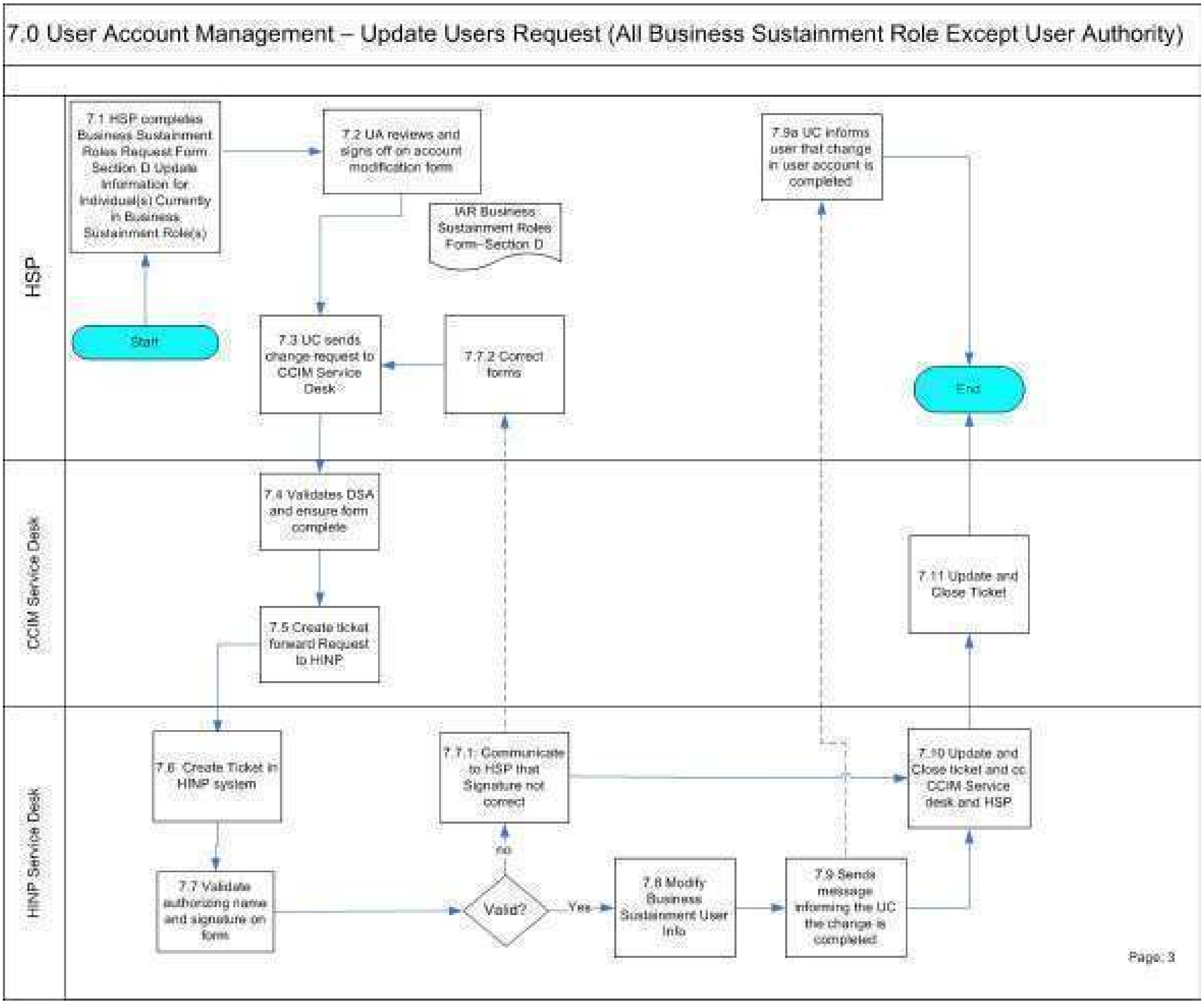
Scenario 6 – Create User Authority Role User


6.0 User Account Management – Add Users Request (User Authority)
HSP
CCIM Service Desk
HINP Service Desk
6.1 HSP completes Business Sustainment Roles Request Form Section B– Request type "Add Individual(s) to Business Sustainment Role(s)."
Start
6.1a UA designate must provide Signature on the "Request Form"
6.2 Privacy Officer (PO) authorizes user account request
IAR Business Sustainment Roles Form
6.3 User Coordinator (UC) sends request to create user account.
6.6.2: HSP Corrects Signature and re-submit
6.8a UC informs UA That the UA role as been created with the HINP
End
6.4 creates/updates ticket (footprints) and sends ticket to HINP
6.10 Update ticket and close
6.5 Create Ticket in HINP system
6.6.1: Communicate to HSP that Signature not correct
6.9 Update and Close ticket and co CCIM Service desk and HSP
6.6 Validate authorizing name and signature on form
no
Valid?
Yes
6.7 add UA Role for the HSP, with authority to Add new USers
6.8 Inform UC that the New UA User is now Authorized to Sign User Forms

Ref No.	Task / Step	Owner	Artifacts
	User Account Management Process – Creation (or add) New Business Sustainment Role **The Process is used for creating or adding the following Business Sustainment Role Users** **Business Sustainment Role (BSR) Definitions:** - User authority (UA) The User Authority and Privacy Officer roles must be held by different individuals - Each new UA account must be authorized by the Privacy officer (PO) of the respective organization.		
6.1	The HSP management team completes the IAR Business Sustainment Roles Form with the required user details	HSP	IAR Business Sustainment Roles Form
6.1c	UA must provide a sample of their signature by signing the IAR Business Sustainment Roles Forms	HSP	IAR Business Sustainment Roles Form
6.2	The Privacy officer checks the IAR Business Sustainment Roles Form to ensure UA have signed it PO then authorizes the user access by signing the IAR Business Sustainment Roles Form and forward the form to User Coordinator	Health Service Providers	IAR Business Sustainment Roles Form
6.3	The User Coordinator sends the User Account Request form to IAR Support Center located at CCIM.	HSP	IAR Business Sustainment Roles Form
6.4	The IAR Support Centre reviews the IAR Business Sustainment Roles Form, ensures that the HSP is IAR participant, raises a ticket, and assigns it to the HINP.	IAR Support Center	IAR Business Sustainment Roles Form
6.5	The HINP User Account Management Team Creates a ticket in the HINP ticketing system		IAR Business Sustainment Roles Form
6.6	The HINP User Account Management Team reviews and validates the HSP User Authority If the signature are fine please skip the next two steps and move to step 6.7	HINP	IAR Business Sustainment Roles Form
6.6.1	If the HINP if not satisfied that the Signature on the form belongs to the Privacy officer it has on the record for the organization, HINP would	HINP	

	inform the HSP. And close the ticket		
6.6.2	HSP corrects the form and gets the correct signatures and resubmit the form via a new ticket.	HSP	
6.7	The HINP User Account Management Team Creates the UA Users for the HSP in its records	HINP	IAR Business Sustainment Roles Form
6.8	A member of the HINP User Account Management Team calls the User Coordinator and informs him that the UA is now authorized to sign user forms	HINP	
6.8a	The Use Controller Update the User authority with the information	HSP	
6.9	The HINP User Account Management Team updates and closes the ticket.	HINP	
6.10	The IAR Support Centre updates and closes the ticket.	IAR Support Centre	

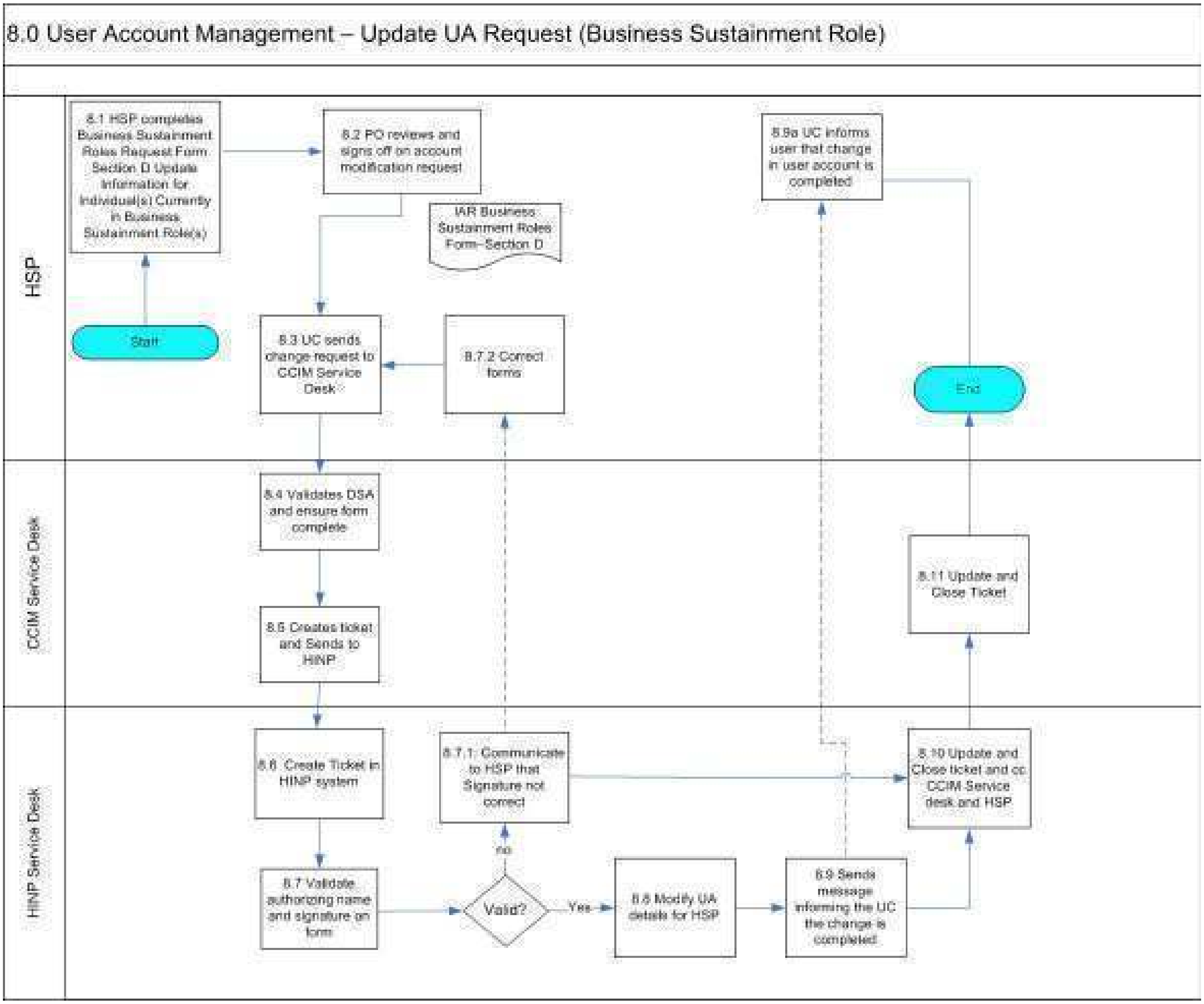
Scenario 7 – Update All Business Sustainment Role (Except User Authority)


7.0 User Account Management – Update Users Request (All Business Sustainment Role Except User Authority)
HSP
CCIM Service Desk
HINP Service Desk
Start
7.1 HSP completes Business Sustainment Roles Request Form Section D Update Information for Individual(s) Currently in Business Sustainment Role(s)
7.2 UA reviews and signs off on account modification form
IAR Business Sustainment Roles Form–Section D
7.9a UC informs user that change in user account is completed
7.3 UC sends change request to CCIM Service Desk
7.7.2 Correct forms
End
7.4 Validates DSA and ensure form complete
7.11 Update and Close Ticket
7.5 Create ticket forward Request to HINP
7.6 Create Ticket in HINP system
7.7.1: Communicate to HSP that Signature not correct
7.10 Update and Close ticket and cc CCIM Service desk and HSP
no
7.7 Validate authorizing name and signature on form
Valid?
Yes
7.8 Modify Business Sustainment User Info
7.9 Sends message informing the UC the change is completed
Page: 3

Ref No.	Task / Step	Owner	Artifacts
	7.0 User Account Management – Update Business Sustainment Role User Information: **The Process cannot be used to change User's Business Sustainment Role.** **Note for Name Changes**: If an individual filling a UA, UC or PO Business Sustainment Role is changing his/her name, ensure his/her signature is also updated in the applicable field. **For the Following Business Sustainment Roles:** User Coordinator (UC), Privacy Officer (PO), Technical Lead and Enterprise Master Patient Index (EMPI) Lead.		
7.1	The HSP management team completes the IAR Business Sustainment Roles Form with the required user details provided in Section D of the form (**UPDATE INFORMATION FOR INDIVIDUAL(S) CURRENTLY IN BUSINESS SUSTAINMENT ROLE(S))**	HSP	IAR Business Sustainment Roles Form
7.2	The User authority at the HSP reviews and signs the IAR User Access Form, authorizing the changes and pass it to the UC at the HSP	HSP	IAR Business Sustainment Roles Form
7.3	The UC forwards the form to IAR support desk at CCIM.	HSP	IAR Business Sustainment Roles Form
7.4	IAR support desk validates the HSP is IAR participant by checking the DSA and checks the submitted form is complete	IAR Support Desk	
7.5	The IAR Support Center raises a ticket, and forward the Account change request to appropriate HINP	IAR Support Centre	IAR Business Sustainment Roles Form
7.6	The HINP User Account Management Team receives the account change request and creates a ticket in their system	HINP	IAR Business Sustainment Roles Form
7.7	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no.7.8 otherwise proceed to step no. 7.7.1	HINP	IAR Business Sustainment Roles Form
7.7.1	If the signature is not verified the HINP User Account Management Team informs the HSP accordingly and closes the ticket	HINP	
7.7.2	The HSP Then corrects the signatures on the form and resubmits the	HSP	

	request		
7.8	After the HSP Authorizing signature have been verified the HINP User Account Management Team modifies the Business Sustainment Role’s user info according to the details provided on the IAR Business Sustainment Roles Form	HINP	
7.9	The HINP User Account Management Team sends the information to the UC that the updates have been completed.	HINP	
7.9a	The User Coordinator informs the Bussiness Sustainment User that the change requested for the user account is complete	HSP	
7.10	The HINP User Account Management Team updates and closes the Ticket as well CC the CCIM desk that the ticket is now closed.	HINP	
7.11	The IAR Support Centre updates and closes the ticket.	IAR Support Centre	

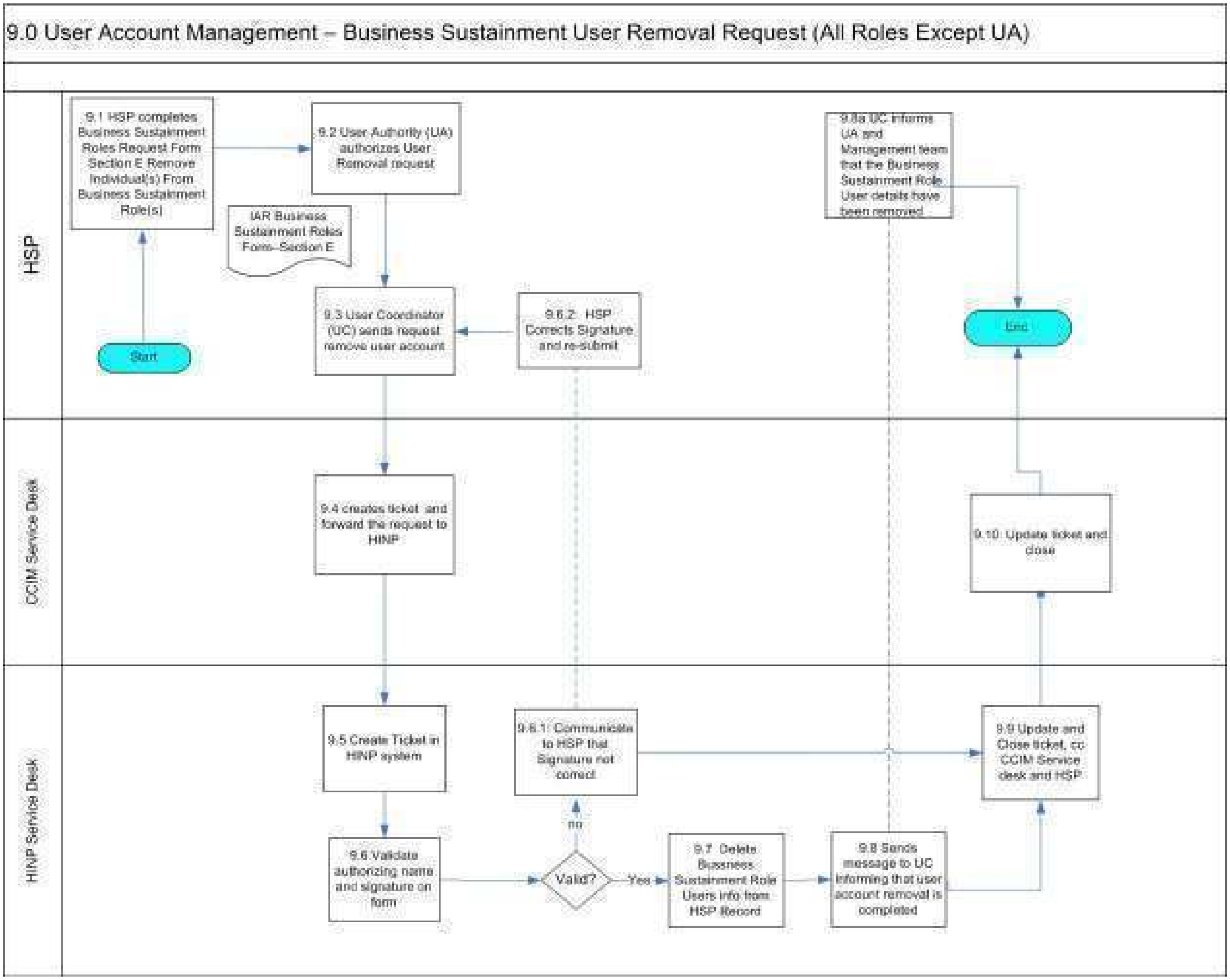
Scenario 8 – Update (or Change) User Authority Role User


8.0 User Account Management – Update UA Request (Business Sustainment Role)
HSP
CCIM Service Desk
HINP Service Desk
Start
8.1 HSP completes Business Sustainment Roles Request Form Section D Update Information for Individual(s) Currently in Business Sustainment Role(s)
8.2 PO reviews and signs off on account modification request
IAR Business Sustainment Roles Form–Section D
8.3 UC sends change request to CCIM Service Desk
8.7.2 Correct forms
8.9a UC informs user that change in user account is completed
End
8.4 Validates DSA and ensure form complete
8.5 Creates ticket and Sends to HINP
8.11 Update and Close Ticket
8.6 Create Ticket in HINP system
8.7.1: Communicate to HSP that Signature not correct
8.10 Update and Close ticket and cc CCIM Service desk and HSP
8.7 Validate authorizing name and signature on form
Valid?
no
Yes
8.8 Modify UA details for HSP
8.9 Sends message informing the UC the change is completed

Ref No.	Task / Step	Owner	Artifacts
	8.0 User Account Management – Update user Authority Information: **The Process cannot be used to change User's Business Sustainment Role.** **Note for Name Changes**: If an individual filling a UA, UC or PO Business Sustainment Role is changing his/her name, ensure his/her signature is also updated in the applicable field. **For the Following Business Sustainment Roles:** User authority (UA)		
8.1	The HSP management team completes the IAR Business Sustainment Roles Form with the User authority user's details provided in Section D of the form (**UPDATE INFORMATION FOR INDIVIDUAL(S) CURRENTLY IN BUSINESS SUSTAINMENT ROLE(S)**)	HSP	IAR Business Sustainment Roles Form
8.2	The Privacy at the HSP reviews and signs the IAR User Access Form, authorizing the changes and pass it to the UC at the HSP	HSP	IAR Business Sustainment Roles Form
8.3	The UC forwards the form to IAR support desk at CCIM.	HSP	IAR Business Sustainment Roles Form
8.4	IAR support desk validates the HSP is IAR participant by checking the DSA and checks the submitted form is complete	IAR Support Desk	
8.5	The IAR Support Center raises a ticket, and forward the Account change request to appropriate HINP	IAR Support Centre	IAR Business Sustainment Roles Form
8.6	The HINP User Account Management Team receives the account change request and creates a ticket in their system	HINP	IAR Business Sustainment Roles Form
8.7	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no.7.8 otherwise proceed to step no. 7.7.1	HINP	IAR Business Sustainment Roles Form
8.7.1	If the signature of the Privacy officer does not match the signature of the PO on record for the HSP, HINP User Account Management Team informs the HSP accordingly and closes the ticket	HINP	
8.7.2	The HSP Then corrects the signatures on the form and resubmits the	HSP	

	request		
8.8	After the HSP Authorizing signature have been verified the HINP User Account Management Team modifies the User Authority info according to the details provided on the IAR Business Sustainment Roles Form	HINP	
8.9	The HINP User Account Management Team sends the information to the UC that the updates have been completed.	HINP	
8.9a	The User Coordinator informs the Use Authority that the change requested for the user account is complete	HSP	
8.10	The HINP User Account Management Team updates and closes the Ticket as well CC the CCIM desk that the ticket is now closed.	HINP	
8.11	The IAR Support Centre updates and closes the ticket.	IAR Support Centre	

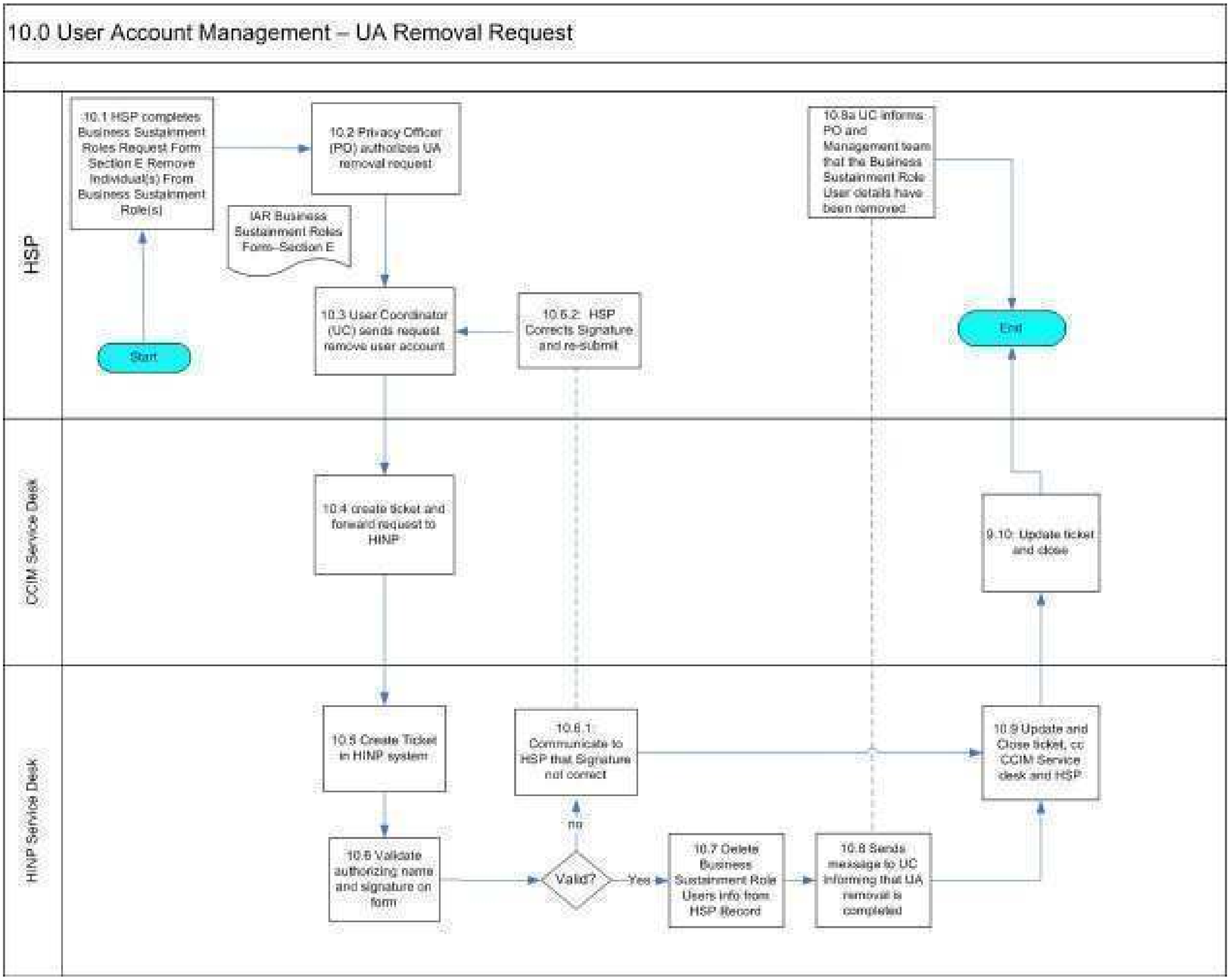
Scenario 9 – Remove All Business Sustainment Role (Except User Authority)


9.0 User Account Management – Business Sustainment User Removal Request (All Roles Except UA)
HSP
CCIM Service Desk
HINP Service Desk
Start
9.1 HSP completes Business Sustainment Roles Request Form Section E Remove Individual(s) From Business Sustainment Role(s)
9.2 User Authority (UA) authorizes User Removal request
IAR Business Sustainment Roles Form–Section E
9.3 User Coordinator (UC) sends request remove user account
9.6.2 HSP Corrects Signature and re-submit
9.8a UC informs UA and Management team that the Business Sustainment Role User details have been removed
End
9.4 creates ticket and forward the request to HINP
9.10 Update ticket and close
9.5 Create Ticket in HINP system
9.6.1 Communicate to HSP that Signature not correct
9.9 Update and Close ticket, cc CCIM Service desk and HSP
9.6 Validate authorizing name and signature on form
Valid?
no
Yes
9.7 Delete Bussness Sustainment Role Users info from HSP Record
9.8 Sends message to UC informing that user account removal is completed

Ref No.	Task / Step	Owner	Artifacts
	9.0 User Account Management – Remove Business Sustainment Role User Information:. due to the following reasons: • User is no longer associated with the participating organization • User responsibilities have changed within the organization, and the user no longer need access to IAR system **For the Following Business Sustainment Roles:** User Coordinator (UC), Privacy Officer (PO), Technical Lead and Enterprise Master Patient Index (EMPI) Lead.		
9.1	HSP's management team member completes the IAR Business Sustainment Roles Form - Section E providing the Details of the user to be removed. The form is then forwarded to the User Authority within the Organization.	HSP	IAR Business Sustainment Roles Form
9.2	UA checks and signs the request. UA then sends it to UC at the Organization.	HSP	IAR Business Sustainment Roles Form
9.3	The User Coordinator forwards the request to CCIM support desk. If the request is urgent, the UC can communicate with the CCIM Support Desk directly, and follow up with the IAR Business Sustainment Roles Form	HSP	IAR Business Sustainment Roles Form
9.4	The IAR Support Centre reviews the IAR Business Sustainment Roles Form, raises a ticket, and forwards the request to the HINP.	IAR Support Centre	IAR Business Sustainment Roles Form
9.5	The HINP User Account Management Team receives the Business Sustainment user removal request and creates a ticket in their system	HINP	IAR Business Sustainment Roles Form
9.6	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no. 9.7 otherwise proceed to step no. 9.6.1	HINP	IAR Business Sustainment Roles Form
9.6.1	If the signature is not verified the HINP User Account Management Team informs the HSP that the Signature of the UA does not match the Signature of UA on records and closes the ticket	HINP	IAR Business Sustainment Roles Form
9.6.2	The HSP then corrects the signatures on the form and resubmits the request	HSP	IAR Business Sustainment Roles Form
9.7	The HINP User Account Management team reviews the details on the	HINP	IAR Business

	IAR Business Sustainment Roles deletion request. User Account Management team removes the Business Sustainment Role user details from the HSP record at HINP.		Sustainment Roles Form
9.8	The User Account Management team informs the UC that the Business Sustainment Role User Details have been deleted.	HINP	
9.8a	The UC informs the User authority and the management team member who made the user account removal request that the user account is removed.	HSP	
9.9	The HINP User Account Management Team updates and closes the ticket, while cc'ing IAR support desk (at CCIM) and the HSP	HINP	
9.10	IAR Support Centre updates and closes the ticket.	IAR Support Centre	

Scenario 10 – Remove User Authority Role User


10.0 User Account Management – UA Removal Request
HSP
CCIM Service Desk
HINP Service Desk
Start
10.1 HSP completes Business Sustainment Roles Request Form Section E Remove Individual(s) From Business Sustainment Role(s)
10.2 Privacy Officer (PO) authorizes UA removal request
IAR Business Sustainment Roles Form–Section E
10.3 User Coordinator (UC) sends request remove user account
10.6.2: HSP Corrects Signature and re-submit
10.8a UC informs PO and Management team that the Business Sustainment Role User details have been removed
End
10.4 create ticket and forward request to HINP
9.10: Update ticket and close
10.5 Create Ticket in HINP system
10.6.1: Communicate to HSP that Signature not correct
10.9 Update and Close ticket, cc CCIM Service desk and HSP
no
10.6 Validate authorizing name and signature on form
Valid?
Yes
10.7 Delete Business Sustainment Role Users info from HSP Record
10.8 Sends message to UC informing that UA removal is completed

Ref No.	Task / Step	Owner	Artifacts
	9.0 User Account Management – Remove User Authority Role User Information:. due to the following reasons: • User is no longer associated with the participating organization • User responsibilities have changed within the organization, and the user no longer need access to IAR system **For the Following Business Sustainment Roles:** User authority (UA)		
10.1	HSP's management team member completes the IAR Business Sustainment Roles Form - Section E, providing the details of the User Authority Role user to be removed. The form is then forwarded to the User Authority within the Organization.	HSP	IAR Business Sustainment Roles Form
10.2	Privacy Officer (PO) checks and signs the request. PO then sends it to UC at the organization.	HSP	IAR Business Sustainment Roles Form
10.3	The User Coordinator forwards the request to CCIM support desk. If the request is urgent, the UC can communicate with the CCIM Support Desk directly, and follow up with the IAR Business Sustainment Roles Form	HSP	IAR Business Sustainment Roles Form
10.4	The IAR Support Centre reviews the IAR Business Sustainment Roles Form, raises a ticket, and forwards the request to the HINP.	IAR Support Centre	IAR Business Sustainment Roles Form
10.5	The HINP User Account Management Team receives the UA removal request and creates a ticket in their system	HINP	IAR Business Sustainment Roles Form
10.6	The HINP User Account Management Team reviews and validates the HSP authorizing signature. With two possible outcomes. If the signature is verified then proceed to step no. 10.7 otherwise proceed to step no. 10.6.1	HINP	IAR Business Sustainment Roles Form
10.6.1	If the signature is not verified the HINP User Account Management Team informs the HSP that the Signature of the UA does not match the Signature of UA on records and closes the ticket	HINP	IAR Business Sustainment Roles Form
10.6.2	The HSP then corrects the signatures on the form and resubmits the request	HSP	IAR Business Sustainment Roles Form
10.7	The HINP User Account Management team reviews the details on the	HINP	IAR Business

	IAR Business Sustainment Roles deletion request. User Account Management team removes the User authority (UA) user details from the HSP record at HINP.		Sustainment Roles Form
10.8	The User Account Management team informs the UC that the UA User Details have been deleted.	HINP	
10.8a	The UC informs the Privacy officer and the management team member who made the user account removal request that the user account is removed.	HSP	
10.9	The HINP User Account Management Team updates and closes the ticket, while cc'ing IAR support desk (at CCIM) and the HSP	HINP	
10.10	IAR Support Centre updates and closes the ticket.	IAR Support Centre	

Appendix A – IAR User Agreement

A user account with the IAR allows authorized personnel to access assessment data from any of the health care organizations that have participated in the IAR program ("**Participating Organizations**"). This agreement outlines the responsibilities that accompany IAR access. Possession of a user account entails responsibility to both your employer and the Participating Organizations whose data is accessible through the IAR.

In return for being given a user account by your employer, you agree that:

1. You will comply with all relevant laws, including the *Personal Health Information Protection Act, 2004*.
2. You will access and use personal health information ("**PHI**") from the IAR only for the purposes of providing health care (or assisting in the provision of health care) to the individual to whom the PHI belongs (the "**Patient**"). Furthermore, you will limit any access and use to what is necessary for these purposes.
3. You will maintain the confidentiality of all data in the IAR, and will not communicate this data to any other person except within the "circle of care" for the Patient.
4. If you become aware that the Patient (or the Patient's substitute decision-maker) has withheld or withdrawn consent for the collection, use or disclosure of the Patient's PHI, you will cease all access, use and disclosure of this PHI. You will advise your employer's Privacy Officer, if necessary.
5. If you transcribe, print or duplicate a Patient's record (or any portion of it) from the IAR, you will ensure that this information is either: a) maintained in the hard copy health record of the Patient, or b) disposed of in a secure manner in accordance with your employer's procedures.
6. You will not disclose your password or secret code. You will not use any other person's password or secret code.
7. You will access the IAR in accordance with these Terms and Conditions and any other conditions, policies and procedures that are required by your employer.
8. You understand that in agreeing to these Terms and Conditions, you are entering into a binding agreement with your employer.

In the event that you breach any of the provisions of this agreement, you may be subject to disciplinary actions up to (and including) dismissal. If these actions result in the suspension or revocation of your right to access PHI in the IAR as an Authorized User, the health care organizations participating in the IAR arrangement will be advised of the actions, as well as the rationale behind them.

____
Name of Authorized User (Print)

______________________________ ____________________
Signature of Authorized User **Date**

Note to user: Sign above and return the signed form to the IAR User Authority of your organization.

Appendix B – IAR HSP and User Access Form

Microsoft Office Word
Document

Appendix C – IAR Business Sustainment Roles Form

Microsoft Office Word
Document

User Account Management Process Implementation Work Sheet

Ref. No.	Integration Point	Analysis	As is Process	To be Process	Actions
1	**Create management process for assigning IAR accounts**	How are current IT user accounts being provisioned? Is there any existing tool or process we can leverage? Who determines whether a staff member has a need to access the IAR? Is it the immediate manager, supervisor, clinical lead or someone else in the organization?	Current process starts with HR — would the clinical lead may be a better person?	IAR access should be authorized by the clinical lead, not the HR manager, and the clinical lead should initiate the completion of the user account request forms (However HR should be part of the process)	- Work with HR to confirm this IAR user account provisioning process. - Develop communications to inform clinical lead of process and his/her responsibility - Privacy Officer to seek approval of this process from senior management
2	**Is a process in place for recording User's acceptance and signing the "IAR User Acceptance Form"**	Where will the signed forms be stored? How will UA verify that the User has signed the form			
3	**Create management process for assigning IAR Business Sustainment Roles**	How to assign, UA and UC, Technical Lead and EMPI lead roles within the HSP (e.g. A UA / UC for each facility) Is the Privacy officer for IAR the same as Organizational Privacy Officer (CPO)			
4	**Who would be assigned to be the backup for each role.**	If the user who fills the role is not available (on holidays or is sick) who would fulfill the role			
5	**Create management Process for reviewing User Roles assignment on a periodic basis**	Is the user fulfilling the role as required. Should the role be assigned to a different person			

6	**Change or update user account details, such as phone number, name, work locations, etc.**	Review current process and determine whether there is any opportunity to leverage existing process for updating user account for IAR. Determine who should be the User Authority, User Coordinator (UC).			
7	**Removal of user accounts when user no longer requires access to IAR**	Review current process and determine whether there is any opportunity to leverage existing process for removing user accounts for IAR. Determine who should be the User Coordinator (UC).			

Audit Log Review Guidelines

Integrated Assessment Record (IAR)

Version 5.0
January 2016

CCIM Community Care Information Management
ACCESS TO INFORMATION

Table of Contents

Introduction

The IAR audit log is a record of the software events occurring within the IAR system so each participating organization can review the events that are pertaining to their organization. The IAR audit log is composed of log entries, where each entry contains information related to a specific event that has occurred within IAR, such as a user login failure, a client search, a search for assessments, a viewing of an assessment, an assessment upload error, printing of an assessment, etc.

The IAR audit log is only accessible to privacy officers. The privacy officer of the participating organization can access the audit log file from their privacy officer account, where they can review the audit log of their respective organization. The global privacy officer (the privacy officer at the Health Integration Network Provider (HINP)), has access to the audit log of all the IAR users.

The Audit Log Review Basic Guidelines described below establish the minimum efforts for the local privacy officers to conduct audit log review activities in their respective operational environments.

The Audit Log Review Additional Guidelines included in this document are helpful examples and scenarios designed to assist the local privacy officers when conducting reviews and investigations using the audit log information.

To support the privacy officer's audit log review efforts, pre-defined audit log reports of key events have been developed to assist the monitoring and review of user activities in the privacy officer's organization.

Basic Guidelines

1. The privacy officer must review the IAR audit log frequently to look for abnormal activities and events. This should be done at minimum on a weekly basis.
2. Any suspicious or unusual event found during the audit log review must be investigated further. If applicable, an incident report should be completed, and appropriate parties should be alerted for further investigation and resolution of the incident.
3. In the event of inquiries or complaints by a client or staff member, audit logs or audit log reports must be reviewed in order to determine if an unauthorized event has occurred. As above, if applicable an incident report should be completed and appropriate parties alerted for further investigation and resolution of the incident.
4. Special attention must be paid to any events in the audit log or audit log reports that may identify potential disclosures of personal health information (PHI), such as unusually high volumes of printing, viewing, and other access events.

Additional Guidelines

The following are additional guidelines designed to help privacy officers review the IAR audit log.

1. Review Frequency

1.1 **Initial reviewing frequency —** For the initial three months of implementation, it is recommended that the privacy officer review the IAR audit log as often as possible or at a minimum of no less than once a week in order to:

- Familiarize themselves with the use of the audit log review user interface,
- Establish a baseline of user activities in the organization, and
- Establish a log review routine.

1.2 **Ongoing reviewing frequency —** Depending on the baseline established within the initial implementation period log review, the privacy officer can adjust the frequency of log review after the first 3 months.

2. Integration with Incident Management Process

2.1 As a result of conducting the review of the audit log and audit reports and any associated investigation, the privacy officer may need to alert other participating organizations (or the HINP) if the privacy officer uncovers an incident that affects these parties. Refer to the *Integrated Incident Management process* for details of how to escalate and communicate with the HINP and other participating organizations.

3. Log Review Techniques

3.1 **Use of the CSV export function —** All audit log reports displayed on the screen can be downloaded as a CSV file, which can be opened and accessed by Excel. Once the report is opened in Excel, data sorting, data filtering, and other Excel functionalities can be used to present the data in a way that will assist the investigation activities by the privacy officers.

4. Possible Incident Patterns

The following are recommended patterns to look for when reviewing the IAR audit log. For more details on establishing usage baselines and investigating incidents, refer to the investigation scenarios below.

4.1 Review Inactive Users

When reviewing the audit log, the privacy officer should pay attention to inactive users. If a user is inactive for an extended period of time, the privacy officer should investigate and determine if the user still has a legitimate reason to maintain an IAR user account.

Once a month, the privacy officer should list users that have not logged in to IAR for the last 30 days. For each inactive user account record on the list, the privacy officer should:

- Confirm with the user's manager or the Human Resources department that the user is still working in the organization.
- Confirm with the user's manager if the user is on vacation, or on any long term absence from his/her position; then consider disabling the user account temporarily, and only re-enable the user account upon the user's return.
- Confirm with the user's manager that the user still performs the functions that require IAR access; otherwise, the privacy officer should initiate the removal of the user account.

4.2 Review User Login Failures

Multiple sequential user login failures or user login authentication errors may indicate attempted unauthorized access (i.e., someone trying to login using someone else's credentials by guessing the passwords).

The privacy officer should use the event type and status filters to display user login failure events by entering date ranges, such as the last 7 days, 14 days, 30 days, etc.

When reviewing the failure login list, the privacy officer should look for unusually high volumes of unsuccessful login events on a single or on multiple user accounts. This may indicate an intruder is trying to gain access to the IAR system by using various user accounts and guessing the respective passwords.

During investigation the privacy officer should look for the physical IP address from which potential intrusion attempts originate, and work with the organization's physical security personnel to conduct further investigations (e.g., reviewing surveillance video footage of the physical location where the IP address is originated from, etc.).

4.3 Review for Unusual User Names

The privacy officer should review the audit log to look for any unusual usernames (usernames that are not of the same username convention). For example, if all usernames take the form "firstname.lastname" and user "mcc0004" logs in, this may indicate unauthorized access.
The privacy officer should contact the HINP privacy officer to investigate the creation of this unusual user account name, as well as the authorization of such a request. The HINP manages new user account creation and keeps records of all user account request forms authorized by the organizations. Contacting the HINP will determine whether the unusual username is a legitimate user of the organization.

4.4 Review for Out-of-Ordinary User Access to IAR

Once a user behavior baseline is established in the organization, it is much easier for the privacy officer to spot unusual or out-of-norm user access to IAR. The privacy officer should look for the following user access activities:

- Login frequency – By displaying only the successful login and logout events, the privacy officer can determine how often the users are logging in to IAR. Filtering the display down to 24-hour segments may make this particular review more manageable depending on the size of the organization and the number of IAR users in the organization.
- When a particular user logs in to IAR significantly more frequently than usual, (e.g., 10 times a day versus once a day), further investigation may be warranted. The privacy officer may consult with the user's immediate manager to determine if there has been a possible shift of the user's job responsibility. Out-of-norm login frequency may also indicate unauthorized use.
- Login duration – From the display of successful user login and logout events, the privacy officer can also determine if login duration for a particular user that is out-of-norm (e.g., between 6 am to 11 pm versus 9 am to 5 pm, etc. The increase of login frequency should also trigger the privacy officer to review the login duration for the same user to determine if there is legitimate business explanation for the increased login frequency and extended login duration in IAR.
- Login interval – From the same successful user login and logout event display, the privacy officer can also determine the interval between login sessions from the users. Again this is used to compare against normal user behavior, if the baseline is established that users login to IAR from Monday to Friday as a norm, and seldom login over the weekend. Then for example, any login sessions over the weekend are worth further examination. Together with the reviews regarding login frequency and login duration, the privacy officer should investigate if the login interval between user access events is out-of-norm when compared to the login frequency and login duration mentioned previously.
- In all of the above mentioned situations regarding access activities, the event by itself may not be a cause for concern (e.g. a user is shown logging in IAR over the weekends for two consecutive weeks and his/her usual usage pattern is always Monday to Friday). While this would be a good starting point for the privacy officer to conduct some preliminary investigation, there are many legitimate business explanations to such behavior, such as a project deadline or new organizational schedule. Therefore it is important to view these user activities variations with the broad understanding of business requirements and changes in the organization in mind.

4.5 Review for Unusually High Volume Client Search

Out-of-norm volumes of client searches from one single user warrant further investigation. The privacy officer should display daily or weekly user activities to determine if client search activities are of higher than normal volume. If the search events are higher than average, use filters to identify if these high search/view activities are from a single user. If that is the case, that particular user may be conducting client information surfing, or there is legitimate clinical reason for the high volume of searching of clients from that user.

The privacy officer may use local sources such as verbal interviews with the user's managers, the users themselves and possibly the user's peers to determine either the rationale for the increased in client search activities or if suspicious circumstances were observed.

4.6 Review for Unusually High Volume Assessment Search

Unusually high volumes of assessment searches from one single user on one or more clients warrant further investigation. The privacy officer should investigate and determine if the particular user has a legitimate reason for examining these client(s) in detail based on his/her job functions.

The privacy officer can use local sources such as verbal interviews with the user's managers, the users themselves and possibly the user's peers to determine rationale for the increased in client search activities or if suspicious circumstances were observed.

4.7 General Failure Events

As a general rule, the privacy officer should investigate any failure activities to determine if there is any logical explanation. For instance, a high surge in login failure activities across multiple users on a Monday morning after the March break holiday can be explained by the fact that the some users have forgotten their passwords due to the extended absence from normal IAR usage. A high volume of user login failure for a brand new user can also be attributed to the user's lack of familiarity with the IAR system. Failure events can be filtered by selecting the "Fail" button under Results.

4.8 Establishing a User Behavior Baseline

In addition to identifying possible incidents by matching the log with the pattern, privacy officers can establish a baseline of your user behaviors in order to conduct more comprehensive log reviews.

The privacy officer should review user activities from the IAR log on a regular basis and document the following:

- Number of search or view events
- Number of print events
- Time period of high user activity
- Time period of low user activity
- Number of user logins on week days
- Number of user logins on weekends
- Average duration of user login sessions
- Number of failed and successful event statuses

Calculating the averages from the data collected over a period of time will assist the privacy officer to establish baselines of user behaviors.

4.9 User did not login for several days or weeks

While reviewing the user activities, privacy officer should pay close attention to user login frequency and should be cognisant of all users who do not login for extended period of time it may be that the user is on holidays or else if the user's responsibilities have change, or because the user is no longer associated with the organization their account should be disabled immediately.

Privacy officer should run the PS8 – Inactive Users Accounts Report weekly to appraise themselves about the users who have not logged in for more than 90 days and ensure that the users who do not need the account are removed from IAR immediately

5. IAR Reports for Privacy Officers

There are two kinds of audit log reports in IAR: privacy and security reports and IAR operations.

5.1 Privacy and Security Reports

Report Names	Report Descriptions
PS1 - IAR User Activities Report	The report presents a list of logged audit events on a user-by-user basis for a specified time period
PS2 - IAR Event Type Report	This report provides summary details of all login events (successful and failed logins) for all users of the organization for a given date range
PS3 – IAR Consent Directives History Report	This report displays a list of both IAR-level and HSP-level consent directive changes for a client in a specified time period. This report shows all consent directives requested by this client and updated in the IAR system during the specified period of time
PS4 – IAR Current Consent Directive Report	This report displays a list of both IAR-level and HSP-level consent directives currently registered for a particular client. If the client has never requested or changed his/her IAR-level consent directive, the default IAR-level consent directive is "GRANTED" and is not presented in this report.
PS5 - IAR User PHI Access Report	This report presents a list of all the assessments accessed by a specific IAR user. Based on the selected User ID and date/time range, the report shows which patient/client and which assessments that user has reviewed or accessed. This report is focused on access related events (i.e. events where either the PHI and/or the assessments were viewed).
PS6 - IAR PHI Disclosure Report	This report, based on the selected client ID and date/time range, will present which user from which organization has accessed this selected client's assessment .
PS7 - Assessment Disclosure Report	This report displays users from outside of the current organization who have accessed a person's assessments belonging to (i.e., uploaded from) the current HSP.
PS8 – Inactive Users Accounts Report	This report displays user's Last successful login, and the days of inactivity. The privacy officer should ensure that any user who has not logged in for more than 90 days has a valid reason or should be disabled in the system

5.2 Operational Reports

Report Names	Report Descriptions
OP1 – List of IAR Users	This report provides a list of all IAR users, primarily sorted by their organizational affiliations and secondarily by their roles
OP2A – List of IAR Locations	The OP2A report shows all of the IAR Locations, Location ID, and associated IP-Address
OP2B – List of IAR Organizations	The OP2B shows all of the IAR organizations, their Organization name, Organization ID, as well as when they

Report Names	Report Descriptions
	joined this particular cluster

5.3 IAR Logs

Log Names	Log Descriptions
LOG1 – Current Activity Log	The Log contains information about all sessions currently active. The organizational privacy officer can view the current activity of all currently logged in users from their organization
LOG2 – Privacy Log	Contains Information about Privacy override. This feature is currently unavailable therefore the privacy logs should be empty
LOG3 – Clinical Log	Clinical Log contains detail information about user activities, including login time, log off time, search performed, upload, change or open any assessments etc. Privacy officers of the organization can use the log to build a history of user activities
LOG4 – System Log	System log contains information about the system activities, and is used to check the start up and shutdown time of the system and to check if the database was exported or imported

Appendix A — IAR Report Review and Investigation Scenarios

Scenario 1: Cleaning Up Inactive User Accounts

Trigger: Monthly, bi-monthly scheduled or user-requested report indicates that some user accounts have been inactive for 90 days.
Pre-condition: Local privacy officers can only see local user accounts.
Starting Report: OP8, where AVG login=0
Pattern: If AVG login=0 and last login date/time is >90 days, then investigate further.
Investigation:
Verify why user is inactive. Use OP8 to determine User details such as the user's name. The privacy officer can then check with the user's manager, HR or other personnel within the organization to determine if:

i. The user is on extended holiday or maternity leave
ii. The user has been transferred to another department or have left the organization
iii. The use has another reason for not using IAR

Depending on why user is inactive, determine if user account should be disabled. IAR queries or reports are not necessary for this step.
Post-Condition: Follow the IAR User Account Management process to disable accounts where appropriate.

Scenario 2: Developing a Usage Pattern

Trigger: Privacy officer wants to get a clearer picture of IAR user activities across the organization.
Pre-condition: Users must be local.
Starting Report: PS1
Pattern: Look for a pattern of user activities: most common events, average number of print events per week, etc. Use this pattern to establish a baseline and then run this report at pre-determined intervals to see if patterns change according to predictable behaviour, or if there is a deviation.
Post-Condition: *See scenario 4: Routine Log review for next steps after a baseline is established.*

Scenario 3: Routine Log Review

Trigger: As part of weekly, bi-weekly or monthly routinely scheduled log review, the local or HINP (global) privacy officer would call up PS1 to look at user activity and compare it with the established baseline usage pattern in an attempt to detect unauthorized or unusual activity as early as possible.
Pre-condition: Local privacy officer can only review usage patterns of users local to their organization. HINP (global) privacy officer can review usage patterns of all users across organizations.
Starting Report: PS1
Pattern: Viewing of an unusually large number of assessments or person records, unusually large number of search, view or print events as compared to average usage.

Investigation:

1. Determine if user has a valid business reason for this surge in activity. (Privacy officer would use local sources such as verbal interviews with the user's manager, the users themselves or possibly their peers to determine unusual events and if suspicious circumstances were observed.)
2. If there is a stated valid business reason to justify the change in usage pattern, verify if the frequency of events (e.g. views, prints, etc.) match anticipated clinical/business events such as "client/person was present for an appointment, client/person's case was under review for care planning, etc". Use report PS5 in correlation with clinical logs viewer.
3. If frequency seems appropriate, and no other suspicious activity was reported, document the investigation.
4. However, if there is no valid reason for this change in activity, the privacy officer should investigate further to get a clearer picture of the user's usage of IAR, including running:
   i. PS5 to determine which person records were accessed by this user and if the person had restricted consent directives
   ii. PS5 to get a clear picture of which assessments were accessed
5. If the user's activity extends to assessments from other organizations, the local privacy officer should document which assessments, which persons and which organizations are affected and provide this information to the HINP (global) privacy officer for further investigation.

Post-Condition: Document breach details using breach/incident investigation policy and templates, take corrective actions and notify affected clients/persons and other applicable parties as per policy.

Scenario 4: Failed logins

Trigger: As part of weekly, bi-weekly or monthly routinely scheduled log review, the local or HINP (global) privacy officer would call up PS2 where EventType=Login and EventStatus=Failed.

Pre-conditions:

- Local privacy officer can only see local users and events.
- User interface should allow this report to be run without requiring the privacy officer to enter any information besides a date and time range – i.e. There should be a "button" or clickable option called "Failed login reports" so the privacy officer doesn't have to choose "event type = login, status =failure".

Starting Report: PS2

Pattern: If there is a higher than average number of failed logins (e.g. more than 10 in 10 minutes, depending on the number of users/established usage patterns) then the privacy officer should investigate further.

Investigation:

1. The local privacy officer should contact the HINP (global) privacy officer to determine if there is a system-wide problem causing users to be unable to log in. If yes, document the reason for the failed logins and continue with other routine log review activities. (If the system-wide failure is a result of a security incident, the HINP Privacy officer will manage the incident and provide a report to affected HSPs as per the IAR Integrated Incident Management Process.)
2. If there is no system-wide reason for login failures, the Local Privacy Officer should validate if the login failures are actual login attempts by the user, or if there are suspicious circumstances involved. (Manual investigation – contact the user directly and get a list of when the users recall using the IAR system and what activities were performed at this time.)
3. If the user(s) do not recall attempting to login and having difficulty logging in during the time range identified in the report, the Privacy Officer should use the IP Address located under "Event Location" in PS2 and work with the operational/IT team to identify if this IP address is onsite, or at a remote location.

4. Additionally, the Privacy Officer should note any other activities by the users with the unexpected failed logins within the same time range to determine if these user accounts have been compromised and what has been viewed/downloaded/printed by these compromised accounts. (use PS5 with the approximate date/time range of the failed logins). If PHI has been compromised, determine which clients were affected,
5. Regardless of location, the Privacy Officer should work with the IT or security team to kick off a security incident investigation to determine what is going on at that node. If the IP address is local, physical security measures (eg cameras and access card readers, etc) may provide additional information as to how to contain the incident.
6. Based on the persons affected and the results of the security investigation, the Privacy officer should follow the IAR Integrated Incident Management Process to resolve the incident.

Post-Condition: Document incident details using breach/incident investigation policy and templates, and take corrective actions and notify affected clients/persons and other applicable parties as per policy.

Scenario 5: VIP or Victim of Violence

Trigger: A newspaper article is published containing a significant amount of a hockey player's PHI and it becomes clear that the PHI may have been leaked by a user at Organization A where the hockey player received services.

Pre-condition: Local privacy officer can see any users from any organizations that have accessed assessments that their HSP uploaded for this person.

Starting Report: PS6

Pattern: List of users that have access the hockey player's assessment information

Investigation:

1. The privacy officer should use the list of users that accessed the hockey player's assessment information and compare it with the organization's list of which clinicians and case workers had valid business reasons to access the hockey player's assessments. If there are user names that do not appear in the valid list, the privacy officer should investigate further manually through interviews with the user's manager and colleagues and other means as per scenario 10 (the nosy neighbour) below.
2. If all users had a valid reason to access the client's assessment, the privacy officer should still investigate with managers and within the care team to determine if it is possible that one of the clinicians used the assessment in an inappropriate manner. This is out of scope for the IAR processes.
3. If the users that accessed the hockey player's PHI did so from another organization, the local privacy officer should work with the HINP (global) privacy officer to coordinate the investigation of valid business reasons for access.

Post-Condition: The incident should be documented according to IAR Integrated Incident Management Process and corrective actions taken as appropriate.

Scenario 6: The Nosy Neighbour

Trigger: Client, user Y, third party, or global (HINP) privacy officer complains that User X is "surfing" persons or assessments, or "spying on" persons.

Pre-condition: If user is local, run report PS5. If user is not local, run report PS7 and then contact HINP privacy officer to continue investigation.

Starting Report: PS5, search by user X or PS7, search by date range when unauthorized disclosures are suspected.

Pattern: If user X has an unusually high number of persons viewed (according to your organization's established user patterns) and/or persons viewed have restricted consent directives, then investigate further.

Please note that when using PS7, you can use OP2 to identify the organizations listed in PS7. For complaints involving users from other organizations, contact the HINP privacy officer to continue your investigation.

Investigation using PS5:

1. Does User X have a valid business reason to view persons? (Privacy officer would use local sources such as: asking User X's manager, checking a roster of user roles to see if User X has a role that works with this type of person, or User X's client list, or potentially speaking with the person/client who raised the concern if applicable.)
2. **If yes, there is a valid business reason**: Verify if the frequency of access events (e.g. views, prints, etc.) match anticipated clinical/business events such as "client/person was present for an appointment, client/person's case was under review for care planning, etc".
   - Use report PS5 in correlation with other administrative logs

   If yes, the frequency of access correlates with valid clinical or business events, end the investigation and document the incident as cleared according to breach/incident investigation policy and templates.
3. **If the answer to either 2 or 2.a is no**:
   i. Identify which persons are affected.
   ii. Identify breach details:
      - Using PS5 identify if the actions performed on the persons and their assessments were "view person" or "view assessment" or "view assessment detail" or "print".
      - Depending on the event type, determine the likely nature of User X's activities: personal/curiosity (view type events) or possibly an external facing breach (print type events).
      - Use any other investigative means (interviews with User X's colleagues, affected client/persons, etc) to determine as many details as possible about User X's activities.

Post-condition: Document breach details using breach/incident investigation policy and templates, and take corrective actions and notify affected clients/persons and other applicable parties as per policy.

Audit Log Review Process Implementation Checklist

Ref. No.	Implementation Task	Action Plan	Status
1	Setup a weekly log review schedule (e.g., every Monday)		
2	Designate an individual or a team of individuals to review the audit log according to your review schedule		
3	Create a checklist for you and your team to use of things to review or look for to ensure nothing is missed when reviewing the audit log file		
4	Create a user activities baseline (e.g. usual login time, login frequency etc.)		
5	Create Assessments and Coordinated Care Plan baseline (e.g. searched per week)		
6	Logs and reports can be exported to CSV file (Excel) for further sorting, filtering, reporting and manipulation – develop a file naming convention for these export reports and sort them in folders (e.g., by month)		

Self-Assessment Checklist

Integrated Assessment Record (IAR)

Version 4.0
January 2016

CCIM
Community
Care
Information
Management
ACCESS TO INFORMATION

Table of Contents

Introduction

As defined in the Integrated Assessment Record (IAR) Data Sharing Agreement, each participating Health Service Provider (HSP) shall conduct a privacy and security self-assessment on an annual basis at its own cost according to the checklist approved by the Common Assessment and IAR Privacy, Security and Data Access Sub-Committee (hereinafter called the "Sub-Committee"). The results of the self-assessment must be acknowledged by HSP's senior management and submitted to the Sub-Committee for review.

This document is the checklist each HSP can use to conduct the annual self-assessment.

Self-Assessment Process

The HSP should complete the self-assessment electronically according to instructions out by the Health Information Network Provider (HINP). Once completed, the HSP Chief Executive Officer or designate shall acknowledge the content of the self-assessment form. A copy of the acknowledged self-assessment form should be provided to the HINP by the date set out by the HINP. The Privacy and Security Committee will review the results of the self-assessment forms.

Each HSP shall designate a privacy contact or privacy officer for the purposes of the self-assessment.

The self-assessment form shall be completed by providing a yes or no answer in the "Yes or No" column.

In completing the assessment, HSPs should also:

- Elaborate on identified gaps or deficiencies including details in the "Comments" column
- Set out an internal mitigation plan to address the identified gaps or deficiencies in the "Comments" column

HSPs should monitor the execution of the mitigation plan until the gaps or deficiencies are resolved as per the HSP's policies and procedures, and update the self-assessment form and forward to the HINP Privacy Officer with the update.

Organization Identification

To identify your HSP, please provide your IAR Organization ID:

This is likely also the number you use for your Management Information System (MIS) / Ontario Healthcare Reporting Standards (OHRS) submissions. If you are not aware of your IAR Organization ID, please contact the CCIM Support Centre at iar@ccim.on.ca.

Self-Assessment Checklist

1 General Questions

No.	Category	Question	Yes or No	Comments
GE1	**Governance**	Does the HSP designate a person responsible for the protection of PHI and the privacy of clients?		
GE2		Does the HSP have Existing Data Retention practice in effect		
GE3		Does the HSP have existing audit controls in place to collect data on all access, copying, disclosure, modification and disposal of client records		
GE4		Does the HSP have privacy policies and procedures in place that address the collection, use, disclosure, retention, disposal and protection of PHI in its custody?		
GE5	**Privacy Operation**	Does the HSP have an established consent management process?		
GE6		Does the HSP have an established breach management process?		
GE7		Does the HSP have an established client privacy right support process?		
GE8		Does the HSP have an established user account management process?		
GE9		Does the HSP have an established Log Review process for existing applications (if any)?		

No.	Category	Question	Yes or No	Comments
GE10	**Privacy Compliance**	Does The HSP have established frequent communication with employees, contractors and clients regarding privacy compliance? Provide estimate of the frequency of such communications		
GE11		How often does the HSP provide privacy and security training to its staff (provide frequency e.g. quarterly, annually)?		

2 Consent Management

No.	Category	Question	Yes or No	Comments
CM1	**Consent Model**	Has the HSP determined the consent model – implied or express consent or combination?		
CM2		Does the HSP consent model cover all PHI usage scenarios?		
CM3		Is the scope of the consent directive clearly defined?		
CM5	**Informing the Client**	Does the HSP define the approach to informing the client for consent?		
CM6		Has the HSP developed the material to inform the client?		
CM7		Does the material cover the following topics: -How and what personal information / personal health information is being collected, used, disclosed, shared and with whom -Purpose for collection/use/disclosure -Positive and negative consequences of giving or withholding consent -Client's privacy rights -Means for Challenging Compliance		

No.	Category	Question	Yes or No	Comments
CM8	**Consent Directive Form or Record of Consent**	Has the HSP developed the consent or consent directive form or an alternative record of consent?		
CM9		Does the form include the following information: -How and what personal information / personal health Information is being collected, used, disclosed, shared and with whom -Purpose for collection/use/disclosure - Positive and negative consequences of giving or withholding consent -Client's privacy rights		
CM10		Does the form capture adequate information for informed consent: -Description of information to be collected/used/disclosed -Purpose for collection/use/disclosure/ sharing -Client privacy rights -Condition for consent or consent directives		
CM11	**Recording the Consent Directive**	Does the HSP archive the consent form and/or log all consent directives provided by clients?		
CM12	**Registering or Updating the Consent Directive**	Has the HSP established the process to register or update the consent directives requested by the clients on paper charts or in the electronic system?		
CM13	**Enforcing the Consent Directive**	Are administrative controls or technical controls in place to effectively enforce the consent directive?		
CM14	**Implementing the Consent Management Process**	Is HSP staff trained on the consent model and consent management process?		
CM15		Is HSP staff involved in providing healthcare services able to		

No.	Category	Question	Yes or No	Comments
		appropriately respond to client's questions about consent?		
CM16		Is HSP staff involved in providing healthcare services able to execute the process appropriately?		

3 Audit Log Review Standards

No.	Category	Question	Yes or No	Comments
AL1	**Log Reviewer's Activity**	Has an individual been identified by your HSP to review the audit log?		
AL2		Is the audit log review being conducted regularly? If yes, provide the frequency in the Comments column (i.e. weekly, bi-monthly, monthly etc.)?		
AL3		Does your Organization collect, use or disclose PHI for "High Profile" clients (e.g. celebrities, politicians etc)		
AL4		If answer to AL3 is "Yes" do you have special audit program for information relating to "High Profile" clients		
AL5	**Incident Patterns**	Has a user behavior baseline (e.g. patterns of misuse) been established during the initial audit log review by the designated audit log reviewer?		
AL6		During regular audit log review, have unsuccessful login events been investigated?		
AL7		During regular audit log review, have inactive users being identified and deleted from the system?		
AL8	**Audit System Activities**	Are the system logs reviewed as part of the audit log review? If yes, provide the frequency in the comments column (i.e. weekly, bi-monthly, monthly etc.)?		

No.	Category	Question	**Yes or No**	**Comments**
AL9		Are the clinical logs reviewed as part of the audit log review? If yes, provide the frequency in the comments column (i.e. weekly, bi-monthly, monthly etc.)?		
AL10		Are the privacy logs reviewed as part of the audit log review? If yes, provide the frequency in the comments column (i.e. weekly, bi-monthly, monthly etc.)?		
AL11	**Audit User Activities**	When auditing the logs, do auditors review IAR reports PS5 and PS6 and confirm the need for user access to client data and the need for any printed copies		
Al12		When auditing the logs, do auditors review IAR reports PS5 and PS6 and confirm that all printed copies of the assessments are safeguarded appropriately and disposed after use.		

4□ Client Privacy Right Supporting Process

No.	Category	Question	Yes or No	Comments
CP1	**Clients Requesting Access to Their Assessment Data**	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	**Clients Requesting Change to Their Assessment Data**	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	**Client Complaint About HSP Privacy Practices**	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?		

5 Integrated Incident Management

No.	Category	Question	Yes or No	Comments
IM1	**Detection**	Has your internal incident management process been reviewed and updated to align with the IAR incident management process?		
IM2		Has the internal incident coordinator been identified for your HSP?		
IM3		Has the internal incident coordinator been made known to your staff so they know who to contact for an incident or breach?		

No.	Category	Question	Yes or No	Comments
IM4		Has the internal incident coordinator been made known to your clients so they know who to contact for an incident or breach?		
IM5		Has the internal incident coordinator been made known to your third party vendors or suppliers/clients so they know who to contact for an incident or breach?		
IM6		Does the incident management process include incident detection control?		
IM7	**Escalation**	Do the incident coordinator and/or privacy breach coordinators know how to contact the HINP Privacy Officer, who is responsible for escalation to other HSPs that are affected?		
IM8		Does the designated Privacy Officer understand his/ her roles and responsibilities within the incident management process?		
IM9		Does your HSP have an Incident Report form that is agreed upon with the HINP? (i.e. the information on your incident report is compatible with the incident registry at the HINP.)		
IM10	**Notification**	Does your HSP have a standard procedure to notify clients if a privacy breach involves the client's PHI?		

6 User Account Management

No.	**Category**	**Question**	**Yes or No**	**Comments**
UA1	**User Accounts**	Is the list of IAR users reviewed and validated regularly?		
UA2		Are required IAR user change and deletion requests communicated regularly?		
UA3		Do the new users read and sign the IAR User Agreement?		

Acknowledgement

By submitting this self-assessment form, I assert that the HSP’s Chief Executive Officer or delegate has acknowledged the content of this self-assessment form.

Name of Submitter of Self-assessment: ____

Name of Privacy Contact for Self-assessment: ____

Enterprise Master Patient Index (EMPI)

Business Process for the EMPI Lead at HSP

Integrated Assessment Record (IAR)

Version 2.0

January, 2016

Table of Contents

Glossary of Terms & Acronyms

1. **EMPI** – An Enterprise Master Patient Index (EMPI) provides a master index that may be used to obtain a unified view of a client across the continuum of care provided by multiple organizations.

2. **IAR** – Integrated Assessment Record is an initiative within CCIM that allows assessment information to move with the client as they go from one HSP to another. HSPs can use the IAR to view timely client assessment information electronically, securely and accurately, The IAR facilitates collaborative client/patient care planning in the community and more efficient and effective delivery of care.

3. **EMPI Lead** – The EMPI Lead is the person at the participating organizations who will receive notices from the EMPI Data Steward that there is a potential issue within client data. The EMPI Lead will need to identify and resolve the issue within their system and then ensure a corrected assessment is uploaded into the IAR.

4. **EMPI Data Steward (EDS) –** The EMPI Data Steward is the role that receives notification from the EMPI that there may be a data quality issue. The EDS also has a responsibility to contact the affected Health Service Provider (HSP) when data needs to be added or amended in their assessment and source system.

5. **Health Information Network Provider (HINP)** – Under the *Personal Health Information and Protection Act*, 2004 (PHIPA) a HINP is "a person [or organization] who provides services to two or more health information custodians [HICs] where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another." O. Reg. 329/04, s. 6 (2). A health information custodian, is also defined under PHIPA as "an individual or organization that has custody and control of personal health information generally for the purposes of providing health care or services."

6. **Local Client Identifier –** This is a number used by organizations to track their client (person). This is not a number for a visit or for an assessment. It is a single number used to identify that person whenever they attend one particular health service provider (HSP).

7. **Enterprise Identifier (EID) –** The EMPI creates a single, unique enterprise identifier for each person; as well as a mapping, or link, between the EID and any local client identifiers used for that person. This link provides the ability to search and find a client represented as a single entity. Then the authorized user can access multiple health data records without the need to know the local client identifier(s) or the point of origin of those records.

8. **Demographics –** In the EMPI, this data relates to an individual and includes name, gender, address, phone, date of birth and healthcard number.

9. **Value of Match –** The EMPI evaluates the demographic data in a just received record (person) by comparing it to records (persons) already contained in the EMPI. Each match has a value. For example, a match on healthcard number is weighted with a higher value than a match on phone number. A match on date of birth is weighted with a higher value than a match on a commonly occurring last name.

10. **Score –** The EMPI evaluation adds together the value of all matches to create a score. For example, the score would be higher for a record matched based on a person's name, date of birth and healthcard number than the score for a record matched with only a person's name and phone number.

11. **Inspector Task –** This is how the EMPI communicates that there is an issue or a potential issue with data. The EMPI creates a task for the EMPI Data Steward (EDS) which directs the EDS on what record needs to be investigated. Below are described two potential Inspector tasks.

12. **Potential Duplicate –** The EMPI thinks it is possible two records (two persons) from a single HSP source are actually the same person. Two local client identifiers for the same person within the same HSP system is called a duplicate. A potential duplicate requires a review by the EMPI Data Steward (EDS). If the EDS agrees that it might be a duplicate, the EMPI Lead Organization (ELO) will be contacted to evaluate with the potential to resolve the duplication in the HSP system.

    Potential Overlay – The EMPI suspects the local client identifier has been inadvertently used for a person different from who used it previously. The EMPI has compared the incoming record (person) to what the HSP sent earlier for this same person. If the demographic changes are too extensive – for example male changed to female, entire date of birth changed, name entirely changed – it alerts the EMPI Data Steward (EDS). The EDS will contact the EMPI Lead at the HSP to evaluate. Due to the client risk associated with an overlay, all the person's records in IAR will be restricted from view, regardless of contributing organization. Viewing will be restored after the HSP solution is determined and completed.

Introduction

An Enterprise Master Patient Index (EMPI) provides a master index that may be used to obtain a unified view of a client across the continuum of care provided by multiple organizations. For any single client, the EMPI creates a single, unique enterprise identifier (EID). The EMPI can establish and maintain a mapping between the EID and the client's identifiers used inside each of the organizations who contribute health data records. This association between the EID and the source systems' identifiers provides the ability to search the index and find a client represented as a single entity, thus allowing the authorized user access to multiple health data records regardless of the point of origin of those records.

The Integrated Assessment Record (IAR) EMPI Business Process for the HSPs deals with IAR-related client records from multiple regions, organizations and sectors. Both the organization hosting the EMPI as well as each participating organization in the IAR will be involved in the EMPI process.

The IAR EMPI system is implemented with matching algorithms. The EMPI compares demographic data in an incoming IAR record to information already existing in the master index. The following is a sample of data elements assessed by the EMPI:

- Name
- Date of Birth
- Gender
- Healthcard Number

Each matching data element is assigned a score that is weighted according to the estimated value of the match. When the total matching score is high, the EMPI has been configured to *automatically link* an existing EID with the incoming IAR record and its local client identifier. When the total score is low, a new EID is created and associated to the incoming client and their local client identifier. Scores between these two thresholds are flagged for manual review. Therefore, even a well tuned EMPI typically requires establishment of a data stewardship role to guide resolution of the following tasks:

1. Potential linkage
2. Potential duplicate
3. Potential overlay

This document describes a defined process and steps to the three above scenarios as they relate to the IAR; as well as identifies roles and responsibilities of the EMPI Lead at the participating organizations when these scenarios occur.

Processes

Scenario 1 – Potential Linkage

Examples:

- Different demographic data collected (use of nickname)
- Missing or invalid attributes

- The EMPI system has compared an incoming record to existing data in its index of clients
- The matching algorithms assigned a score too low for auto-linking
- The score is sufficiently high for the EMPI to flag the record for review by a EMPI Data Steward (EDS)
- The EDS lacks sufficient data for resolution
- The EDS notifies the EMPI Lead at the contributing organization for evaluation and resolution
- The EDS communicates to the EMPI Lead using template form (refer to Appendix A)
- The request may include one or more of the following:
  a. confirmation of one or more demographic data elements
  b. amendment of one or more demographic data elements
  c. addition of one or more missing demographic data elements
  d. action to resubmit the IAR submission which triggered the EMPI flag
- The HSP EMPI Lead receives the notification
- The EMPI Lead facilitates evaluation and resolution internally among stakeholders such as the clinicians, case managers, health record team, or the privacy officer
- The EMPI Lead follows up with stakeholders to ensure issue is resolved
- If necessary, the last assessment which triggered the EMPI flag is resubmitted/uploaded
- The EMPI Lead notifies the EDS that the data issues have been resolved

Scenario 2 – Potential Duplicate

Example:

– The person is given a new local client identifier in his/her return visit to the organization

- The EMPI system has compared an incoming record to existing data in its index of clients
- Another record from the same contributing organization appears to be a match
- The EMPI system suspects the contributing organization may have assigned a second, different local identifier to the same client
- The EMPI flags the two client records as needing review by an EMPI Data Steward
- The EDS does not have sufficient data for resolution
- The EDS notifies the contributing organization to resolve the duplicate
- The EDS requests the EMPI Lead to do one or more of the following:
    a. Confirm the 2 Local Client Identifier numbers reference the same client and resolve the duplicate identifiers into a single ID
    b. Confirm the two Local Client Identifiers reference two different patients
    c. Amend data elements where appropriate
    d. Resubmit assessment where applicable
- The HSP EMPI Lead receives the notification
- The EMPI Lead facilitates evaluation and resolution internally among stakeholders such as the clinicians, case managers, health record team, or the privacy officer
- The EMPI Lead follow s up with stakeholders to ensure issue is resolved (i.e. true duplicate or not)
- If necessary, the last assessment which triggered the EMPI flag is resubmitted/uploaded
- The EMPI Lead notifies EDS that data issues have been resolved

Scenario 3 – Potential Overlay

Example:

- Registration errors where a person record is accidentally used for a different person (e.g. Jane was using id 123, then id 123 was inadvertently used for Tom)

- The EMPI system has compared an incoming record to an IAR record previously received where both IAR records used the same Local Client Identifier from the same contributing organization
- The EMPI finds the demographic data element differences between a previous submission and the current submission to be large and significant
- The EMPI flags a potential "overlay"
- The EMPI suspects a second, different client may have been inadvertently attached to the local identifier
- Assessments using this client's EID will be made unavailable for viewing from the IAR repository until the potential overlay issue is resolved
- The EMPI flags the two sets of client demographics for review by the EMPI Data Steward (EDS)
- The EDS notifies the contributing organization immediately
- The EDS requests the EMPI Lead to do one or more of the followings:
  a) Confirm the Local Client Identifier does reference the same client
  b) Confirm the Local Client identifier has had a different client's demographic data overwritten into it. Cause the second patient to have their own Local Client Identifier. For the original client, restore the demographics associated to the original Local Client Identifier.
  c) Resubmit assessment where applicable
- The HSP EMPI Lead receives the notification
- The EMPI Lead facilitates evaluation and resolution internally among stakeholders such as the clinicians, case managers, health record team, or the privacy officer
- The EMPI Lead follows up with stakeholders to ensure issue is resolved
- If necessary the last assessment which triggered the EMPI flag is resubmitted/uploaded
- The EMPI Lead notifies the EMPI Data Steward that data issues have been resolved
- The EMPI Data Steward may contact the IAR technical team if the resolution requires the support at the IAR technical level. The IAR technical team will work with the EMPI Data Steward and the HSP to resolve the data quality issue.

Appendix A – Potential Linkage Notification

IAR System Data Quality Inquiry

Potential Linkage

1. Contact Information

Name of EMPI Lead:	Organization Number:	Date of Notification (dd/mm/yyyy)

2. Client/Patient Information:

Local Client Identifier:

Date Identified (dd/mm/yyyy)	Date Reviewed by EDS (dd/mm/yyyy)

3. Requested Action – Description of actions required by the EMPI Lead

To the EMPI Lead*: Please review the client/patient demographic information mentioned below and confirm, add or amend the data according to the action required and re-submit the assessment to IAR.*

Data Element	**Action Required**	**Data Element**	**Action Required**
Last Name	Confirm/Amend	Date of Birth	Confirm/Amend
First name		Gender	
Middle Name		Phone Number	
Healthcard Number		Address	

Please DO NOT reply to the EDS team with any Personal Health Information. The indicated information above is for you to review, confirm and/or amend at your organization. You are not to communicate this information back to the EDS team.

4. Recommended Best Practices

Refer to the IAR EMPI business process document for more information (provided by CCIM)

5. Resolution – EMPI Lead, please provide a brief description of how the above has been resolved or the plan to be resolved

Please DO NOT include any actual client data or personal health information in your resolution description.

Date Resolved (dd/mm/yyyy)	Date Sent to EDS (dd/mm/yyyy)

If you have any questions, please contact the IAR Support Desk at 1-866-909-5600 option 8

Appendix B – Potential Duplicate Notification

IAR System Data Quality Inquiry ***Potential Duplicate***		
1. Contact Information		
Name of EMPI Lead:	Organization Number:	Date of Notification (dd/mm/yyyy)
2. Client/Patient Information:		
Local Client Identifier:		
Date Identified (dd/mm/yyyy)	Date Reviewed by EDS (dd/mm/yyyy)	
3. Requested Action – Description of actions required by the EMPI Lead		
Potential duplication is found for the following two (2) Local Client Identification numbers. ***Please compare these two Local Client Identification numbers:*** ▪ ________________________________ ▪ ________________________________ *If the two records refer to the same client, please resolve the duplication.* *It is recommended the client be referenced by a single Local Identifier (eg. Chart Number or Medical Record Number - MRN)*		
4. Recommended Best Practices		
Refer to the IAR EMPI business process document for more information (provided by CCIM)		
5. Resolution– EMPI Lead, please provide a brief description of how the above have been resolved or plan to be resolved		
Please DO NOT include any actual client data or personal health information in your resolution description.		
Date Resolved (dd/mm/yyyy)	Date Sent to EDS (dd/mm/yyyy)	

If you have any questions, please contact the IAR Support Desk at
1-866-909-5600 option 8

Appendix C – Potential Overlay – Critical Alert

IAR System Data Quality Inquiry

Potential Overlay – Critical Alert

1. Contact Information

Name of EMPI Lead:	Organization Number:	Date of Notification (dd/mm/yyyy)

2. Client/Patient Information:

Local Client Identifier:

Date Identified (dd/mm/yyyy)	Date Reviewed by EDS (dd/mm/yyyy)

3. Requested Action – Description of actions required by the EMPI Lead

There is a potential overlay with the above mentioned client, please review the following:

- Significant changes have been made to the following data ***marked with an*** **X** --
- Please confirm a second, different patient has not been inadvertently attached to the Local Client Identifier referenced above.
- The EDS resource may be contacted via telephone in order to obtain the "before" and "after" demographic data elements.
- Please phone <*insert EDS name*> at 519-____ - __________

Data Element	**Review Marked Data Elements**	**Data Element**	**Review Marked Data Elements**
Last Name		Date of Birth	
First name		Gender	
Middle Name		Phone Number	
Healthcard Number		Address	

Please DO NOT reply to the EDS team with any Personal Health Information. The indicated information above is for you to review, confirm and/or amend at your organization. You are not to communicate this information back to the EDS team.

4. Recommended Best Practices

Refer to the IAR EMPI business process document for more information (provided by CCIM)

5. Resolution – EMPI Lead, please provide a brief description of how the above has been resolved or the plan to be resolved

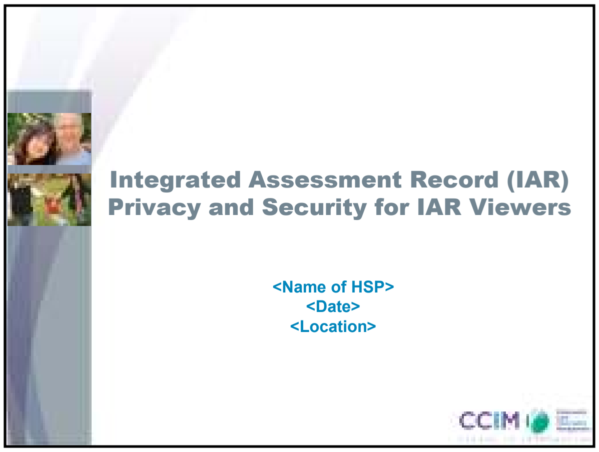
Please DO NOT include any actual client data or personal health information in your resolution description.

Date Resolved (dd/mm/yyyy)	Date Sent to EDS (dd/mm/yyyy)

If you have any questions, please contact the IAR Support Desk at
1-866-909-5600 option 8

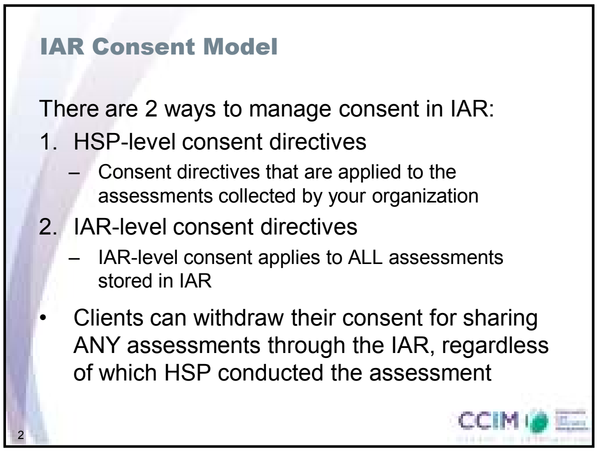
EMPI Process Implementation Checklist

Ref. No.	Implementation Task	Action Plan	Status
1	Identify a person to be the Health Record Lead for the EMPI Data Steward to contact to inform about data element issues or errors.		
2	Develop a high-level process for the Health Record Lead to work with clinicians or case workers to resolve any data quality or data element issues detected by EMPI.		
3	Develop Process updating / correction of Client / Patient Records		
4	Review process for re-upload assessment or Coordinated Care Plans once data quality or data element issues are resolved.		
5	Provide Health Record Lead contact information for EMPI Data Steward		
6	Arrange to have the Health Record Lead trained on the EMPI HSP process		



Integrated Assessment Record (IAR) Privacy and Security for IAR Viewers

<Name of HSP>
<Date>
<Location>

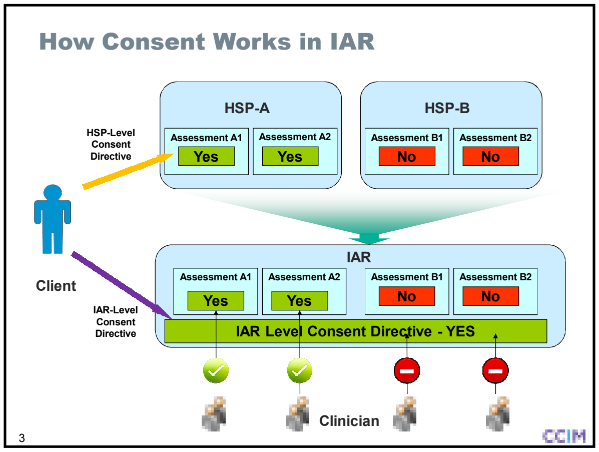


IAR Consent Model

There are 2 ways to manage consent in IAR:

1. HSP-level consent directives
   - Consent directives that are applied to the assessments collected by your organization
2. IAR-level consent directives
   - IAR-level consent applies to ALL assessments stored in IAR

- Clients can withdraw their consent for sharing ANY assessments through the IAR, regardless of which HSP conducted the assessment



How Consent Works in IAR

HSP-A

Assessment A1	Assessment A2
Yes	Yes

HSP-B

Assessment B1	Assessment B2
No	No

HSP-Level Consent Directive

Client

IAR-Level Consent Directive

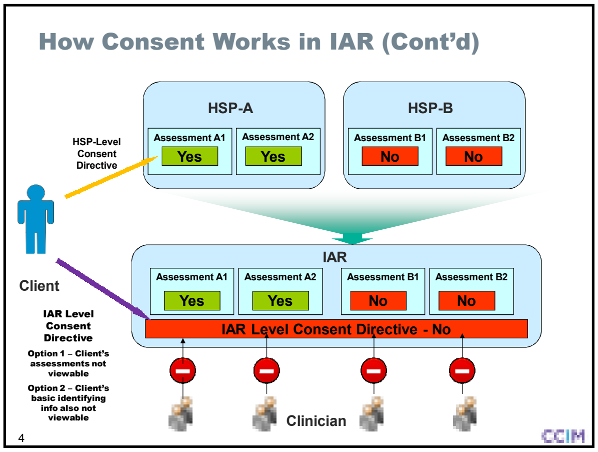
IAR

Assessment A1	Assessment A2	Assessment B1	Assessment B2
Yes	Yes	No	No

IAR Level Consent Directive - YES

✓ ✓ ⊖ ⊖

Clinician



How Consent Works in IAR (Cont'd)

HSP-A

Assessment A1	Assessment A2
Yes	Yes

HSP-B

Assessment B1	Assessment B2
No	No

HSP-Level Consent Directive

Client

IAR Level Consent Directive

Option 1 – Client's assessments not viewable

Option 2 – Client's basic identifying info also not viewable

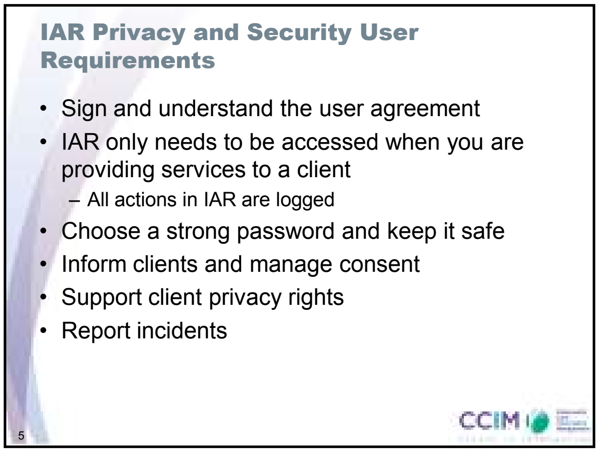
IAR

Assessment A1	Assessment A2	Assessment B1	Assessment B2
Yes	Yes	No	No

IAR Level Consent Directive - No

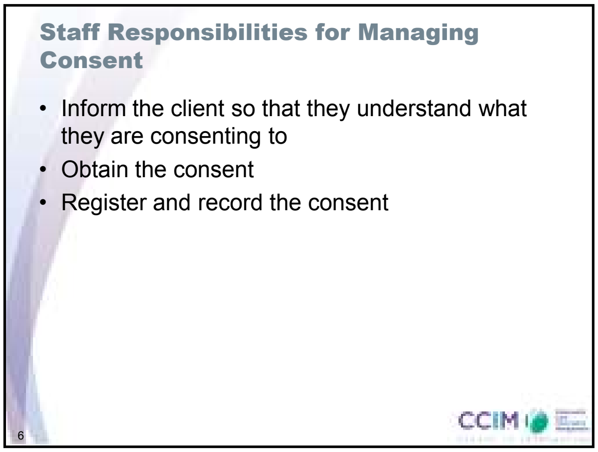
⊖ ⊖ ⊖ ⊖

Clinician



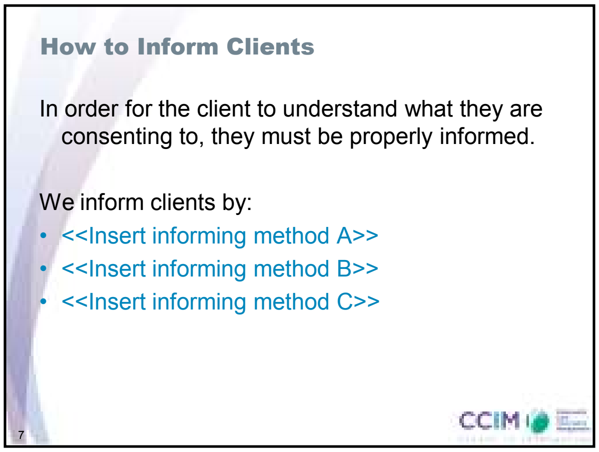
IAR Privacy and Security User Requirements

- Sign and understand the user agreement
- IAR only needs to be accessed when you are providing services to a client
  - All actions in IAR are logged
- Choose a strong password and keep it safe
- Inform clients and manage consent
- Support client privacy rights
- Report incidents



Staff Responsibilities for Managing Consent

- Inform the client so that they understand what they are consenting to
- Obtain the consent
- Register and record the consent

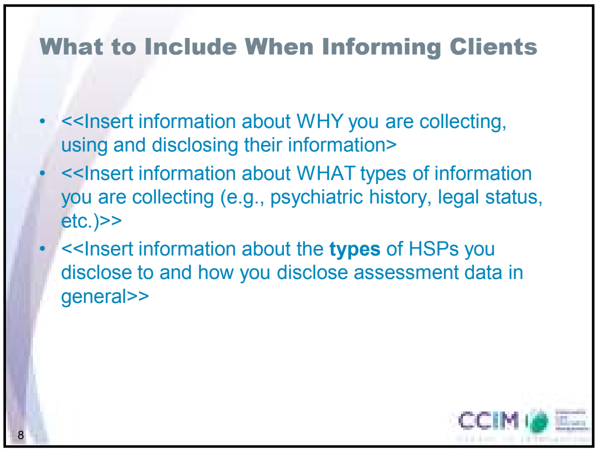


How to Inform Clients

In order for the client to understand what they are consenting to, they must be properly informed.

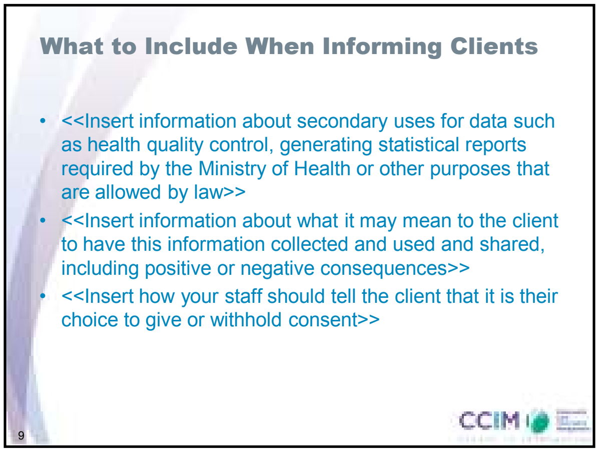
We inform clients by:

- <<Insert informing method A>>
- <<Insert informing method B>>
- <<Insert informing method C>>



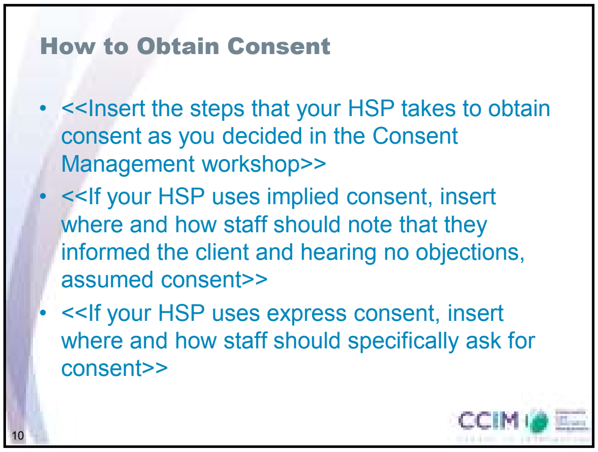
What to Include When Informing Clients

- <<Insert information about WHY you are collecting, using and disclosing their information>
- <<Insert information about WHAT types of information you are collecting (e.g., psychiatric history, legal status, etc.)>>
- <<Insert information about the **types** of HSPs you disclose to and how you disclose assessment data in general>>



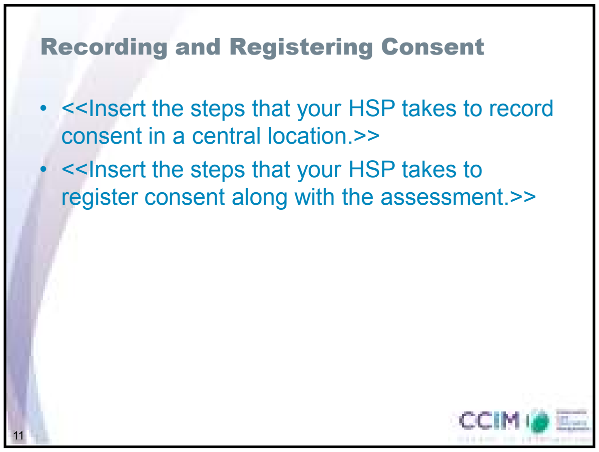
What to Include When Informing Clients

- <<Insert information about secondary uses for data such as health quality control, generating statistical reports required by the Ministry of Health or other purposes that are allowed by law>>
- <<Insert information about what it may mean to the client to have this information collected and used and shared, including positive or negative consequences>>
- <<Insert how your staff should tell the client that it is their choice to give or withhold consent>>



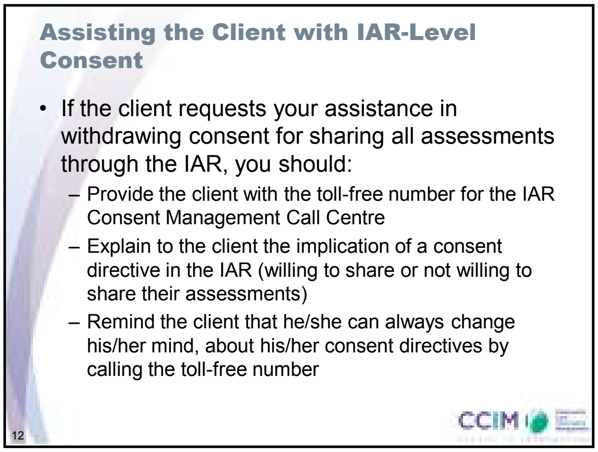
How to Obtain Consent

- <<Insert the steps that your HSP takes to obtain consent as you decided in the Consent Management workshop>>
- <<If your HSP uses implied consent, insert where and how staff should note that they informed the client and hearing no objections, assumed consent>>
- <<If your HSP uses express consent, insert where and how staff should specifically ask for consent>>



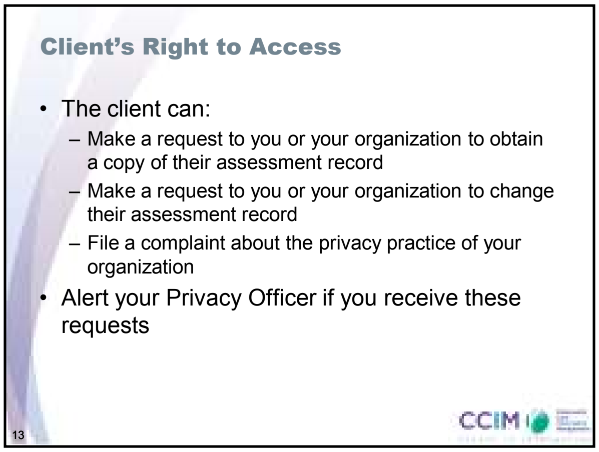
Recording and Registering Consent

- <<Insert the steps that your HSP takes to record consent in a central location.>>
- <<Insert the steps that your HSP takes to register consent along with the assessment.>>



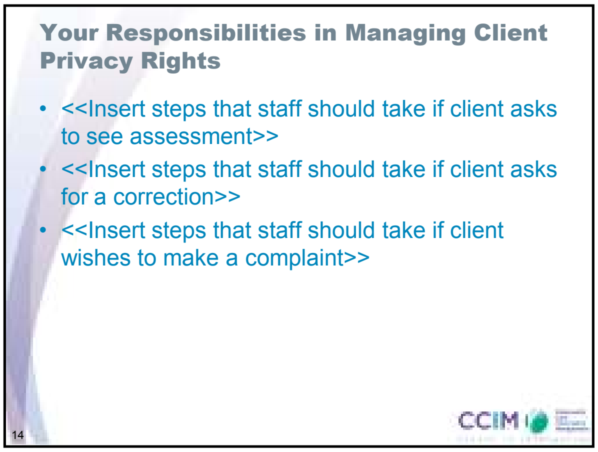
Assisting the Client with IAR-Level Consent

- If the client requests your assistance in withdrawing consent for sharing all assessments through the IAR, you should:
  - Provide the client with the toll-free number for the IAR Consent Management Call Centre
  - Explain to the client the implication of a consent directive in the IAR (willing to share or not willing to share their assessments)
  - Remind the client that he/she can always change his/her mind, about his/her consent directives by calling the toll-free number



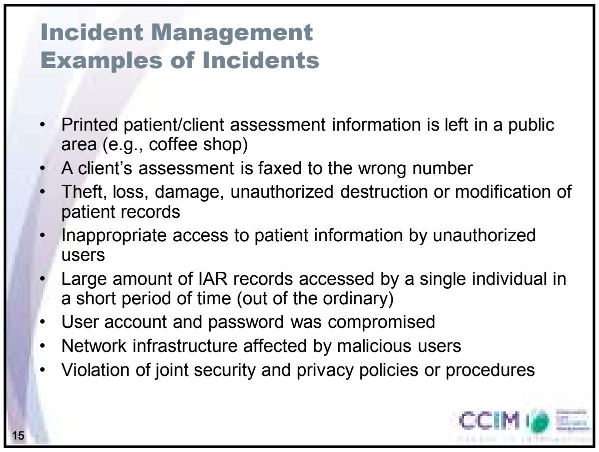
Client's Right to Access

- The client can:
  - Make a request to you or your organization to obtain a copy of their assessment record
  - Make a request to you or your organization to change their assessment record
  - File a complaint about the privacy practice of your organization
- Alert your Privacy Officer if you receive these requests



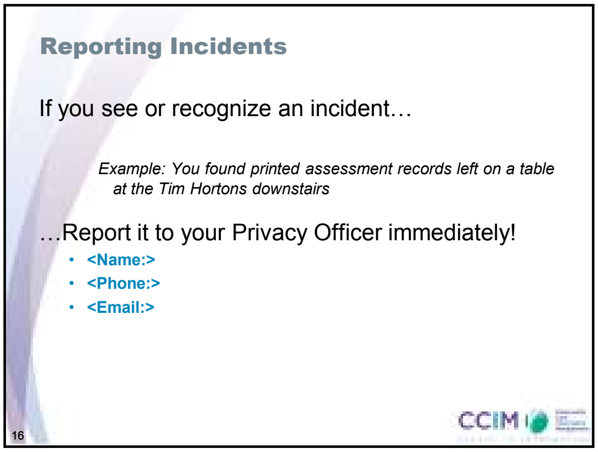
Your Responsibilities in Managing Client Privacy Rights

- <<Insert steps that staff should take if client asks to see assessment>>
- <<Insert steps that staff should take if client asks for a correction>>
- <<Insert steps that staff should take if client wishes to make a complaint>>



Incident Management Examples of Incidents

- Printed patient/client assessment information is left in a public area (e.g., coffee shop)
- A client's assessment is faxed to the wrong number
- Theft, loss, damage, unauthorized destruction or modification of patient records
- Inappropriate access to patient information by unauthorized users
- Large amount of IAR records accessed by a single individual in a short period of time (out of the ordinary)
- User account and password was compromised
- Network infrastructure affected by malicious users
- Violation of joint security and privacy policies or procedures



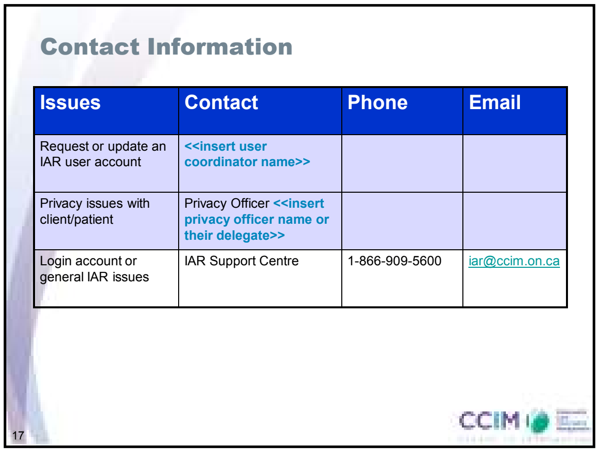
Reporting Incidents

If you see or recognize an incident…

Example: You found printed assessment records left on a table at the Tim Hortons downstairs

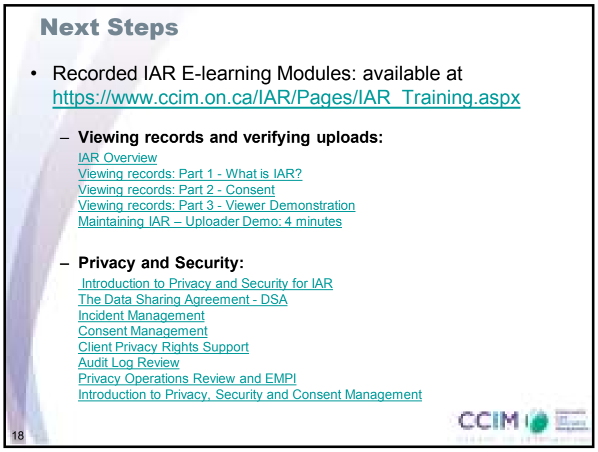
…Report it to your Privacy Officer immediately!

- **<Name:>**
- **<Phone:>**
- **<Email:>**



Contact Information

Issues	Contact	Phone	Email
Request or update an IAR user account	**<<insert user coordinator name>>**		
Privacy issues with client/patient	Privacy Officer **<<insert privacy officer name or their delegate>>**		
Login account or general IAR issues	IAR Support Centre	1-866-909-5600	iar@ccim.on.ca



Next Steps

- Recorded IAR E-learning Modules: available at https://www.ccim.on.ca/IAR/Pages/IAR_Training.aspx
  - **Viewing records and verifying uploads:**

    IAR Overview
    Viewing records: Part 1 - What is IAR?
    Viewing records: Part 2 - Consent
    Viewing records: Part 3 - Viewer Demonstration
    Maintaining IAR – Uploader Demo: 4 minutes

  - **Privacy and Security:**

    Introduction to Privacy and Security for IAR
    The Data Sharing Agreement - DSA
    Incident Management
    Consent Management
    Client Privacy Rights Support
    Audit Log Review
    Privacy Operations Review and EMPI
    Introduction to Privacy, Security and Consent Management