RM&R Privacy Training
Full Package for HIC Privacy Officers

Content

Topics	
1	RM&R Overview
2	Privacy and Security Program Overview
3	Supporting Patients in Meeting Their Privacy Rights
4	Assurance
5	Handling PHI Securely
6	Privacy Breach Management

Definitions

Personal Health Information (PHI)

- Defined in PHIPA as identifiable health information about an Individual
- PHI includes information such as diagnoses, provider name, or SDM information
- Everything in the RM&R System that is related to an identifiable Individual is PHI, including information found in audit logs, reports, or bug reports
- Any information about an identifiable patient or SDM in forms or reports (e.g., Privacy Breach Report, Request for Access to the patient's own PHI)

Health Information Custodian (HIC)

- A health care organization that contributed PHI for the purpose of health care
- HICs have authority and accountability over the PHI
- Also have the relevant PHIPA responsibilities for PHI they collect for health care purposes by viewing PHI contributed by other organizations

Agent

- Acts under the authority of the HIC for the purposes established by the HIC
- An agent of an organization has the authority to view or handle PHI according to the organization's policies and procedures

Definitions (cont'd)

Health Information Network Provider (HINP)

- A person (or organization) who provides services to two or more health information custodians where the services are provided primarily to enable the custodians to use electronic means to disclose personal health information to one another

Disclosure

- A HIC that contributes PHI discloses it to the HIC that views it (when it is viewed)

Collection

- A HIC that views PHI collects it from the HIC that discloses it (when it first views the PHI)

Use

- A HIC that views PHI that it previously collected or that views PHI it contributed

Consent Directive

- Colloquially called a “lockbox”, a consent directive is a patient instruction about how an organization may manage that patient’s PHI

RM&R Overview

RM&R… because we need to know

Resource Matching & Referral (RM&R) is a shared web-based application that matches patients to appropriate clinical programs/services and sends electronic referrals. The application is currently live in 80 acute, rehabilitation, complex continuing care, home care, long-term care and community support health service providers in Toronto Central and Central LHINs. It was introduced in Toronto Central LHIN in 2008 and in Central LHIN as of 2011.

By creating a centralized tool, the RM&R application, allows Health Service Providers to match patients to the most appropriate programs and services in a timely manner. It also provides clear methods to identify capacity issues and service gaps. Lastly, the RM&R application is a single repository of information used by Health Service Providers to improve the patient experience.

RM&R – By the Numbers

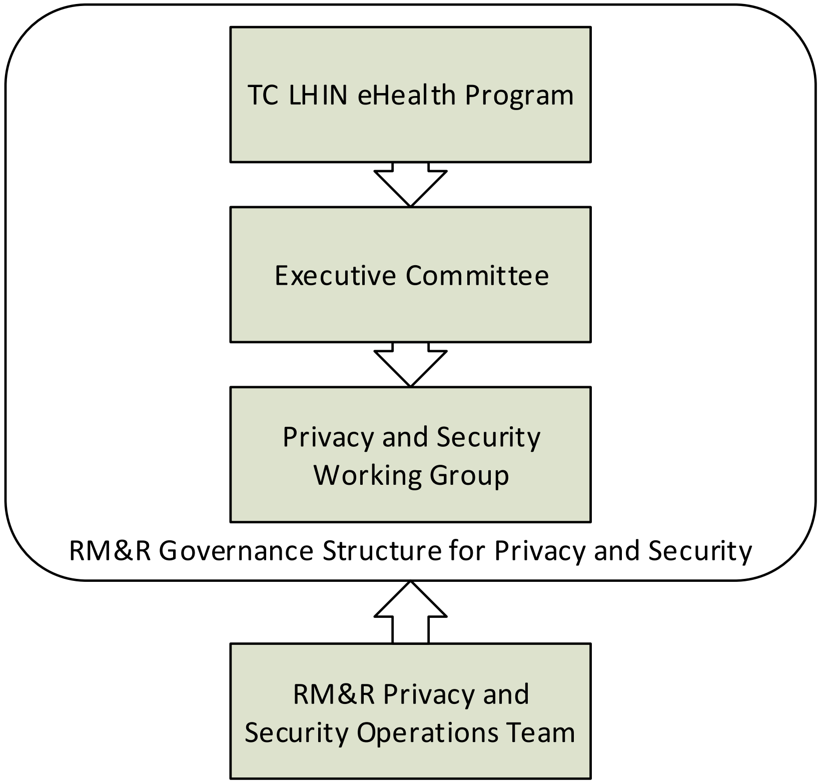
- **80** Participating Organizations

- **24,000+** Registered users
- **~500,000** referrals sent since 2009
- **~6000** Long-Term Care Beds for Patient Matching

*Patients identified using unique MRN or CHRIS numbers

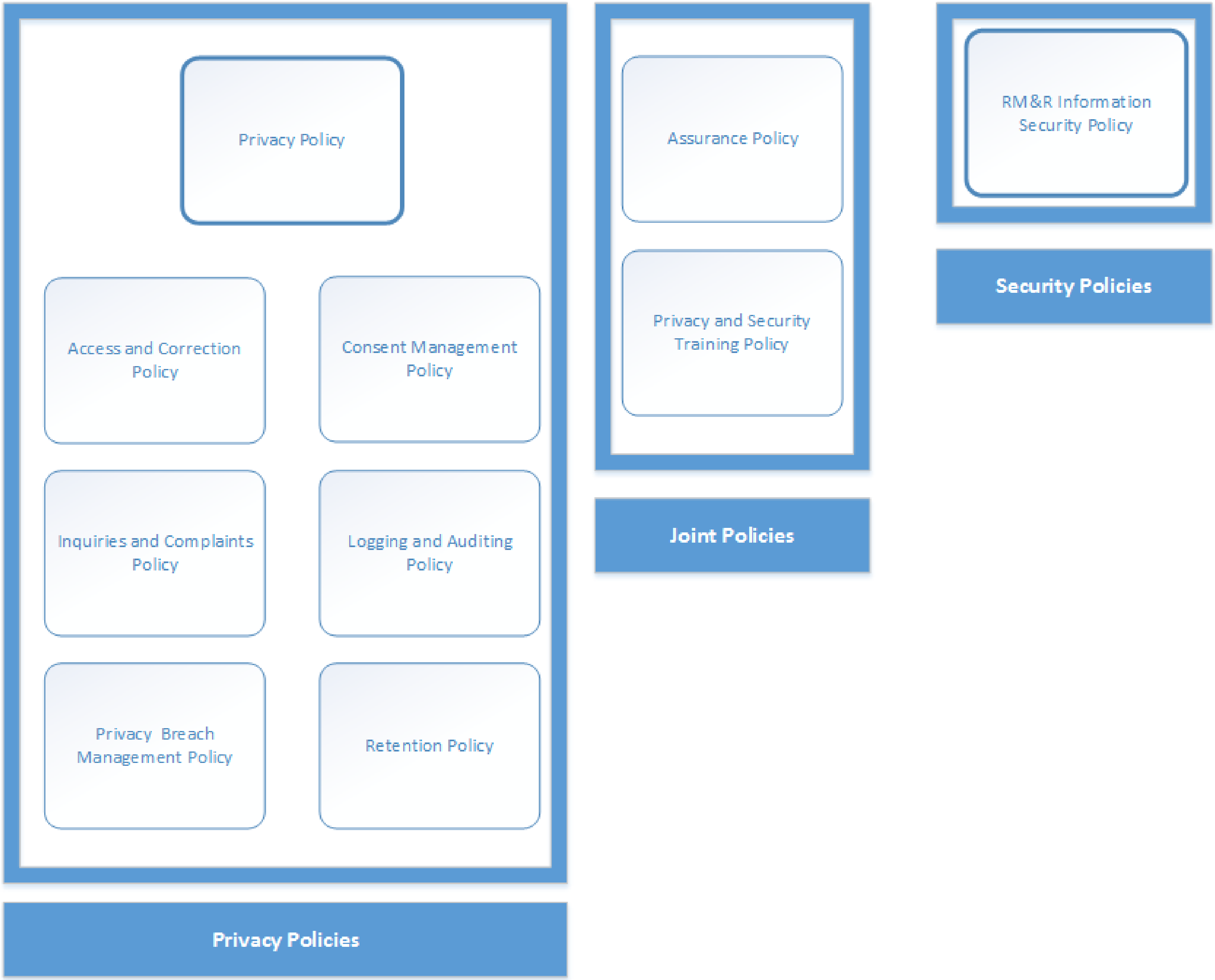
RM&R Privacy and Security Program

Privacy and Security Governance


TC LHIN eHealth Program
Executive Committee
Privacy and Security Working Group
RM&R Governance Structure for Privacy and Security
RM&R Privacy and Security Operations Team

- **RM&R Executive Committee**
  Overall accountability for the RM&R initiative
- **Privacy and Security Working Group**
  Reports to the RM&R Executive Committee and supports management of tactical operational planning and issues management
- **Privacy and Security Operations Team**
  Responsible for the day-to-day operations of RM&R's privacy and security programs, and supporting the Privacy and Security Working Group

Privacy and Security Policies



Privacy Policy

Access and Correction Policy

Consent Management Policy

Inquiries and Complaints Policy

Logging and Auditing Policy

Privacy Breach Management Policy

Retention Policy

Privacy Policies

Assurance Policy

Privacy and Security Training Policy

Joint Policies

RM&R Information Security Policy

Security Policies

Privacy Operations

What are Privacy Operations?

- Activities conducted by HICs and RM&R related to supporting Individual privacy rights or managing the privacy program (e.g., assurance)
- They are guided by the RM&R Privacy Policies

What are RM&R's privacy objectives?

- Individuals (i.e., patients or their SDMs) have a streamlined experience when exercising their privacy rights
- HICs and RM&R work together to protect privacy

Operational Privacy and Security Manual

The manual includes operational processes, policies, governance, and an overview of the RM&R Privacy and Security Program.

The manual will be updated from time to time. The most up-to-date version of the manual will be available on the RM&R Website

What should you do if you get a privacy request related to RM&R?

- Review the summary of the relevant policy in Section 4 of the *RM&R Operational Privacy and Security Manual* to orient yourself
- Review the associated flowcharts in Section 4 of the manual to assist you in understanding the key process steps
- Read the relevant section of the policies in Section 5 of the manual to understand the detailed obligations
- Use the required forms in section 6 of the manual to exchange information with RM&R

Privacy and Security Safeguards

Administrative

- Appointed Privacy and Security Leads
- Privacy and Security Working Group to oversee operational activities
- Public communications regarding the Program
- Privacy and security training
- Agreements with agents and electronic service providers
- Privacy and security policies
- Operating procedures and practices established in privacy and security policies
- Conducted PIAs and TRAs

Physical

- Physically controlled access to servers and networking equipment
- PHI in a secure and redundant data centre
- Formalized processes and procedures for the disposal and replacement of hardware

Technical

- Logical access controls
- Additional authentication mechanisms for system administrators and others with privileged access
- Encryption when data is in transit and at rest
- Vulnerability and patch management
- Formal change management and testing procedures
- Protection against anti-virus and malware
- Secure, offsite backups
- Logging and auditing capabilities
- Intrusion detection and alerting
- Operational monitoring of services for performance and integrity

Permitted Purposes for Collection, Use, and Disclosure of PHI in the RM&R System

Participating HICs

- Collection: providing or assisting in the provision of health care (authority is based on consent)
- Use & Disclosure: providing health care or assisting in the provision of health care, implementation and maintenance of the application

UHN

UHN plays multiple roles that are established through PHIPA and RM&R Agreements:

1. HINP: providing information technology services to enable HICs to use electronic means to disclose PHI to one another and to procure (including identifying specifications for technology products and services and enforcing the obligations of the ESPs)
2. Agent: when handling PHI in the System for which another HIC is the custodian or when supporting the processing of requests from patients associated with PHI that another HIC contributed (e.g., access request, consent directive management)
3. HIC: collection, use and disclosure, as above, for the purpose of providing health care or assisting in the provision of health care when acting as a participating site

Supporting Patients in Exercising Their Privacy Rights

Patient Privacy Rights

What are the Individual privacy rights that you will support as an RM&R Participating Site CPO?

1. **Consent** - Provide or withdraw consent (for health care purposes)
2. **Request for Access** - View PHI that a HIC holds
3. **Request for Correction** - Ask to correct PHI if it is incomplete, inaccurate, or out-of-date
4. **Inquiries** – Ask a question about information handling practices and privacy
5. **Complaints** – Make a complaint about the information handling practices and privacy

Note: RM&R policies and procedures help HICs meet those obligations with respect to RM&R. They do not replace the internal privacy program, but augment it to ensure effective coordination where an issue relates to more than one HIC.

Important!

When in doubt:

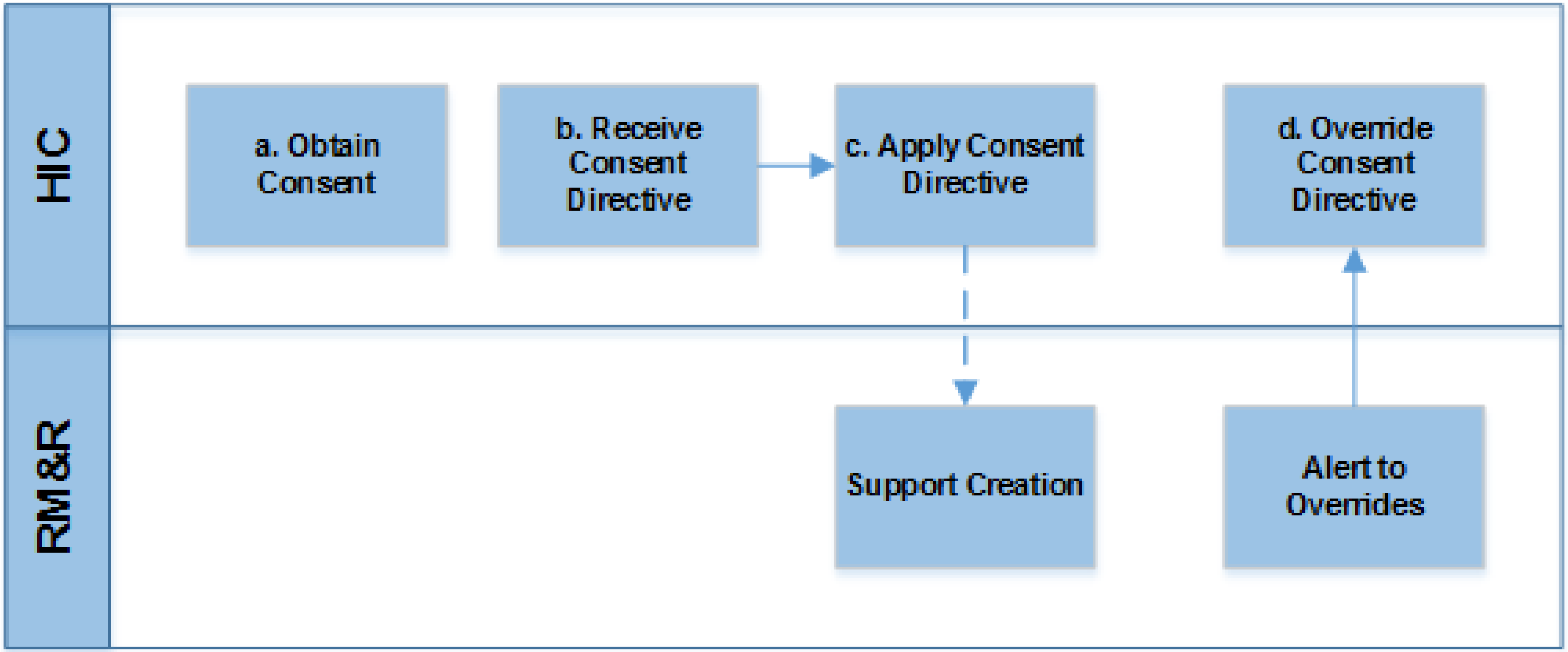
- **First consult the RM&R *Operational Privacy and Security Manual***
- **If you still have questions, email: rmr_program@uhn.ca**

Consent – Overview

What are the HIC’s obligations in consent?

- Obtain consent
- Receive and process Consent Directives
- Override Consent Directives only in appropriate circumstances
- Follow-up on Consent Directives overrides

Consent – Process Summary


HIC
RM&R
a. Obtain Consent
b. Receive Consent Directive
c. Apply Consent Directive
d. Override Consent Directive
Support Creation
Alert to Overrides

Consent – a. Obtaining Consent

- Collection, use, and disclosure in RM&R for health care purposes is consent based
- Any form of consent is acceptable (i.e., implied, express), but must be knowledgeable and meet policy standards
- “Layered approach” to notices is recommended
  - Existing notices likely meet the standards except maybe for requirement to communicate participation in shared electronic health networks
  - Provide more information about RM&R on request or direct the Individual to: www.resourcematchingandreferral.com

Consent – b. Receiving Consent Directives

Consent Directive Requests

Make

Modify

Remove

How do you receive Consent Directives?

1. Receive, Log and Document Consent Directives as usual (i.e., use your own forms)
2. Inform the Individual about the Impact of the Directive, and about how Consent Overrides work.

Important!

You are accountable for ensuring the Consent Directive is registered.

Consent – b. Receiving Consent Directives (cont'd)

What types of Consent Directives does the RM&R System support?

1. **Global** – Restricts access to all PHI in the RM&R System (except some demographic data used to identify the Individual in the system for the purpose of managing the individual's record) for all users of the system. The information can be viewed by overriding the consent directive restriction.

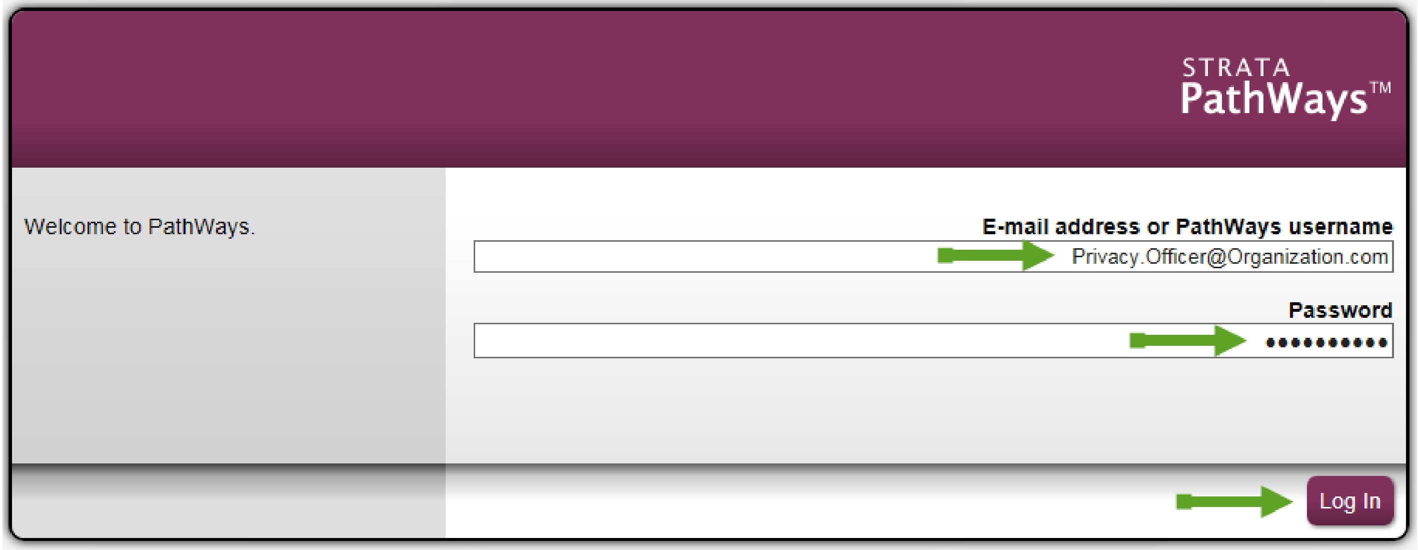
This is currently the only type of consent directive restriction available in RM&R.

Consent – c. Applying Consent Directives

What is the Process to apply Consent Directives?

1. Log that the request was made
2. Verify identity of the Individual or SDM (and authority if SDM)
3. Discuss the implications of creating a Consent Directive, when it can be overridden, and that the Individual can change their mind
4. Get contact information for the Individual
5. Apply the Consent Directive in the system as soon as possible. ***Note:*** *it must be within two business days of verifying the Individual's identity*
6. After applying the Consent Directive in the system, you must immediately tell the Individual that the request was implemented.

Consent – c. Applying the Consent Directive (cont'd) Logging In



STRATA PathWays™

Welcome to PathWays.

E-mail address or PathWays username

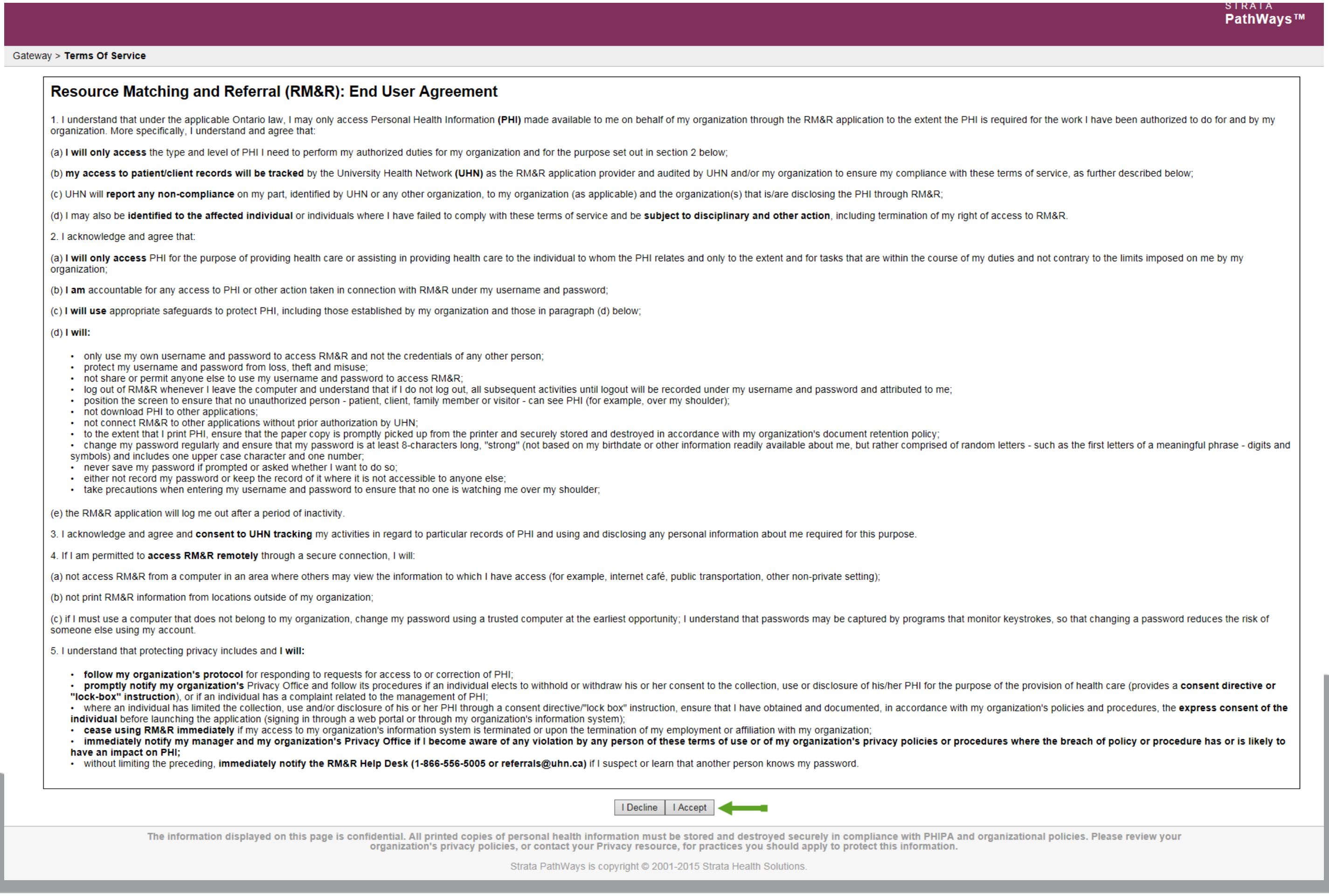
Privacy.Officer@Organization.com

Password

●●●●●●●●●●

Consent – c. Applying the Consent Directive (cont'd) First Time Logging In (and Annually Thereafter): ToS/EUA

1. Press the "I Agree" button to agree to the terms of the End User Agreement



Resource Matching and Referral (RM&R): End User Agreement

1. I understand that under the applicable Ontario law, I may only access Personal Health Information **(PHI)** made available to me on behalf of my organization through the RM&R application to the extent the PHI is required for the work I have been authorized to do for and by my organization. More specifically, I understand and agree that:

(a) **I will only access** the type and level of PHI I need to perform my authorized duties for my organization and for the purpose set out in section 2 below;

(b) **my access to patient/client records will be tracked** by the University Health Network **(UHN)** as the RM&R application provider and audited by UHN and/or my organization to ensure my compliance with these terms of service, as further described below;

(c) UHN will **report any non-compliance** on my part, identified by UHN or any other organization, to my organization (as applicable) and the organization(s) that is/are disclosing the PHI through RM&R;

(d) I may also be **identified to the affected individual** or individuals where I have failed to comply with these terms of service and be **subject to disciplinary and other action**, including termination of my right of access to RM&R.

2. I acknowledge and agree that:

(a) **I will only access** PHI for the purpose of providing health care or assisting in providing health care to the individual to whom the PHI relates and only to the extent and for tasks that are within the course of my duties and not contrary to the limits imposed on me by my organization;

(b) **I am** accountable for any access to PHI or other action taken in connection with RM&R under my username and password;

(c) **I will use** appropriate safeguards to protect PHI, including those established by my organization and those in paragraph (d) below;

(d) **I will:**

- only use my own username and password to access RM&R and not the credentials of any other person;
- protect my username and password from loss, theft and misuse;
- not share or permit anyone else to use my username and password to access RM&R;
- log out of RM&R whenever I leave the computer and understand that if I do not log out, all subsequent activities until logout will be recorded under my username and password and attributed to me;
- position the screen to ensure that no unauthorized person - patient, client, family member or visitor - can see PHI (for example, over my shoulder);
- not download PHI to other applications;
- not connect RM&R to other applications without prior authorization by UHN;
- to the extent that I print PHI, ensure that the paper copy is promptly picked up from the printer and securely stored and destroyed in accordance with my organization's document retention policy;
- change my password regularly and ensure that my password is at least 8-characters long, "strong" (not based on my birthdate or other information readily available about me, but rather comprised of random letters - such as the first letters of a meaningful phrase - digits and symbols) and includes one upper case character and one number;
- never save my password if prompted or asked whether I want to do so;
- either not record my password or keep the record of it where it is not accessible to anyone else;
- take precautions when entering my username and password to ensure that no one is watching me over my shoulder;

(e) the RM&R application will log me out after a period of inactivity.

3. I acknowledge and agree and **consent to UHN tracking** my activities in regard to particular records of PHI and using and disclosing any personal information about me required for this purpose.

4. If I am permitted to **access RM&R remotely** through a secure connection, I will:

(a) not access RM&R from a computer in an area where others may view the information to which I have access (for example, internet café, public transportation, other non-private setting);

(b) not print RM&R information from locations outside of my organization;

(c) if I must use a computer that does not belong to my organization, change my password using a trusted computer at the earliest opportunity; I understand that passwords may be captured by programs that monitor keystrokes, so that changing a password reduces the risk of someone else using my account.

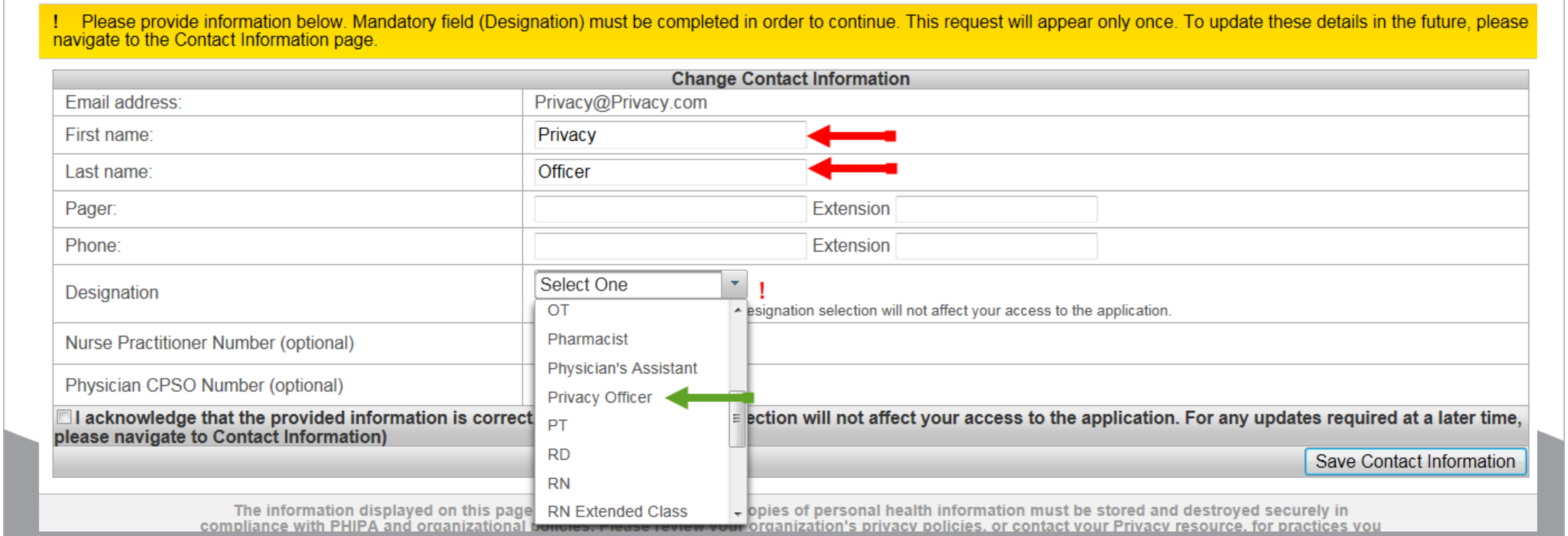
5. I understand that protecting privacy includes and **I will:**

- **follow my organization's protocol** for responding to requests for access to or correction of PHI;
- **promptly notify my organization's** Privacy Office and follow its procedures if an individual elects to withhold or withdraw his or her consent to the collection, use or disclosure of his/her PHI for the purpose of the provision of health care (provides a **consent directive or "lock-box" instruction**), or if an individual has a complaint related to the management of PHI;
- where an individual has limited the collection, use and/or disclosure of his or her PHI through a consent directive/"lock box" instruction, ensure that I have obtained and documented, in accordance with my organization's policies and procedures, the **express consent of the individual** before launching the application (signing in through a web portal or through my organization's information system);
- **cease using RM&R immediately** if my access to my organization's information system is terminated or upon the termination of my employment or affiliation with my organization;
- **immediately notify my manager and my organization's Privacy Office if I become aware of any violation by any person of these terms of use or of my organization's privacy policies or procedures where the breach of policy or procedure has or is likely to have an impact on PHI;**
- without limiting the preceding, **immediately notify the RM&R Help Desk (1-866-556-5005 or referrals@uhn.ca)** if I suspect or learn that another person knows my password.

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Consent – c. Applying the Consent Directive (cont'd) First Login: Review and Confirm Contact Information

1. Confirm that your name and email address are correct
2. Update "Designation" field to "**Privacy Officer**"
3. Acknowledge the disclaimer about your contact information
4. Press: "Save Contact Information" button



! Please provide information below. Mandatory field (Designation) must be completed in order to continue. This request will appear only once. To update these details in the future, please navigate to the Contact Information page.

Change Contact Information

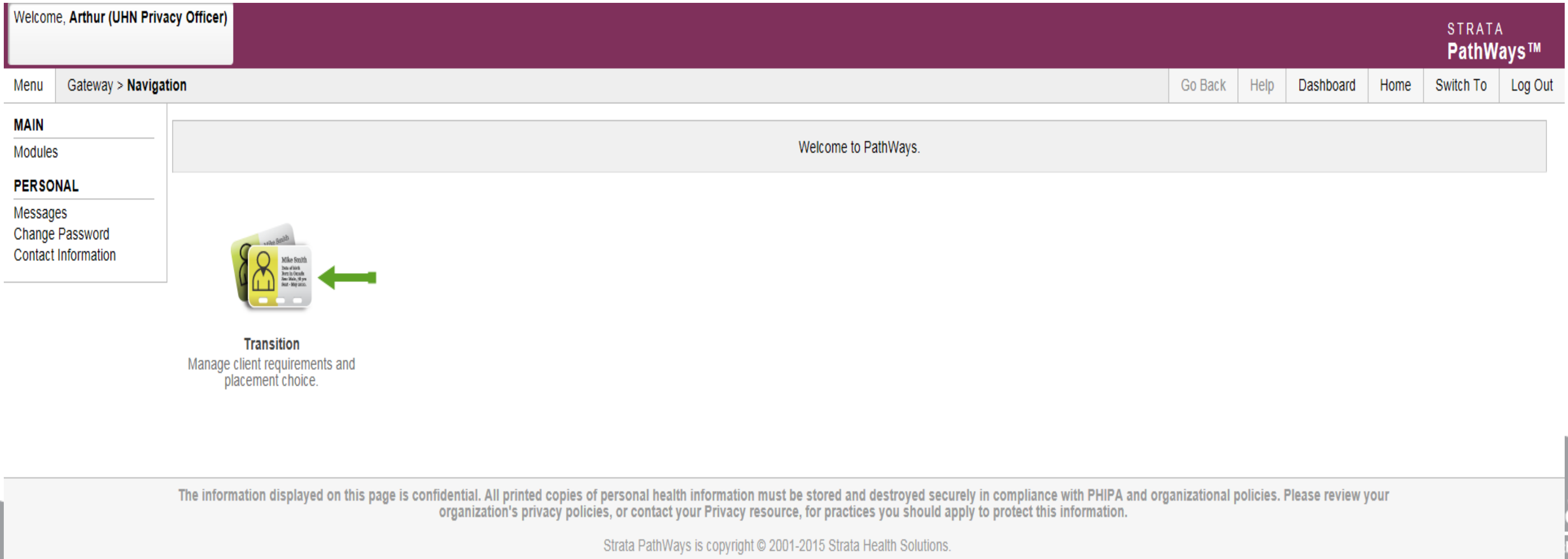
Email address:	Privacy@Privacy.com
First name:	Privacy
Last name:	Officer
Pager:	Extension
Phone:	Extension
Designation	Select One ! esignation selection will not affect your access to the application.
Nurse Practitioner Number (optional)	
Physician CPSO Number (optional)	

□ **I acknowledge that the provided information is correct ection will not affect your access to the application. For any updates required at a later time, please navigate to Contact Information)**

The information displayed on this page opies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you

Consent – c. Applying the Consent Directive (cont'd) Select "Transition" Module

- The "Transition" module will be your only option when logged in as a Privacy Officer
- If you use RM&R in other capacities (i.e., if you are also a clinician that uses RM&R to provide health care, or in another role that otherwise supports the provision of health care), a separate account will be created for you that you should use when acting in the other role



Welcome to PathWays.

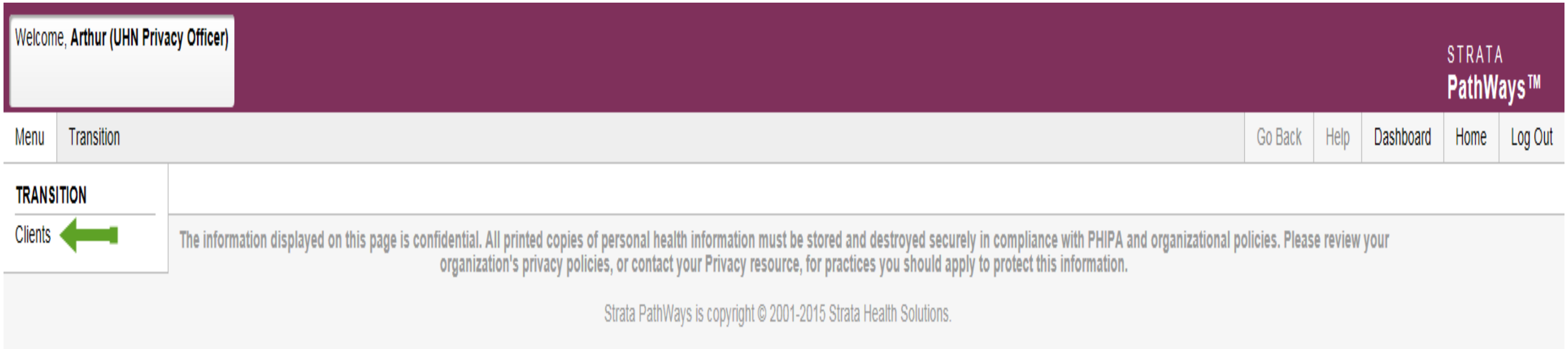
Manage client requirements and placement choice.

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent – c. Applying the Consent Directive (cont'd)
Choose Clients

- "Clients" will be your only option in the Transition module, unless you use RM&R in other capacities and have logged in using your separate account for the role (i.e., if you are also a clinician that uses RM&R to provide health care, or in another role that otherwise supports the provision of health care)



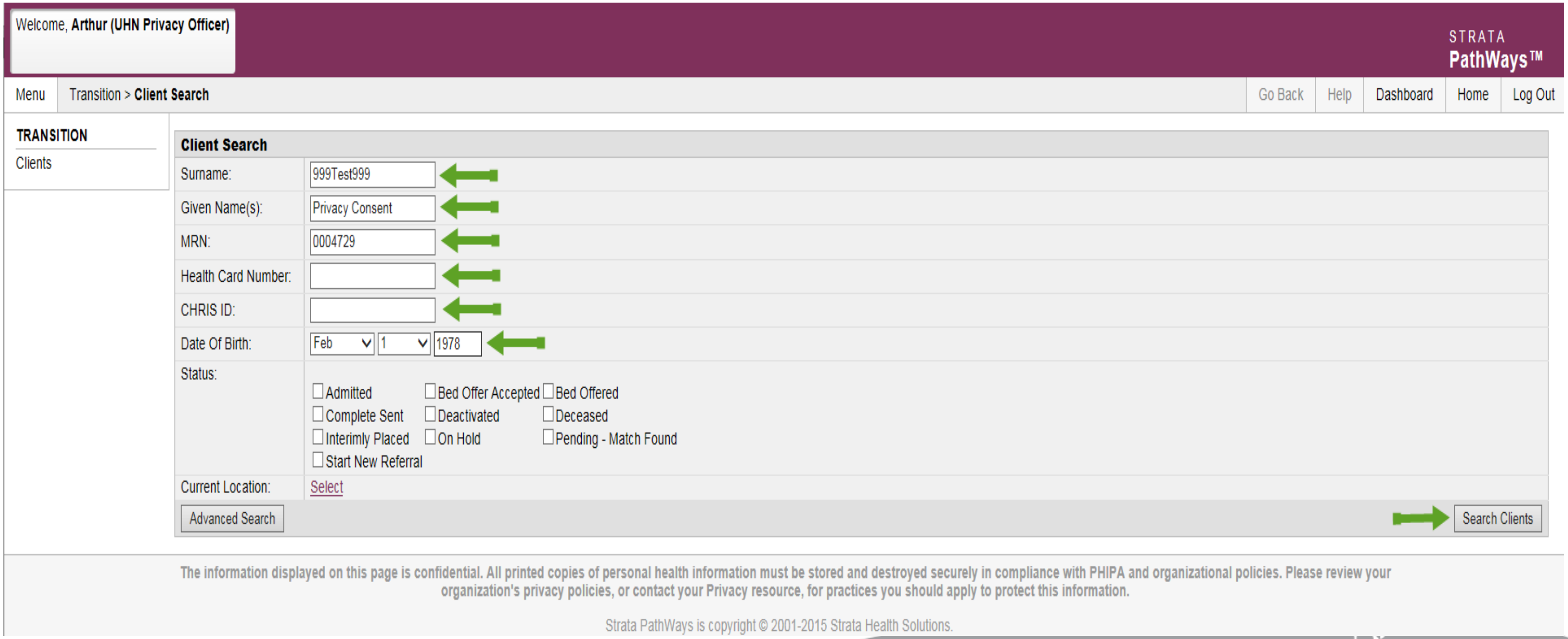
The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Toronto Central LHIN

Consent – c. Applying the Consent Directive (cont’d)Find Patient Record

1. Search by any one of the identified fields and choose the correct patient record



Welcome, Arthur (UHN Privacy Officer)

STRATA PathWays™

Menu | Transition > Client Search | Go Back | Help | Dashboard | Home | Log Out

TRANSITION

Clients

Client Search

Surname:	999Test999
Given Name(s):	Privacy Consent
MRN:	0004729
Health Card Number:	
CHRIS ID:	
Date Of Birth:	Feb 1 1978
Status:	□ Admitted □ Bed Offer Accepted □ Bed Offered □ Complete Sent □ Deactivated □ Deceased □ Interimly Placed □ On Hold □ Pending - Match Found □ Start New Referral
Current Location:	Select

Advanced Search | Search Clients

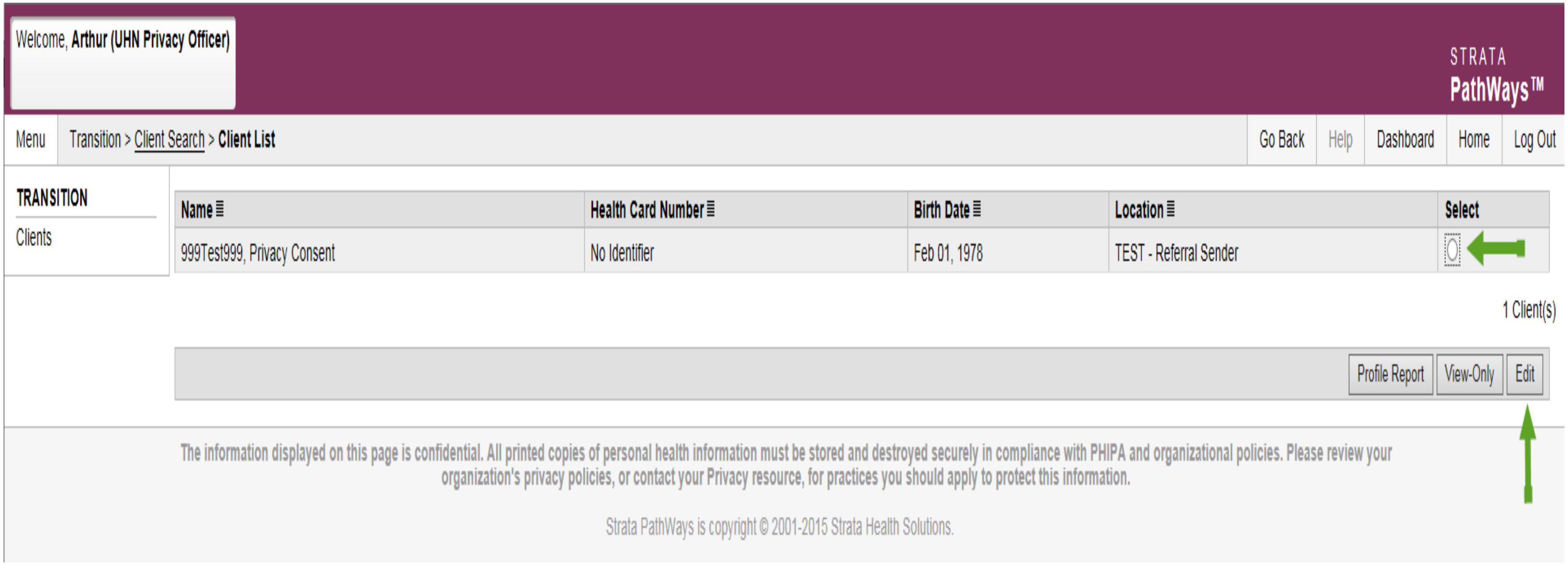
The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Ontario
Local Health Integration Network

Consent – c. Applying the Consent Directive (cont’d) Select Patient Record

1. Select the radio-button for the correct patient record
2. Press the “Edit” button



Welcome, **Arthur (UHN Privacy Officer)**

Transition > Client Search > **Client List**

TRANSITION

Clients

Name	Health Card Number	Birth Date	Location	Select
999Test999, Privacy Consent	No Identifier	Feb 01, 1978	TEST - Referral Sender	○

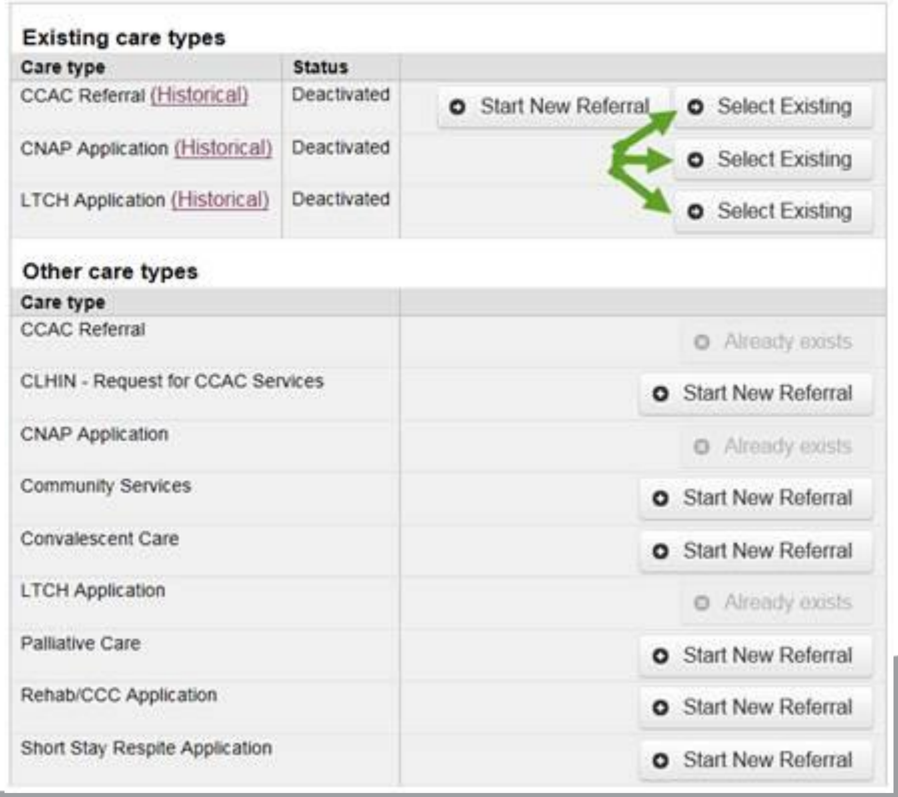
1 Client(s)

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent – c. Applying the Consent Directive (cont'd) Choose Referral

1. Press the "Select Existing" button for any one of the **existing** care types (Do NOT start a new referral)



Existing care types

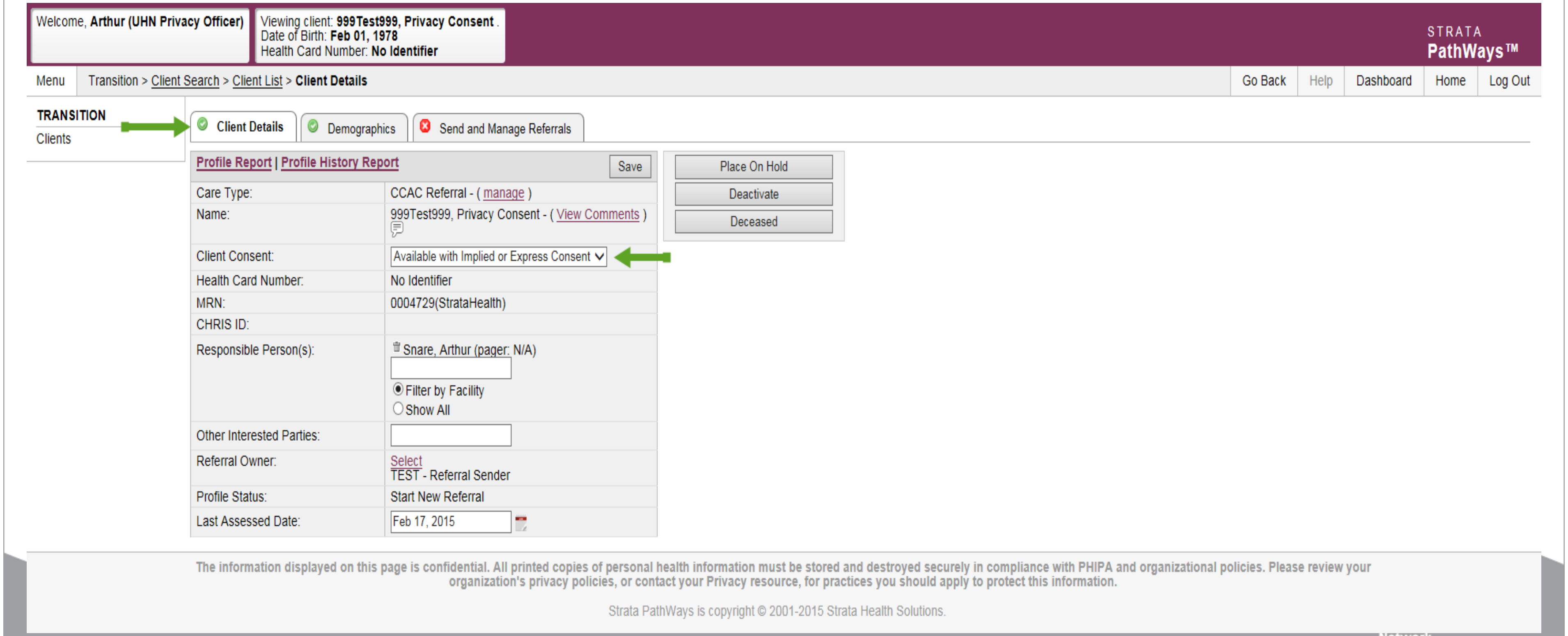
Care type	Status		
CCAC Referral (Historical)	Deactivated	● Start New Referral	● Select Existing
CNAP Application (Historical)	Deactivated		● Select Existing
LTCH Application (Historical)	Deactivated		● Select Existing

Other care types

Care type	
CCAC Referral	○ Already exists
CLHIN - Request for CCAC Services	● Start New Referral
CNAP Application	○ Already exists
Community Services	● Start New Referral
Convalescent Care	● Start New Referral
LTCH Application	○ Already exists
Palliative Care	● Start New Referral
Rehab/CCC Application	● Start New Referral
Short Stay Respite Application	● Start New Referral

Consent – c. Applying the Consent Directive (cont'd) Apply Consent Directive Instruction

1. Choose the "Client Details" tab
2. Select a Consent Directive option from the "Client Consent" dropdown list



Welcome, **Arthur (UHN Privacy Officer)**

Viewing client: **999Test999, Privacy Consent**
Date of Birth: **Feb 01, 1978**
Health Card Number: **No Identifier**

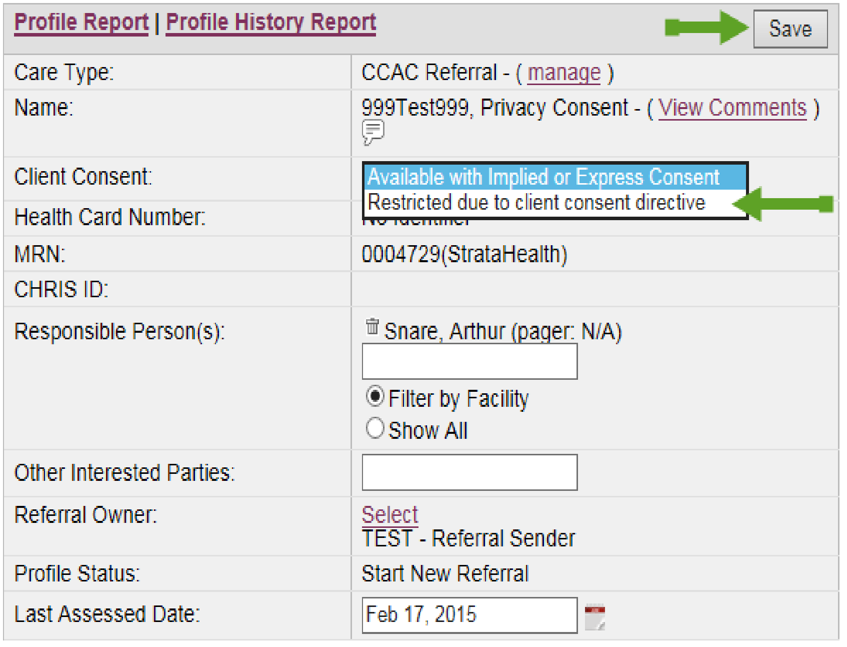
Care Type:	CCAC Referral - (manage)
Name:	999Test999, Privacy Consent - (View Comments)
Client Consent:	Available with Implied or Express Consent
Health Card Number:	No Identifier
MRN:	0004729(StrataHealth)
CHRIS ID:	
Responsible Person(s):	Snare, Arthur (pager: N/A) ● Filter by Facility ○ Show All
Other Interested Parties:	
Referral Owner:	Select TEST - Referral Sender
Profile Status:	Start New Referral
Last Assessed Date:	Feb 17, 2015

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent – c. Applying the Consent Directive (cont'd) Choose Consent Directive Option

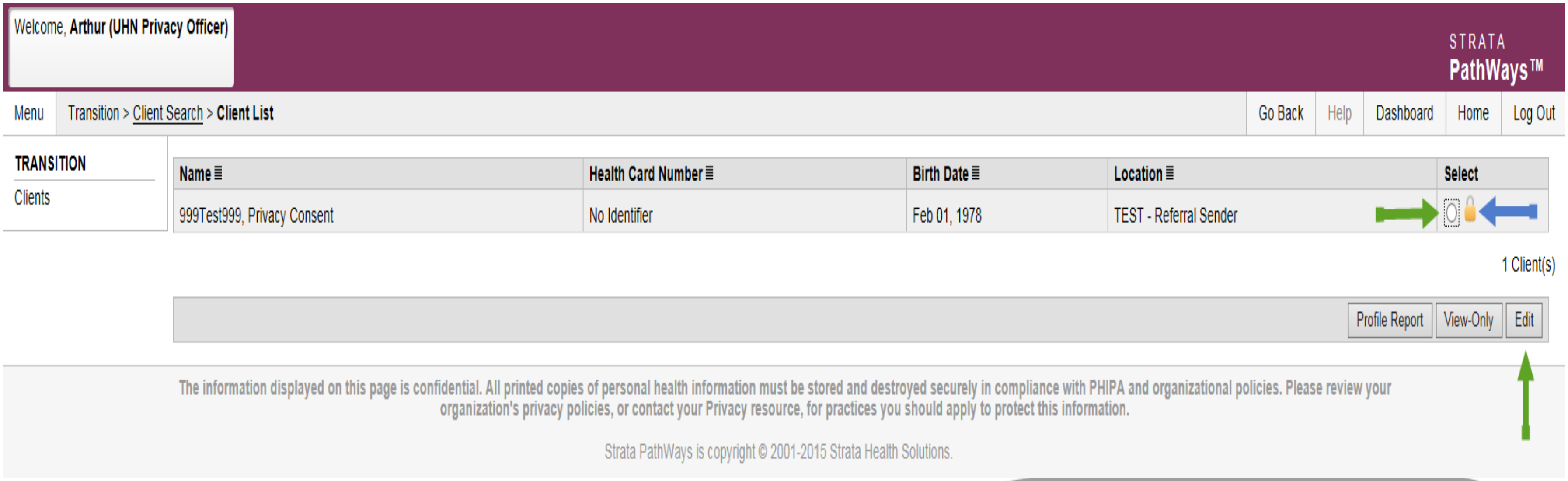
1. Select either:
   - "Available with Implied or Express Consent" (to withdraw an existing Consent Directive restriction); OR
   - "Restricted due to client consent directive" (to apply a new Consent Directive restriction)
2. Press the "Save" button



Care Type:	CCAC Referral - (manage)
Name:	999Test999, Privacy Consent - (View Comments)
Client Consent:	Available with Implied or Express Consent Restricted due to client consent directive
Health Card Number:	No Identifier
MRN:	0004729(StrataHealth)
CHRIS ID:	
Responsible Person(s):	Snare, Arthur (pager: N/A) ● Filter by Facility ○ Show All
Other Interested Parties:	
Referral Owner:	Select TEST - Referral Sender
Profile Status:	Start New Referral
Last Assessed Date:	Feb 17, 2015

Consent – c. Applying the Consent Directive (cont'd) Validate that Consent Directive Applied

1. The "lock" icon indicates that the Consent Directive has been applied
2. If the Consent Directive was incorrectly applied (e.g., if it was applied to the wrong record), select the radio button
3. Press the "Edit" button



Welcome, Arthur (UHN Privacy Officer)

Menu | Transition > Client Search > Client List

TRANSITION
Clients

Name ≡	Health Card Number ≡	Birth Date ≡	Location ≡	Select
999Test999, Privacy Consent	No Identifier	Feb 01, 1978	TEST - Referral Sender	○ 🔒

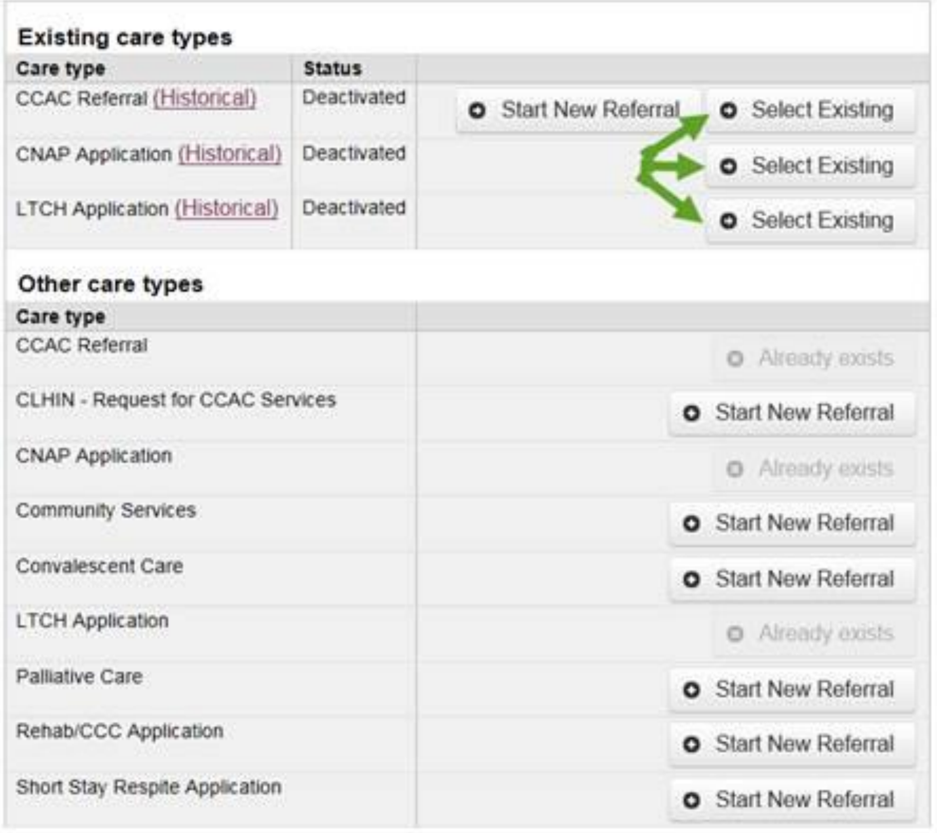
1 Client(s)

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent – c. Applying the Consent Directive (cont’d) Confirm Record

1. Ensure the correct patient record is chosen
2. Press the “Select Existing” button for any one of the **existing** care types (Do NOT start a new referral)



Existing care types

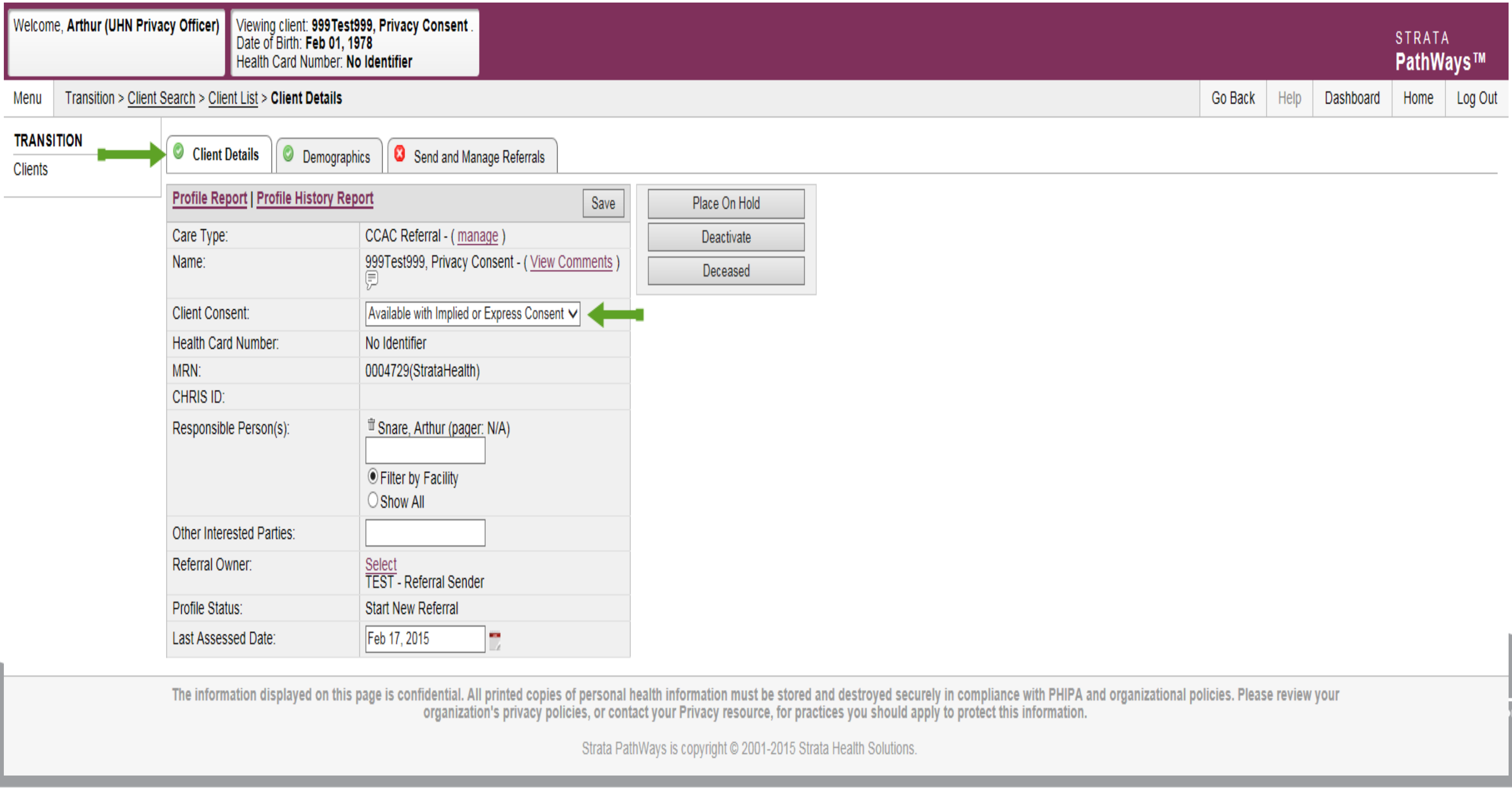
Care type	Status	
CCAC Referral (Historical)	Deactivated	● Start New Referral ● Select Existing
CNAP Application (Historical)	Deactivated	● Select Existing
LTCH Application (Historical)	Deactivated	● Select Existing

Other care types

Care type	
CCAC Referral	○ Already exists
CLHIN - Request for CCAC Services	● Start New Referral
CNAP Application	○ Already exists
Community Services	● Start New Referral
Convalescent Care	● Start New Referral
LTCH Application	○ Already exists
Palliative Care	● Start New Referral
Rehab/CCC Application	● Start New Referral
Short Stay Respite Application	● Start New Referral

Consent – c. Applying the Consent Directive (cont'd)
Update or Remove Consent Directive

1. Use the "Client Details" tab
2. Select the "Client Consent" dropdown



Welcome, **Arthur (UHN Privacy Officer)**

Viewing client: **999Test999, Privacy Consent** .
Date of Birth: **Feb 01, 1978**
Health Card Number: **No Identifier**

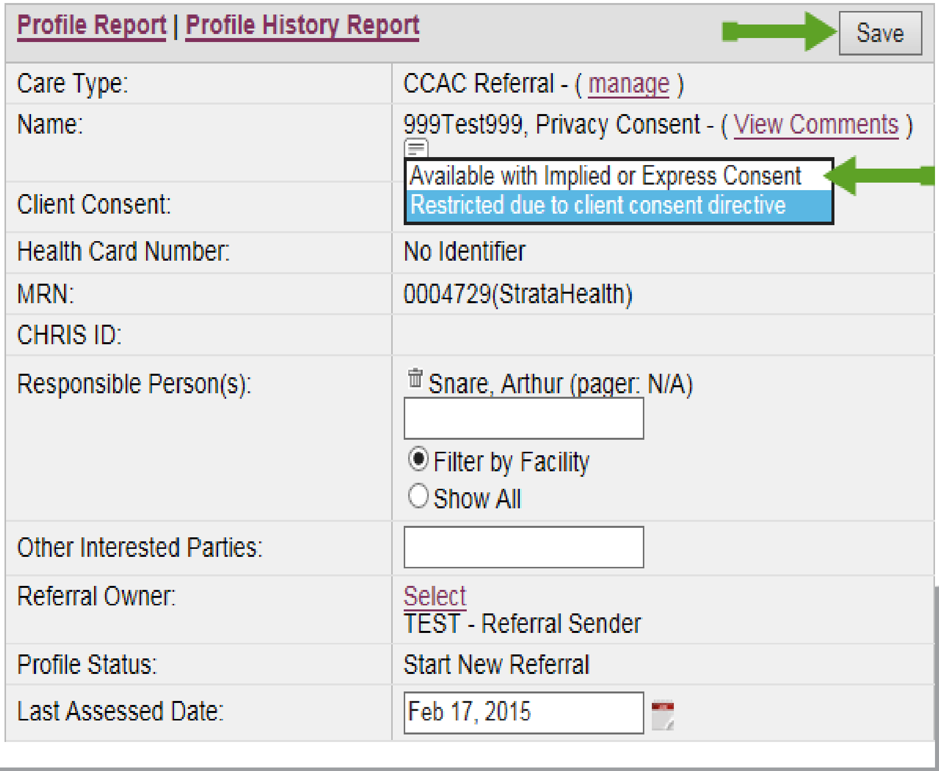
Care Type:	CCAC Referral - (manage)
Name:	999Test999, Privacy Consent - (View Comments)
Client Consent:	Available with Implied or Express Consent
Health Card Number:	No Identifier
MRN:	0004729(StrataHealth)
CHRIS ID:	
Responsible Person(s):	Snare, Arthur (pager: N/A) ● Filter by Facility ○ Show All
Other Interested Parties:	
Referral Owner:	Select TEST - Referral Sender
Profile Status:	Start New Referral
Last Assessed Date:	Feb 17, 2015

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent – c. Applying the Consent Directive (cont'd) Select Consent Directive Option

1. Remove the Consent Directive by choosing "Available with Implied or Express Consent"
2. Press the "Save" button



Profile Report | Profile History Report

Care Type:	CCAC Referral - (manage)
Name:	999Test999, Privacy Consent - (View Comments)
Client Consent:	Available with Implied or Express Consent Restricted due to client consent directive
Health Card Number:	No Identifier
MRN:	0004729(StrataHealth)
CHRIS ID:	
Responsible Person(s):	Snare, Arthur (pager: N/A) ● Filter by Facility ○ Show All
Other Interested Parties:	
Referral Owner:	Select TEST - Referral Sender
Profile Status:	Start New Referral
Last Assessed Date:	Feb 17, 2015

Consent – c. Applying the Consent Directive (cont'd)

What do you need to include when notifying the Individual?

- Tell the Individual what they requested
- Describe the Consent Directive and its impact
- Confirm the Consent Directive was made and the date that it was made
- Describe the circumstances under which the Consent Directive may be overridden (i.e., consent, risk of harm to self or others)
- Inform them that they will be notified when overridden
- Include the contact information for the Privacy Lead at your organization
- Inform them that they may change or remove the Consent Directive at any time

Consent – d. Overriding a Consent Directive

What are acceptable reasons for override once clinical viewing allowed?

- Express consent by patient or SDM
- Foreseeable risk of significant bodily harm to the patient and it is not reasonable to get consent in a timely manner
- Foreseeable risk of significant bodily harm to another Individual or group

Consent – d. Overriding a Consent Directive (cont'd)

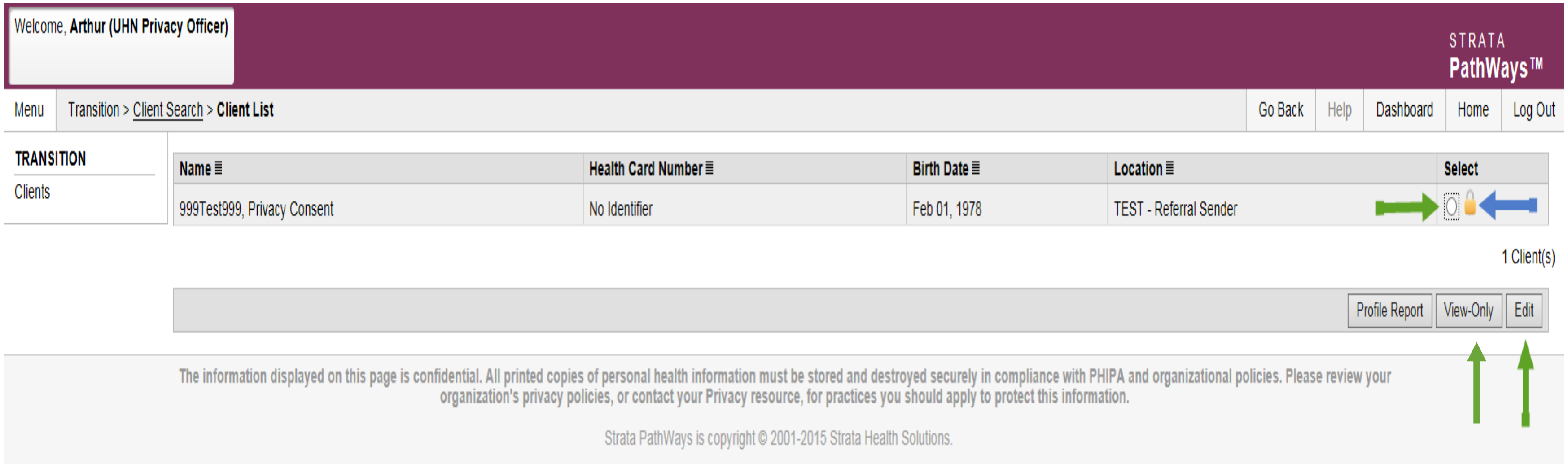
How does a Clinician get express consent?

- For the purposes of express consent, the clinician must ensure that consent is **knowledgeable** by speaking with the Individual about:
  - Purpose of collection
  - Reminder that consent does not need to be given
  - Override is for the duration of the login to the application. Subsequent logins will require an additional override
  - PHI will be available only to the person overriding the directive
  - PHI can only be used or disclosed for the purpose of the override

Consent – d. Overriding a Consent Directive (cont’d) Overriding a Consent Directive Restriction

A Consent Directive restriction can be overwritten by:

1. Selecting the radio button for a patient with a Consent Directive restriction applied (i.e., the “lock” icon flags the record as being restricted)
2. Pressing either the “View Only” or “Edit” button



Welcome, **Arthur (UHN Privacy Officer)**

Name	Health Card Number	Birth Date	Location	Select
999Test999, Privacy Consent	No Identifier	Feb 01, 1978	TEST - Referral Sender	○ 🔒

1 Client(s)

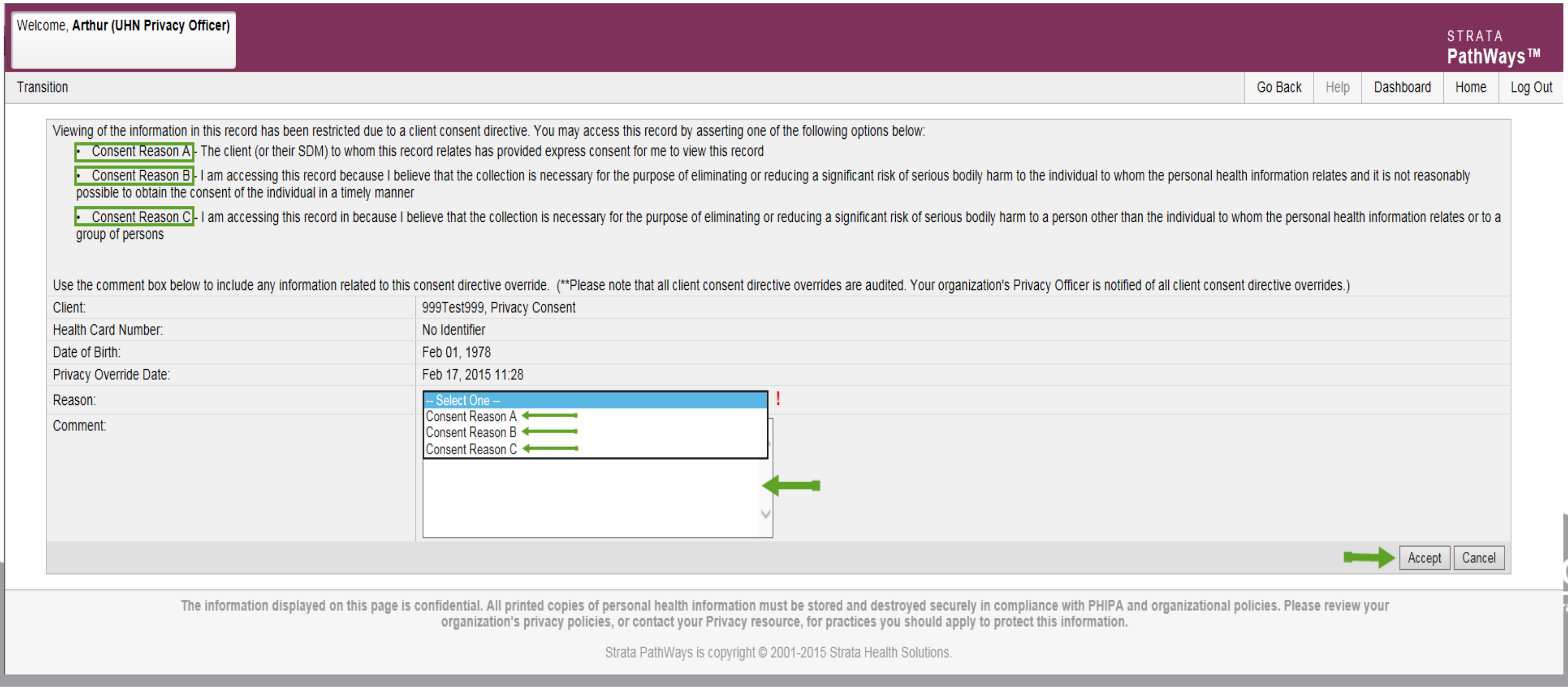
The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent – d. Overriding a Consent Directive (cont'd) Overriding a Consent Directive Restriction - Continued

Clinicians may override a Consent Directive restriction, and access the Personal Health Information found in the referral under the authority of one of three reasons listed in the image below.

1. Chose the "Consent Reason" corresponding to the authority that you're using to access the information.
2. Press the "Accept" button



Viewing of the information in this record has been restricted due to a client consent directive. You may access this record by asserting one of the following options below:

- Consent Reason A - The client (or their SDM) to whom this record relates has provided express consent for me to view this record
- Consent Reason B - I am accessing this record because I believe that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom the personal health information relates and it is not reasonably possible to obtain the consent of the individual in a timely manner
- Consent Reason C - I am accessing this record in because I believe that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the personal health information relates or to a group of persons

Use the comment box below to include any information related to this consent directive override. (**Please note that all client consent directive overrides are audited. Your organization's Privacy Officer is notified of all client consent directive overrides.)

Client:	999Test999, Privacy Consent
Health Card Number:	No Identifier
Date of Birth:	Feb 01, 1978
Privacy Override Date:	Feb 17, 2015 11:28
Reason:	-- Select One --
Comment:	

The information displayed on this page is confidential. All printed copies of personal health information must be stored and destroyed securely in compliance with PHIPA and organizational policies. Please review your organization's privacy policies, or contact your Privacy resource, for practices you should apply to protect this information.

Strata PathWays is copyright © 2001-2015 Strata Health Solutions.

Consent - d. Overriding a Consent Directive (cont'd)

How do you follow up on an override?

1. Privacy Lead from the HIC that overrode the Consent Directive, and Privacy Lead from the HIC where the patient is located, will receive a secure notification from RM&R of an override.
2. Privacy Lead(s) review the details of the override in RM&R and confirm whether the override was appropriate.
3. Privacy Lead notifies the Individual that an override occurred and provides the relevant information.
4. Privacy Lead logs that the notice occurred

Example

- Dr. Merl from Organization A overrides a Consent Directive for an individual at Organization B
- Privacy Lead at Organization A:
  - Receives notice that an override occurred (directly from UHN at this time)
  - Tells the Individual that an override occurred
- Privacy Lead at Organization B :
  - Receives notice that an override occurred

Important!

If the Consent Directive override is inappropriate, the Privacy Lead must initiate Privacy Breach Management procedures

Consent - d. Overriding a Consent Directive (cont'd)

- **What do you tell the Individual?**
  - Name of the clinician and HIC who overrode the Consent Directive
  - Date and time of the override
  - Type of PHI collected and the name of the HIC that contributed the PHI to the RM&R System
  - Reason for the override (i.e., reason that the clinician chose in the System)
  - Contact information for the Privacy Lead at your organization

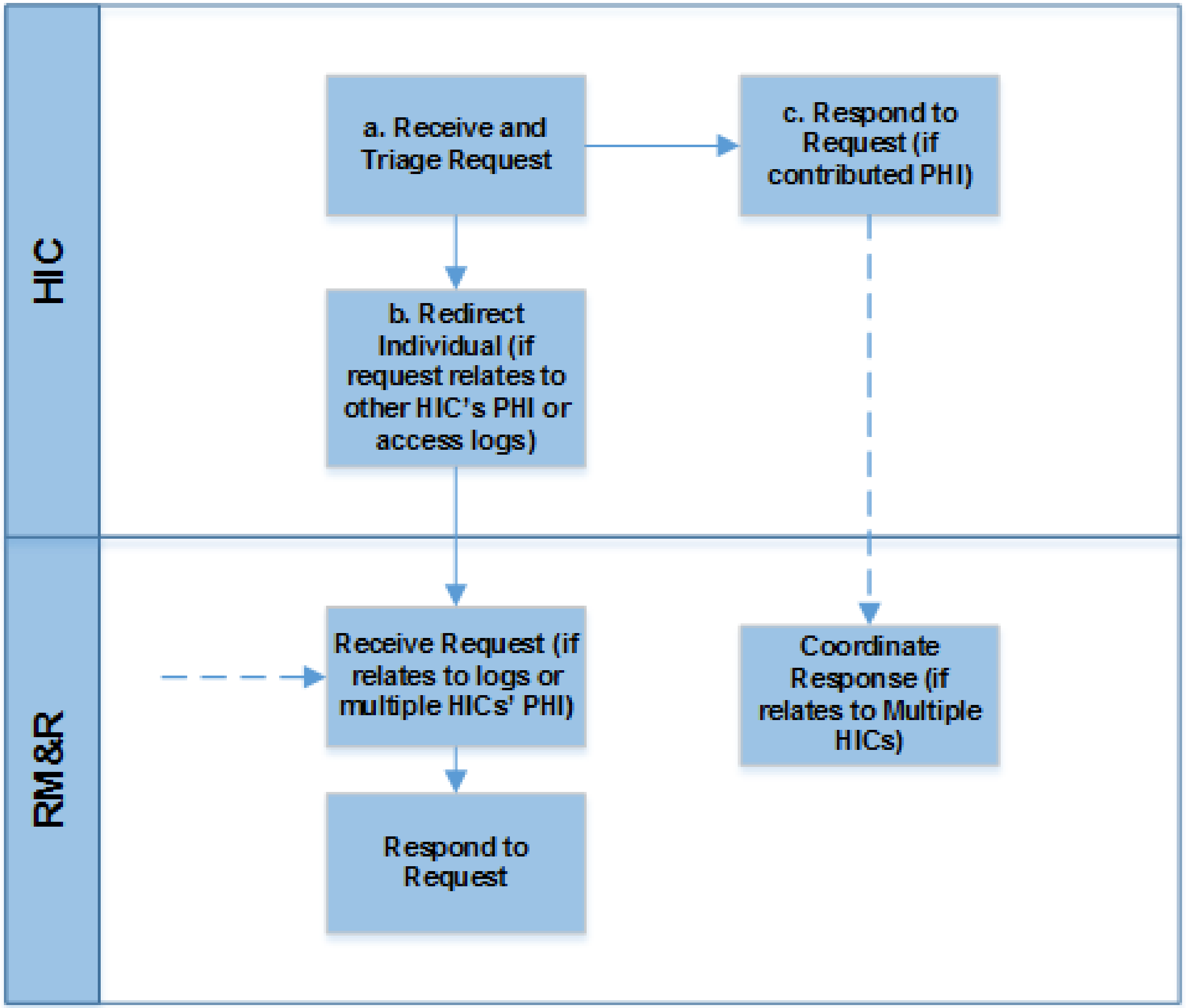
Request for Access – Overview

- **What does a HIC do if they receive the request?**
  - Respond if it relates to PHI that you contributed or collected (i.e., viewed)
  - Ask Individual to contact the HIC that contributed the PHI, and provide the individual with the HIC's contact information.
- **What does RM&R do if they receive the request?**
  - Ask Individual to contact the HIC that contributed the PHI, and provide the individual with the HIC's contact information if it involves just one HIC
  - Respond to the request if it involves logs (e.g., who access my PHI?)
  - Coordinate the response and perform all the administrative functions if it relates to multiple HICs

Important!

If you receive an access request for PHI that you contributed, contact referrals@uhn.ca to obtain a copy of the relevant information.

Request for Access – Process Summary



HIC

RM&R

a. Receive and Triage Request

b. Redirect Individual (if request relates to other HIC's PHI or access logs)

c. Respond to Request (if contributed PHI)

Receive Request (if relates to logs or multiple HICs' PHI)

Respond to Request

Coordinate Response (if relates to Multiple HICs)

Request for Access – a. Receiving and Triaging a Request for Access

What are the types of access requests?

- PHI in the RM&R System
- Report of who has viewed the Individual's PHI
- Report of history of Consent Directives
- Report of Consent Directive overrides

How do you receive and triage an access request?

1. Receive the Request as normal (i.e. use existing forms, processes, and identity verification practices)
2. Determine whether to:
   - Respond if the Request relates to PHI your organization contributed or an audit report to which you have access
   - Redirect Individual to the HIC that contributed the PHI if request relates to PHI contributed by another HIC

How would you answer?

- Individual asks for PHI?
- Individual asks about who has viewed their record?
- Individual asks for PHI from another HIC?

Request for Access – b. Redirecting an Individual to RM&R

What if the request does not involve your organization?

Redirect the Individual to the HIC that contributed the PHI when the request involves:

- PHI contributed by another HIC

Redirect the Individual to RM&R when the request involves:

- Access to audit reports
  - Who has viewed the patient’s information
  - History of the patient’s Consent Directives
  - History of Consent Directive overrides

Ask the Individual to visit www.resourcematchingandreferral.com for contact information or send an email with their contact information to referrals@uhn.ca.

Important!

The Individual should not email PHI, including the nature of the request (e.g., access request). If the Individual sends their contact information, ConnectingGTA’s privacy team will contact them to identify the nature of and address the request or issue.

Request for Access – c. Responding to a Request for Access (cont'd)

How do you respond when RM&R sends you a request that relates to multiple organizations?

1. Determine as soon as possible, but within 21 days:
   - The fee estimate
   - Whether to grant the Request or apply exceptions
   - If an extension is required
2. Complete the following letters from the *Privacy and Security Manual (as applicable)*:
   - *Letter Refusing a Request for Access in Whole or in Part*
   - *Letter Notifying of an Extension*
3. Securely send a PDF of the letter and instructions on fulfilling the Request to RMR_Program@uhn.ca

Note: *If you do not respond within 21 days, RM&R will inform the Individual and inform them of their right to make a complaint.*

Request for Access –
c. Responding to a Request for Access (cont'd)

Can you charge fees?

- HICs may charge fees to fulfill access requests associated with information in RM&R (even if RM&R coordinates the response)
- When RM&R is coordinating a response, HICs must communicate the fee estimate to RM&R. RM&R will collect the fee from the Individual, if any, and forward it to the HIC.
- Fees must:
  - Be communicated to the Individual prior to charging them;
  - Not exceed the amount of reasonable cost recovery; and
  - Be consistent with applicable orders of the Information and Privacy Commissioner of Ontario (Refer to Order HO-009)
- Individuals with concerns about the fee estimate will be asked to complain directly to the HIC charging the fee

Request for Correction – Overview

What does a HIC do if they receive the request?

- Make the correction if it relates to PHI that you contributed
- If one other HIC contributed the PHI, ask Individual to contact that HIC
- If multiple other HICs contributed the PHI, ask the individual to contact RM&R

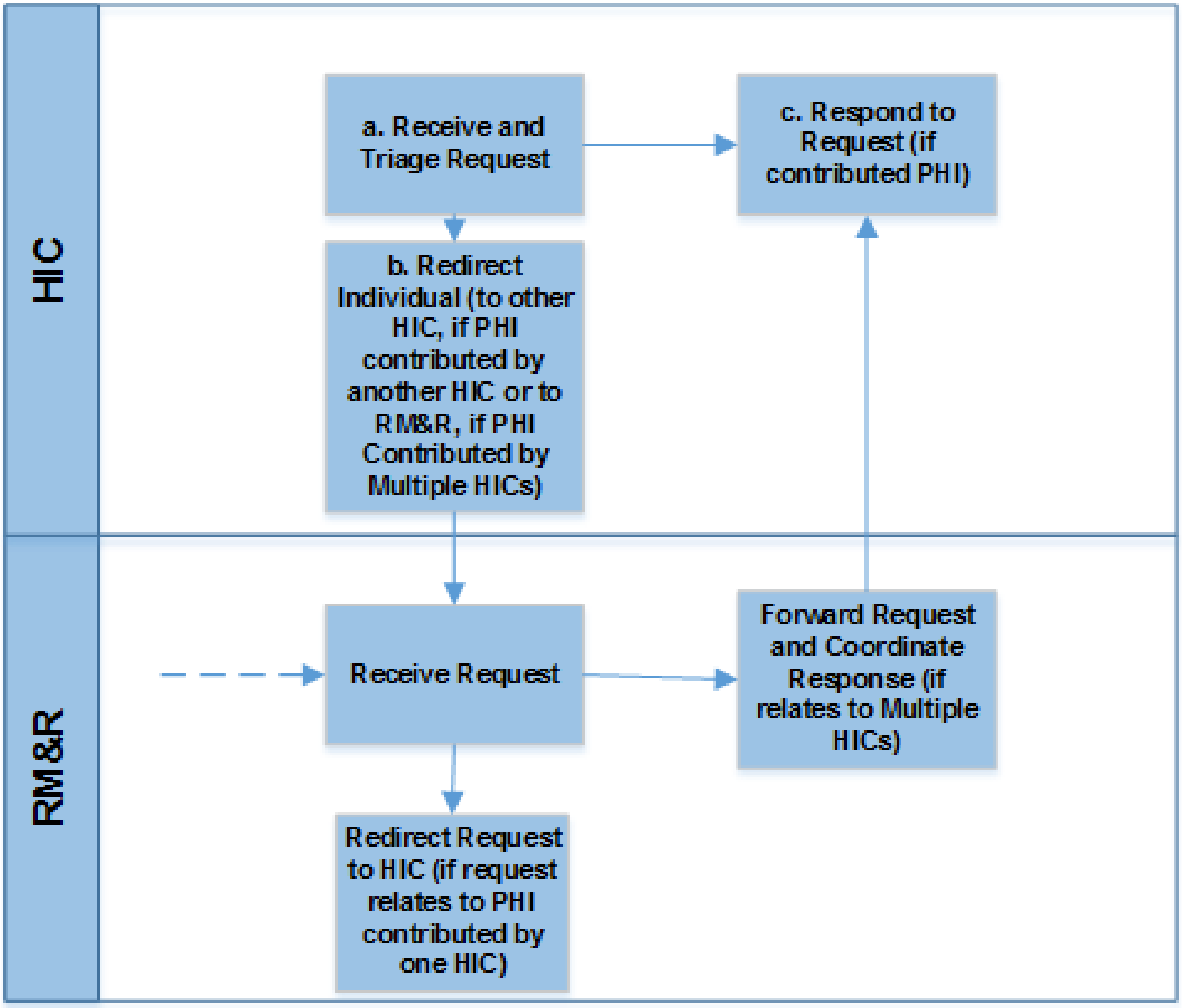
What does RM&R do if they receive the request?

- Forward to the HIC(s) that contributed the PHI

Important!

Corrections in your local HIS **may** automatically uploaded into the RM&R System. After making the change in you're HIS, you must validate the correction in RM&R, and make it manually in RM&R, if necessary. If the correction cannot be made in RM&R, contact RMR_Program@uhn.ca for assistance.

Request for Correction – Process Overview



HIC

a. Receive and Triage Request

b. Redirect Individual (to other HIC, if PHI contributed by another HIC or to RM&R, if PHI Contributed by Multiple HICs)

c. Respond to Request (if contributed PHI)

RM&R

Receive Request

Forward Request and Coordinate Response (if relates to Multiple HICs)

Redirect Request to HIC (if request relates to PHI contributed by one HIC)

Request for Correction –
a. Receive and Triage a Request for Correction

How do you receive and triage a correction request?

1. Receive the Request as normal (i.e. use existing forms, processes, and identity verification practices)
2. Determine whether to:
   - Respond if:
     The Request relates to PHI that you contributed
   - Redirect Individual to another HIC if: The correction relates to PHI contributed by one other HIC
   - Redirect Individual to RM&R if: The correction relates to PHI contributed by multiple other HICs

How would you answer?

- Individual requests correction to PHI that your organization contributed?
- Individual requests correction to multiple pieces of PHI?
- RM&R sends you a correction request?

Request for Correction – b. Redirecting an Individual

What do you do if the correction does not relate to PHI that your organization contributed?

- Redirect the Individual to another HIC when the request involves:
  - PHI contributed by another HIC
- Redirect the Individual to RM&R when the request involves:
  - PHI contributed by multiple other HICs

- Ask the Individual to visit www.resourcematchingandreferral.com for more information or have them send an email with their contact information to referrals@uhn.ca.

Important!

The Individual should not email PHI, including the nature of the request (e.g., correction request). If the Individual sends their contact information, RM&R's privacy team will contact them to identify the nature of and address the request or issue.

Request for Correction – c. Responding to a Request for Correction

How do you respond to a request for correction?

1. Follow internal policies and procedures to determine if the correction should be made
2. Make the correction (or attach a notice of disagreement) in the source system
   - Contact RM&R if you are not able to make the correction or attach a notice of disagreement
3. If medically relevant and the Individual requests, inform the persons to whom the PHI was disclosed of the correction
4. Log the response

Important!

Corrections to PHI in the source system may be uploaded into the RM&R System and marked as a change in the record. If a correction in your source system does not update the RM&R System, and if you cannot make the change manually in the RM&R system, contact RMR_Program@uhn.ca, who will make the change in the RM&R System on your behalf (as possible). You will need to include enough information about the correction (e.g., Patient ID, original value, corrected value, date of service) to be able to accurately identify the patient and the requested change.

NOTE: *Do not send this information using an unsecured communication method (e.g., unencrypted email). A secure communication option you may use is the UHN File Portal (https://fileportal.uhn.ca/Upload.aspx).*

Inquiries – Overview

What does a HIC do if they receive an inquiry?

- Respond if it relates to your HIC or relates to another HIC, but you are able to answer it
- If the inquiry relates to another HIC, and you are not able to answer it, ask the individual to contact the other HIC
- If the inquiry relates to multiple organizations, and you are not able to answer it, ask the Individual to contact RM&R

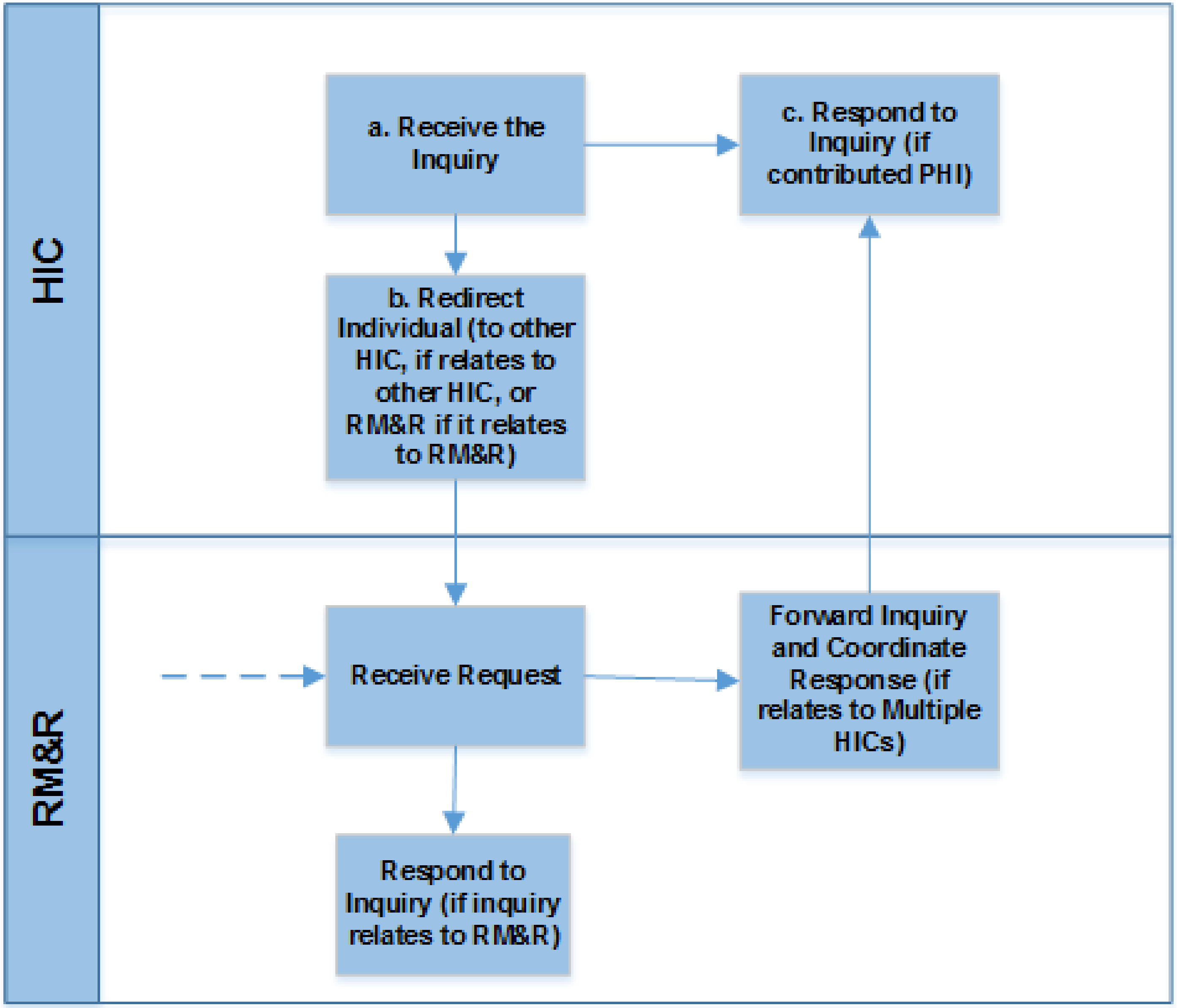
What does RM&R do if they receive an inquiry?

- RM&R will address it if it is about the Program or are able to answer it
- If it relates to just one HIC, and RM&R isn't able to answer it, ask the individual to contact the HIC
- Facilitate communication with the HICs and draft a response if it relates to multiple HICs

Important!

If RM&R is responsible for coordinating and the HIC does not respond, RM&R will tell the Individual there was no response and tell the Individual to contact the HIC directly or make a complaint to the IPC.

Inquiries – Process Overview



HIC
RM&R
a. Receive the Inquiry
b. Redirect Individual (to other HIC, if relates to other HIC, or RM&R if it relates to RM&R)
c. Respond to Inquiry (if contributed PHI)
Receive Request
Forward Inquiry and Coordinate Response (if relates to Multiple HICs)
Respond to Inquiry (if inquiry relates to RM&R)

Inquiries –
a. Receiving an Inquiry

How do you receive and triage an inquiry?

1. Receive the Inquiry as normal (i.e. use existing forms, processes)
2. Determine whether to:
   - Respond if:
     - The Inquiry relates to your organization
     - The Inquiry relates to another HIC/ RM&R but is easy to address
   - Redirect Individual to another HIC if:
     - It relates to another HIC and you cannot address it
   - Redirect Individual to RM&R if:
     - It relates to multiple other HICs or to RM&R and you cannot address it

How would you answer?

- Where are the RM&R privacy policies?
- What type of information does your organization contribute to the database?
- What have you done to protect my information?
- How do I get out of the database?
- Does the government have access to my information?

Inquiries – b. Redirecting an Inquirer to RM&R

What do you do if the Inquiry does not relate to your organization?

- If the Inquiry relates to another HIC and you are unable to address it, redirect the Inquirer to the other HIC
- If the Inquiry relates to multiple other HICs or RM&R, redirect the Inquirer to RM&R
- Ask the Individual to visit www.resourcematchingandreferral.com for more information or send an email with their contact information to referrals@uhn.ca.

Important!

The Individual should not email PHI, including the nature of the request (e.g., inquiry about specific PHI). If the Inquiry involves PHI, the Individual should send their contact information and RM&R's privacy team will contact them to identify the nature of and address the Inquiry.

Inquiries –
c. Responding to an Inquiry

How do you respond to an Inquiry?

1. Follow internal policies and procedures to respond to the Inquiry

Inquiries –
d. Providing Information to Support RM&R in Responding to Inquiry

How do you support RM&R in responding to an Inquiry?

1. Provide information to RM&R as soon as possible, but within the timeline agreed to, allowing RM&R to respond within 30 days of receipt of the Inquiry.
2. Review and comment on the draft response that RM&R develops as soon as possible, but within the timeframe agreed to.

Why would RM&R ask for information?

RM&R receives an inquiry related to multiple HICs and is coordinating the response

Important!

If you do not provide information to support the response within the timeframe agreed to by all organizations involved, RM&R will notify the Individual of this infringement, and inform them of their right to make a complaint.

Complaints – Overview

What does a HIC do if they receive the Complaint?

- If it relates to your HIC – respond
- If it relates to just one other HIC – ask the Individual to contact the HIC (provide contact information)
- If it relates to RM&R - ask Individual to contact RM&R (provide contact information)

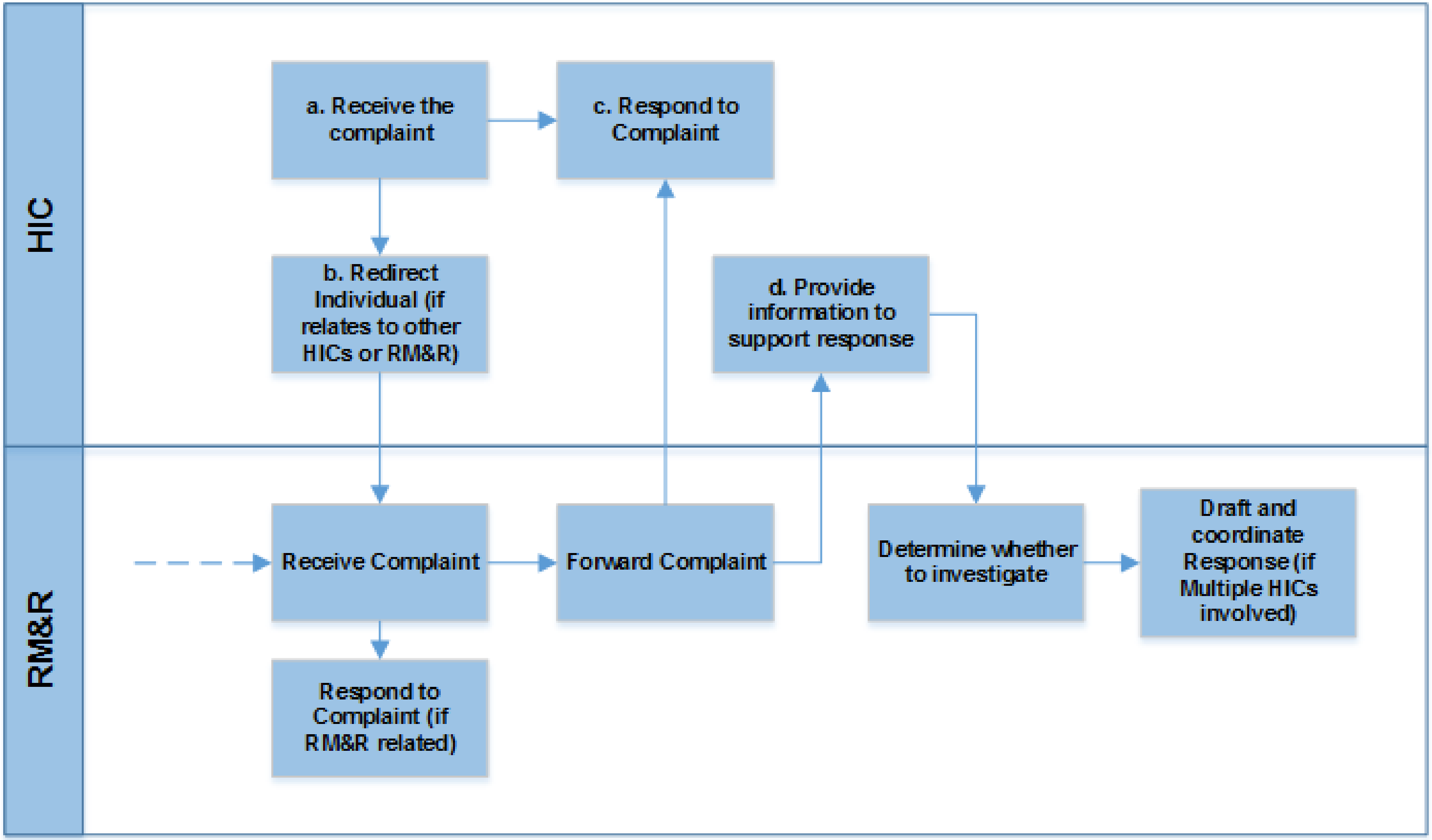
What does RM&R do if they receive the Complaint?

- If it is about RM&R - address it
- If it relates to just one HIC – ask the Individual to contact the HIC
- If it relates to multiple HICs - Facilitate communication with the HICs and draft a response

Important!

If RM&R is responsible for coordinating and the HIC does not respond, RM&R will tell the Individual there was no response and tell the Individual to contact the HIC directly or make complaint to IPC.

Complaints – Process Overview



HIC
RM&R
a. Receive the complaint
c. Respond to Complaint
b. Redirect Individual (if relates to other HICs or RM&R)
d. Provide information to support response
Receive Complaint
Forward Complaint
Determine whether to investigate
Draft and coordinate Response (if Multiple HICs involved)
Respond to Complaint (if RM&R related)

Complaints –
a. Receiving a Complaint

How do you receive and triage a Complaint?

1. Receive the Complaint as normal (i.e. use existing forms, processes)
2. Determine whether to:
   - Respond if the Complaint relates to your organization alone
   - Redirect Individual to another HIC if the Complaint relates to the other HIC
   - Redirect Individual to RM&R if the complaint relates to RM&R or multiple HICs

How would you answer?

- RM&R has too much information about people.
- I don't think your organization should put information in the database.
- I think someone at another hospital looked at my information inappropriately.

Complaints – b. Redirecting a Complainant

What do you do if the complaint does not relate to your organization?

- Redirect the Complaint to a HIC when the Complaint involves:
  - The other HIC
- Redirect the Complainant to RM&R when the Complaint involves:
  - RM&R or multiple other HICs
- Ask the Complainant to visit www.resourcematchingandreferral.com for more information or send an email with their contact information to referrals@uhn.ca.

Important!

The Individual should not email PHI, including the nature of the issue (e.g., complaint). If the Complaint involves PHI, the Individual should send their contact information and RM&R's privacy team will contact them to identify the nature of and address the Complaint.

Complaints –
c. Responding to a Complaint

How do you respond to a complaint?

1. Follow internal policies and procedures to respond to the Complaint

Complaints – d. Providing Information to Support RM&R in Responding to Complaint

How do you support RM&R in responding to a Complaint?

1. Provide information to RM&R as soon as possible, but within the timeline agreed to, allowing RM&R to respond within 30 days of receipt of the Inquiry.
2. Review and comment on the draft response that RM&R develops as soon as possible, but within the timeframe agreed to.

Why would RM&R ask for information?

RM&R receives a Complaint related to multiple HICs and is coordinating the response

Important!

The Individual should not email PHI, including the nature of the issue (e.g., complaint). If the Complaint involves PHI, the Individual should send their contact information. RM&R's privacy team will contact them to identify the nature of and address the Complaint.

Assurance Activities

Overview

Why is assurance important?

- To ensure agents and ESPs are compliant with policies and procedures
- This enables trust amongst the HICs that each has a comparable and sufficient level of privacy and security protection for RM&R

What are the regular activities and who is responsible for conducting them?

- Logging and auditing – you will receive reports by email on a quarterly basis that your organization is responsible for reviewing to assess appropriateness of accesses
- Training – you are responsible for ensuring that all users who access RM&R have been appropriately trained about their privacy and security responsibilities stemming from PHIPA and RM&R agreements, policies and procedures
- Assertion Surveys – you will be asked to complete and submit assertion surveys on an annual basis, and to mitigate all identified risks

How do you ensure your agents and ESPs' are compliant?

- Reviewing audit reports
- Following-up on Consent Directive override notifications to confirm appropriateness
- Ensuring new agents/ESPs are informed of their duties
- Ensuring new agents/ESPs agree to their obligations
- Ensuring agents/ESPs understand their obligations on an ongoing basis

Logging and Auditing

What you need to do?

- Regularly review audit reports to look for suspicious activities

When should you review the reports?

- On a regularly-scheduled basis
- If you suspect that PHI was inappropriately collected, used, or disclosed
- On a quarterly basis, when received from RM&R

What should you be looking at?

- What have my staff been looking at?
- What Consent Directives have been overridden?
- Who has been overriding my patients' Consent Directives or looking at their PHI?

Important!

HICs will not have access to the tools that allow them to generate their own audit reports; email RM&R_Program@uhn.ca to request audit reports for the RM&R System.

Privacy and Security Training

What you need to do:

- Ensure that everyone with access to the RM&R System understands their privacy and security responsibilities generally, and specific obligations related to RM&R
- Be able to demonstrate on an ongoing basis that the agents/ESPs understand their obligations

Important!

HICs are responsible for informing their own agents and ESPs of their duties. The training slides included as part of this slide deck can be included in existing training and awareness programs at the HIC's discretion.

Groups to be trained

- Clinicians (i.e., end-users)
- Privacy Officers (who are expected to liaise with RM&R)
- Security Officers (who are expected to liaise with RM&R)
- LRAs and HDUs (who register users on RM&R)
- Technical Staff (who maintain the connection to RM&R and do the HL7 mapping

Assertion Surveys

What you need to do:

- Complete and submit RM&R Assertion Surveys to the RM&R program, including a mitigation plan for all identified risks, on an annual basis
- Complete all mitigation tasks within the timeframe established by you in the survey
- Notify the RM&R program when risks have been mitigated

Important!

HICs are responsible for ensuring that all identified risks are mitigated within timeframes established through the surveys. If you have questions or require assistance, contact the RM&R program!

Handling PHI Securely

Handling PHI

Yes

- **Do:**
  - Only email PHI to RM&R when using your corporate account, and only to RM&R_Program@uhn.ca (if you are on ONEMail, this is a secure transmission)
  - If you aren’t on ONEMail, encrypt emails that contain PHI using a secure file transfer solution (you can use UHN’s solution at: https://fileportal.uhn.ca/Upload.aspx - choose the Patient Information setting)
  - Store forms with PHI in secure locations on your network

No

- **Don’t:**
  - Send PHI to RM&R from your personal email accounts (e.g., Hotmail, Gmail, etc.)
  - Store PHI in locations outside your organization’s IT environment (e.g. iCloud, DropBox, etc.)

Accessing the RM&R System

Yes

- **Do:**
  - Always use your assigned ID for RM&R
  - Lock your workstation (e.g., Ctrl-Alt-Delete and “Lock this computer”) when it is left unattended and logged into the RM&R System
  - Use only approved remote access solutions for remote access

No

- **Don’t:**
  - Allow another person to use your ID to access the System
  - Disable or override security controls, or exploit any suspect security weaknesses
  - Knowingly perform an act that will interfere with the normal operations of the RM&R System

Creating and Protecting Your Passwords

Yes

- **Do:**
  - – Create passwords that are at least eight characters long and include at least three of the following:
    - A number
    - An uppercase letter
    - A lowercase letter
    - A special character
  - – Keep your password a secret and change it immediately if you think it may have been compromised
  - – Ensure your portal passwords are different from your passwords used for personal accounts (e.g., banking password)

No

- **Don’t:**
  - – Tell anyone your password, including a system administrator, help desk personnel or a manager
  - – Create passwords that include:
    - All or part of your ID
    - Easily obtained personal information about yourself, or
    - Three consecutive characters
  - – Change passwords in an easily recognized pattern (e.g., changing “IL0v3EatingP!zza1” to “IL0v3EatingP!zza2”)

And we know you know, but…

Don’t:

- Troll for patients in the RM&R System
- Discuss PHI that you see except with those authorized to hear about it and only in the context of what your defined job responsibilities requires
- Allow shoulder surfing

Privacy Breach Management

Privacy Breaches and Security Incidents

What is a Privacy Breach?

Where one of the following has been or are about to be contravened:

- A provision of PHIPA or its regulations
- The privacy provisions of any agreement in respect of the RM&R program
- The privacy policies, procedures and practices implemented for RM&R
- PHI is lost or stolen or has been or is about to be accessed by an unauthorized person; or
- Records of PHI have been or are about to be copied, modified or disposed of in an unauthorized manner

What is a Security Incident?

- Any violation or imminent threat of violation of a RM&R information security policy, standard, procedure or practice
- Any information security event that may compromise operations or threaten the security of an information system or business process

Examples

- Unauthorized person (e.g., researcher with no clinical duties) provided with an account for the RM&R System
- Physician with a legitimate account uses the PHI for inappropriate purposes (e.g., research)
- Virus or malware infection
- Compromised password
- Leaving a workstation unattended and logged into RM&R

Privacy Breaches and Security Incidents

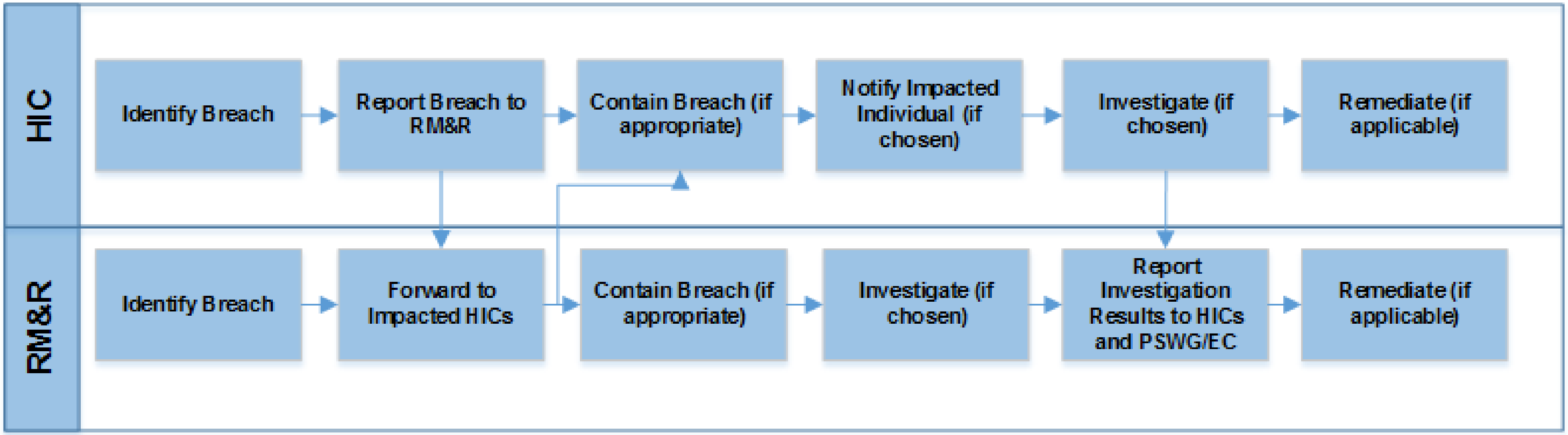
What is the CPOs role?

- Report any suspected or actual privacy breaches to RM&R by end of the next business day (after becoming aware of it); security incidents to be reported by your CSO within the same timeframe
- Work with RM&R as required to contain, investigate and remediate the breach
- Notify impacted individuals, when applicable
- Work with RM&R to meet reporting requirements

Consequences of Breach

- Individuals responsible for a Breach are subject to the disciplinary procedures of their organizations (and may be subject to disciplinary proceedings of their colleges)
- Disciplinary action may include any of the following: termination of employment or other relationship with organization, termination of access to the system, reporting to applicable professional college(s), fine and/or other legal proceedings
- PSWG/EC reviews breaches, and may require containment, remediation, and prevention activities to be conducted by your organization

Privacy Breach Management – Process Overview



HIC
Identify Breach
Report Breach to RM&R
Contain Breach (if appropriate)
Notify Impacted Individual (if chosen)
Investigate (if chosen)
Remediate (if applicable)
RM&R
Identify Breach
Forward to Impacted HICs
Contain Breach (if appropriate)
Investigate (if chosen)
Report Investigation Results to HICs and PSWG/EC
Remediate (if applicable)

Breaches: Your Organization Contributed PHI

Step 1 – Report *all* breaches

- Report any breaches involving the RM&R System, even if it just impacts PHI that your organization contributed
- Telephone the RM&R program at: 1 (866) 556-5005
- Email the completed *Privacy Breach Report* form to RM&R_Program@uhn.ca
- Make the report as complete as possible
- Reporting allows RM&R to understand trends and potentially improve training or other controls

Step 2 – Contain, investigate, notify, and remediate

Contain, investigate, notify, and remediate according to your internal policies and procedures, or as directed by the RM&R PSWG and/or EC

Breaches: Other Organizations Contributed the PHI

Step 1 – Report *all* breaches

- *Report all breaches involving the RM&R System as soon as possible but no later than the end of the next business day after the privacy lead becomes aware of the issue*
- Telephone the RM&R program at: 1 (866) 556-5005
- Email the completed *Privacy Breach Report* form to RM&R_Program@uhn.ca
- Make the report as complete as possible

Step 2 – Contain the Breach

- Containment must begin as soon as possible to prevent a small Breach turning into a big one!
- If multiple HICs (or their agents or ESPs) caused the Breach, the HICs may choose an appropriate HIC to act as the Breach Response Lead and oversee containment of the Breach
- If RM&R (or their agents or ESPs) caused the Breach, it will act as the "Breach Response Lead" and begin containment

Breaches: Other Organizations Contributed the PHI (cont'd)

Step 3 – Notify Individuals impacted by the Breach

- Notification must happen as soon as reasonably possible if PHI is "stolen, lost, or accessed by unauthorized persons"; *PHIPA, s12 (2)*
- The Breach Response Lead will choose the most appropriate HIC to notify

Who Notifies?

The Breach Response Lead will identify a HIC to notify based on:

- The HIC that caused the Breach
- The HIC where the Individual most recently received care
- The HIC where the Individual typically receives care

Step 4 – Investigate the Breach and identify remediation steps

- Investigation to begin within 7 days
- Report to be written within 7 days of completing the investigation, using *Privacy Breach Report*
- Impacted HICs will have an opportunity to comment on the report

Who Investigates?

The Breach Response Lead will conduct the investigation, with assistance from the other HICs and RM&R, as needed.

Breaches: Other Organizations Contributed the PHI (cont'd)

Step 5 – Remediating a Breach

- Conduct the remediation steps requested by the RM&R Executive Committee
- Status updates to be emailed to RM&R_Program@uhn.ca on a timeframe determined by the Executive Committee

Contact Information

Contact Information

RM&R	20 Dundas St West, 3rd floor Toronto, ON M5G 2C2 (416) 340-4800 / 1 (866) 556-5005 www.resourcematchingandreferral.com (for information to be used by RM&R Participating sites and clients/patients/public) Email: referrals@uhn.ca (for CPOs and CSOs) Email: referrals@uhn.ca (for Individuals)

Important!

The Individual should not email PHI, including the nature of the request. Ask the Individual to email his or her contact information and someone from the RM&R program will contact them.

Thank you!
Questions?