Operational Privacy and Security Manual

Resource Matching and Referral (RM&R)

Operational Manual for Health Information Custodian's

Version: 1.1

Date: October, 2014

This page left intentionally blank.

Document History

Date	Approver	Version	Change(s)
September 16, 2014	PSWG	1	Initial Version
October 14, 2014	PSWG	1.1	Approved by PSWG

Table of Contents

1 Introduction 6

About The Manual 6
Release Cycle For The Manual 6
Definitions 8
Background 13

2 Privacy And Security Management Framework 14

Overview 15
Privacy And Security Domains 17

3 Privacy And Security Governance 19

RM&R Executive Committee (Ec) 19
Privacy And Security Working Group 20
Privacy And Security Operations Team 20

4 Policies And Procedures Overview 21

Privacy Policy (Ps.Pol.001) 22
Access And Correction Policy (Ps.Pol.002) 23
Consent Management Policy (Ps.Pol.003) 28
Inquiries And Complaints Policy (Ps.Pol.004) 32
Logging And Auditing Policy (Ps.Pol.005) 36
Privacy Breach Management Policy (Ps.Pol.006) 38
Privacy And Security Training Policy (Ps.Pol.07) 40
Retention Policy (Ps.Pol.008) 42
Assurance Policy (Ps.Pol.09) 43
RM&R Information Security Policy (Ps.Pol.101) 44

5 Policies 45

Privacy Policy (Ps.Pol.001) 45
Access And Correction Policy (Ps.Pol.002) 55
Consent Management Policy (Ps.Pol.003) 64
Inquiries And Complaints Policy (Ps.Pol.004) 69
Logging And Auditing Policy (Ps.Pol.005) 74
Privacy Breach Management Policy (Ps.Pol.06) 78
Privacy And Security Training Policy (Ps.Pol.07) 85
Retention Policy (Ps.Pol.008) 89
Assurance Policy (Ps.Pol.009) 92
RM&R Information Security Policy (Ps.Pol.101) 101

6 Supporting Forms And Templates 105

Access And Correction Policy (Ps.Pol.002) Forms 105
Letter Refusing A Request For Access In Whole Or In Part 105
Letter Notifying Of An Extension 107
Instructions To RM&R To Notify Hics Of A Correction To Phi 109
Consent Management Policy Forms 111
Consent Directive Intake And Communication Form 111
Consent Directive Management Checklist 114
Privacy Breach Management Policy 122
Privacy Breach Report 122
Privacy Breach Investigation Report 124
Update On Status Of Remediation Activities 127
Assurance Policy 129
Privacy And Security Readiness Assessments 129
Privacy Assertion Survey Template 131
Information Security Assertion Survey Template 150
7 Additional Supporting Materials 168
Hics Participating In The RM&R Program 169
Inventory Of Personal Health Information 171
Notice Of Purposes 173
Notice Of Purposes Addition To Information Notice 176

1 Introduction

About the Manual

This manual is intended to be used by site privacy and security leads to assist them in understanding the operational privacy and security framework to be followed in order to protect the personal health information (PHI) related to the RM&R Program. The policies and procedures identified in this manual do not replace the existing privacy or security programs at Health Information Custodians (HICs), but rather describe how the HICs' privacy and security programs must interface with RM&R to ensure an appropriate level of privacy and security protection for Individuals and their PHI. The manual will provide HICs with the policies governing the Program as well as the operational practices, and supporting materials and templates required to meet their obligations in the policies.

Release Cycle for the Manual

This manual is a living document that will continue to evolve as the RM&R Program changes and new functionality or capabilities are introduced.

All versions of the manual will include a similar layout; however, the content in many sections of the manual will be refreshed as the Program evolves to accommodate any changes in the privacy and security framework. The distribution of the manual will be delivered through the standard process.

As the manual evolves, this section of the manual will explain any updates made.

This version of the manual includes the following changes:

Section	Contents	Changes
Section 1: Overview of RM&R and Privacy and Security Manual	Introduction to the RM&R Program and Privacy and Security Manual	• Version1 of the document – No Changes
Section 2: Privacy and Security Governance	A description of the governance structure for RM&R and how HICs' privacy and security interests and concerns are represented within the decision-making structure	• Version1 of the document – No Changes
Section 3: Privacy and Security Management Framework Overview	The key domains of the Privacy and Security Management Framework which provides the reader with an understanding of the various activities and components associated with managing privacy and security in the RM&R Program	• Version1 of the document – No Changes
Section 4: Policies and Procedures Overview	Provides a summary of the policies and procedures that the HICs must follow to participate in the Program. This section also links to the relevant policies and any forms that the HIC is required to follow to meet its obligations under the policy.	• Version1 of the document – No Changes
Section 5: Policies	Provides the policies and procedures that HICs must follow to participate in	• Version1 of the document – No Changes

Section	Contents	Changes
	the RM&R Program	
Section 6: Required Forms and Documentation	Forms and documentation that the HIC is required to use to meet its obligations established in the policies	• Version1 of the document – No Changes
Section 7: Supporting Materials	Optional materials that the HICs can use to support their integration with the RM&R Program	• Version1 of the document – No Changes

Definitions

The following definitions are used in this manual:

Term	Definition
Agent[1]	• A person who works on behalf of a HIC, RM&R, or one of the third-party service providers;

Auditing	• The practice of inspecting logs for the purpose of:
	  ○ Verifying activity performed on an information system or network by any agent or Electronic Service Provider of RM&R, or a HIC, their agents or Electronic Service Providers;
	  ○ Verifying that an information system is in a desirable state; and
	  ○ Answer questions about how an information system arrived at a particular state.

Breach Investigator	• A HIC or RM&R who is chosen as lead to direct and oversee investigation, containment, remediation and reporting activities for management of the Breach. The Breach Investigator is identified by RM&R in collaboration with the HICs that contributed to PHI to the RM&R system and who were otherwise involved with the breach.
Collect, use, and disclose	• Each has the same meaning as in *PHIPA, 2004*.
Complaint	• A concern raised by any person[2] in respect of the RM&R Solution including, but not limited to, concerns raised in respect of compliance with the *Personal Health Information Protection Act, 2004* (*PHIPA*) and the policies, procedures and practices implemented in respect of the RM&R Solution.

[1] University Health Network (UHN) will serve as an Agent of the Originating HICs when aggregating data for the purpose of reporting to the HICs and the applicable LHIN(s), and when performing other privacy or security-related functions on behalf of the HICs, as directed by them.

[2] Note that "person" is used in this policy instead of "Individual" because "Individual" refers to a patient or his or her substitute decision maker; whereas, an inquiry or complaint may be made by anyone, including a person who is not a patient or his or her substitute decision maker.

Consent Directive	• A directive made by the Individual to give, withhold or withdraw, in whole or in part, his or her consent to the collection, use or disclosure of the Individual's PHI in the RM&R Solution for the purpose of providing or assisting in the provision of health care to the Individual, and includes a directive to modify or withdraw a directive that has already been made.
	• The following demographic information cannot be made subject to a Consent Directive because it is required to uniquely identify the Individual in the RM&R Solution for the purpose of managing privacy procedures related to the Individual and to ensure accuracy of the system data:
	  ○ First Name
	  ○ Last Name
	  ○ Gender
	  ○ Date of Birth
	  ○ Primary Address (street, postal code, city, province, country)
	  ○ Health Card Number (if available)
	  ○ Health Information Custodian (HIC) ID and MRN assigned by the HIC (if available)
	• Information on the RM&R dashboard when the individual is receiving care or treatment at the organization

Custodian	• Has the same meaning as "health information custodian" in PHIPA;
Data Sharing Agreement (DSA)	• The agreement signed amongst HICs participating in the RM&R Program
Electronic Service Provider	• Means a person who provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.
End-User	• Is any health professional or other authorized person who has been granted access to the RM&R Solution for the purposes of providing care or assisting in the provision of health care to an individual.
End User Agreement	• The agreement identified in paragraphs 4.1 to 4.3 of the *Privacy and Security Training Policy* and its associated procedures, as amended from time to time;
Executive Committee	• Is the group mandated to oversee the RM&R program, including the privacy and security program,
Global Consent Directive	• A Consent Directive made by the Individual to withhold or withdraw consent to the collection, use and disclosure of all of the Individual's PHI in the RM&R Solution[3] from all End Users of the RM&R Solution.
Health care	• Has the same meaning as in *PHIPA, 2004*.
Health Information Custodian (HIC)	• A HIC defined under *PHIPA*, *2004* which is also a participant in the RM&R Program.

[3] Future releases may include more than one domain and require this definition to be amended accordingly.

Health Information Network Provider (HINP)	• HINP has the same meaning as Ontario Regulation 329/04: "a person 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:.
Identity Management	• Allows provisioning of Administrator and user accounts for all the services in the RM&R system.
Individual	• A person whose PHI is retained in the RM&R Solution • May also include the person's substitute decision-maker if applicable (e.g., Request for Access).
Information security	• Refers to the protection of all types of information, information systems and information technologies from unauthorized access, collection, use, disclosure, transfer, disruption, modification, destruction or disposal.
Information security incident	• Any violation or imminent threat of violation of information security policies, standards, procedures or practices or any information security event that may compromise operations or threaten the security of an information system or business process.
Information system	• A discrete set of information technology organized for the retention, collection, processing, maintenance, use, disclosure or disposition of information.
Integrated Environment	• Refers to a Participating Organization that accesses the RM&R application via that organization's Hospital Information System, by way of a Single Sign-On protocol.
Inquiry	• A question raised by any person in respect of the RM&R Solution including, but not limited to, questions raised in respect of: o When, how and the purposes for which PHI in the RM&R Solution is collected, used and disclosed; o The administrative, technical and physical safeguards and practices maintained with respect to PHI in the RM&R Solution; o The policies, procedures and practices implemented in respect of the RM&R Solution; and o Compliance with *PHIPA*, *2004*.
IPC	• Is the office of the Information Privacy Commissioner of Ontario.
Logging	• The process of recording a pre-defined set of HIC, agent or Electronic Service Provider or information system or network activities. The automated logging processes serve as the basis for establishing audit trails for activities and events on an information system.
Non-integrated environment	• Refers to a Participating Organization that accesses RM&R/ORBIT independent of any of that organization's Hospital Information Systems (see also *integrated environment*).
Originating HIC	• Means the Participant that has collected or compiled PHI, a copy of which is transferred to the RM&R System;

Participant	• Means a HIC engaged in the Project;
Patient	• Means a recipient of health care services from an Originating HIC;
PHI	• Personal Health Information • Elements of information that is personal health information within the meaning of *PHIPA*, *2004* that are in the RM&R Solution.
PHIPA	• Ontario's *Personal Health Information Protection Act, 2004*.
Privacy and Security Operations	• The Privacy and Security Operations Team is made up of RM&R agents who support RM&R privacy and security-related activities, initiatives and processes.
Privacy Breach	• A Privacy Breach[4] includes circumstances where: o A provision of the Personal Health Information Protection Act, 2004 (*PHIPA*) or its regulations has been or is about to be contravened; o The privacy provisions of the Participation Agreement, End User Agreement or any other agreement in respect of the RM&R Solution have been or are about to be contravened; o The privacy policies, procedures and practices implemented in respect of the RM&R Solution have been or are about to be contravened; o PHI in the RM&R Solution is lost or stolen or has been or is about to be accessed by an unauthorized person; or o Records of PHI in the RM&R Solution have been or are about to be copied, modified or disposed of in an unauthorized manner.
Privacy Law	• Any privacy laws applicable to Participants including but not limited to *PHIPA*, *2004*.
Privacy and Security Working Group (PSWG)	• Means the group mandated to develop privacy and security guidelines and policies, approve privacy and security requirements, review and oversee the privacy program, and report to the RM&R Executive Committee on the adherence of RM&R to legal and privacy requirements and privacy best practices. The group is comprised of privacy and security knowledgeable representatives from each Healthcare sector participating in RM&R to support the privacy and information security governance structure.
Provider	• Means a health care provider that is an Agent of an Originating HIC.
Request for Access	• A request made by an Individual to exercise the right under Part V of the *Personal Health Information Protection Act, 2004* (*PHIPA*) to access the Individual's records of PHI in the custody or control of a HIC. • Without limiting the generality of the foregoing, an Individual may make a request for access to the following records in respect of the RM&R Solution: o Clinical records of the Individual; o Records of all instances where all or part of the PHI of the Individual is viewed, handled or otherwise dealt with by HICs or their agents and Electronic Service Providers;

[4] Note that "breach" is the term used in this policy. Some HICs may use the term "incident".

	○ Records of all instances where a consent directive is made, withdrawn or modified by the Individual; and ○ Records of all instances where a consent directive made by the Individual is overridden and the purpose for which the consent directive is overridden.
Request for Correction	• A request made by an Individual to exercise the right under Part V of *PHIPA, 2004* to request a correction of the Individual's records of PHI that the Individual believes are inaccurate or incomplete for the purposes for which the PHI has been collected or used or is being used.
RM&R	• Means the RM&R Program, including the RM&R system, run by the University Health Network (UHN), including services provided by Service Providers to UHN.
RM&R Executive Committee (EC)	• The committee mandated to approve strategies, escalate and/or resolve issues and risks, make decisions on key strategic objectives and deliverables and consider and, as applicable, approve recommendations of the Privacy and Security Working Group (PSWG) for the Program.
RM&R Services	• The services that RM&R agrees to provide in connection with the RM&R Solution from time to time, as described in the Data Sharing Agreement and Description of Services.
RM&R Solution	• The RM&R solution is a system that enables the electronic matching of patients to appropriate clinical programs/services and transmission of electronic referrals between 85 acute, rehabilitation, complex continuing care, home care, and long-term care and community support health service providers (HSPs).
Substitute Decision Maker	• Means SDM, as defined in PHIPA;
Security Breach	• Has the same meaning as in the *RM&R Information and Information Technology Policy (PS.Pol.101)* and its associated procedures, as amended from time to time;
Suppliers	• Means suppliers of information technology that have entered into an agreement with UHN as Agent of the Originating HICs for software and services.
User	• Any person (i.e., a HIC, agent or Electronic Service Provider of either a HIC or RM&R) that is assigned an ID to the RM&R Solution.

Background

Resource Matching and Referral is a shared web-based application that matches patients to appropriate clinical programs/services and sends electronic referrals from sending organizations to receiving organizations. The program has been developed and is managed by University Health Network (UHN) and funded by Toronto Central Local Health Integration Network (TC LHIN). To deliver the program, UHN has implemented a technology solution (RM&R solution) provided by Strata Health Solutions (Strata); this solution supports an electronic referral and matching process.

The application is currently live in over 80 acute, rehabilitation, complex continuing care, home care, long-term care and community support health service providers in Toronto Central and Central LHIN. It was introduced in Toronto Central LHIN in 2008 and in Central LHIN as of 2011.

The RM&R system streamlines the referral process and thereby reducing the length of time that patients in acute care wait to be matched to programs that can better address their clinical needs. Once it is determined by a clinical care team that a patient no longer needs to occupy an acute care bed they are referred to alternate level of care (ALC) programs or services. Examples of ALC programs include Long-Term Care homes, Rehab clinics or Continuing Complex Care programs. A paper-based referral process can be time-consuming and ineffective in appropriately matching patients to programs that could support their needs; long wait times may be a result.

The Resource Matching & Referral program provides clarity and efficiency by creating an electronic solution for the referral process. Clinicians log into the RM&R application and enter the pertinent data required to match a patient to an appropriate ALC programs or services. Referrals are immediately sent to applicable ALC organizations. The receiving ALC organization, after examining the patient's data, may either choose to accept or decline the referral or submit a request for more information. By creating a centralized tool, the RM&R application, Health Service Providers can match patients to the most appropriate programs and services in a timely manner. The tool also provides a clear methodology to identify capacity issues and service gaps. Lastly, the RM&R application is a single repository of referral-related information used by Health Service providers.

2 Privacy and Security Management Framework

The core principle of maintaining the privacy and security of personal health information (PHI) does not change with the introduction of privacy and security policies and procedures for the RM&R Program. The policies and procedures continue to uphold the basic principle of ensuring the privacy and security of Individuals and their PHI. However, operationalizing that same principle changes as we move from a health care system where paper, couriers and faxes are replaced with centralized, electronic repositories of PHI, enabling providers access to an individual's PHI no matter who collected the PHI initially.

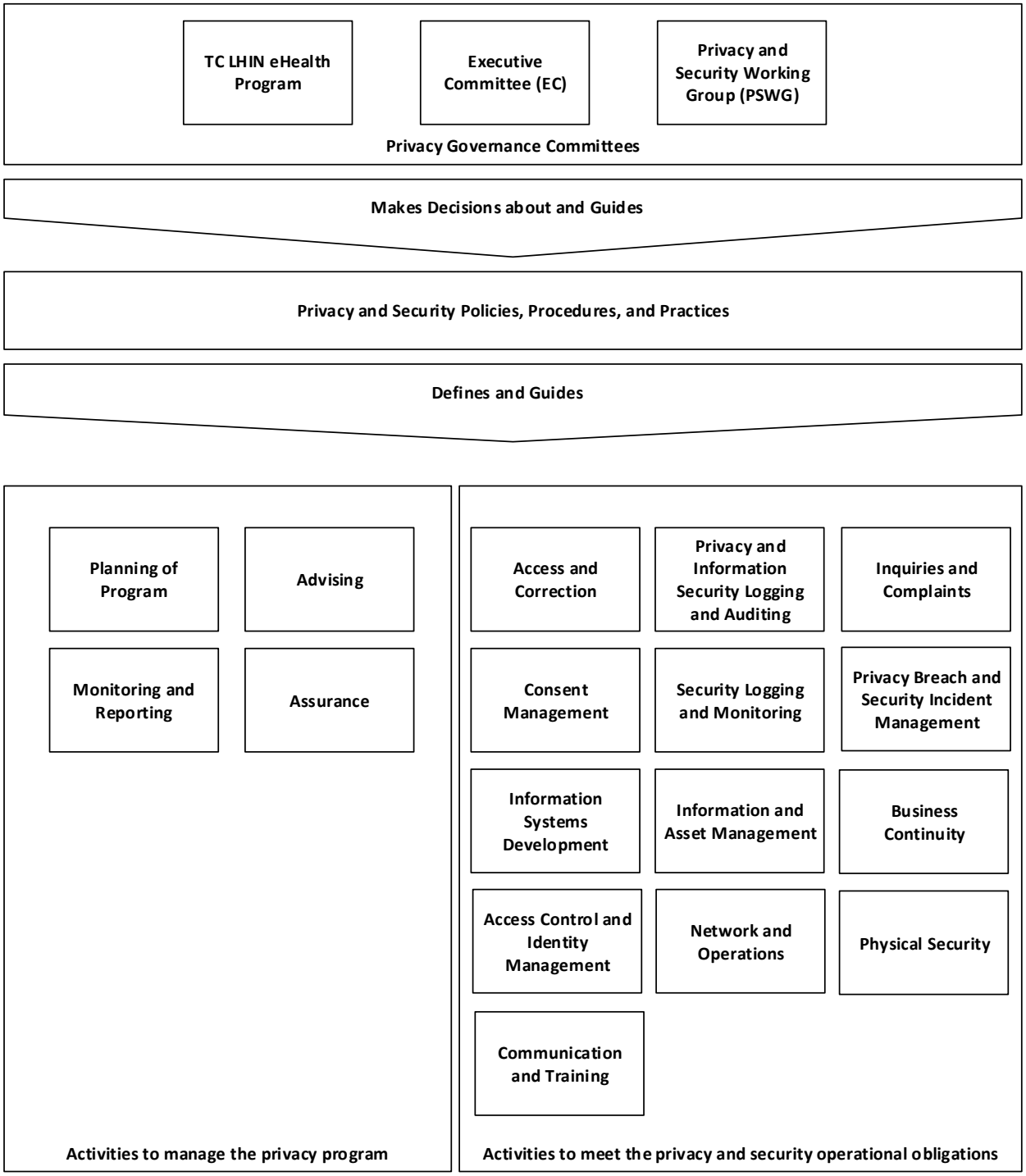
The RM&R's Privacy and Security Program builds on the following principles:

- Extends, not replaces, HICs' existing privacy and security programs to connect them with the privacy and security programs of all the other organizations
- Ensures that each HIC is meeting the same basic obligations and standards for privacy and security
- Establishes mutual trust amongst the HICs that the others afford the same level of protection to PHI and Individuals that they themselves do
- Supports individual rights under *PHIPA*, *2004*

Overview

Privacy and security management for RM&R involves a comprehensive framework of people, processes, and technology. It is broken into a number of domains[5] that will be developed as the RM&R Solution continues to evolve.

[5] Adapted from http://www.blueimpact.info/framework/


TC LHIN eHealth Program
Executive Committee (EC)
Privacy and Security Working Group (PSWG)
Privacy Governance Committees
Makes Decisions about and Guides
Privacy and Security Policies, Procedures, and Practices
Defines and Guides
Planning of Program
Advising
Monitoring and Reporting
Assurance
Activities to manage the privacy program
Access and Correction
Privacy and Information Security Logging and Auditing
Inquiries and Complaints
Consent Management
Security Logging and Monitoring
Privacy Breach and Security Incident Management
Information Systems Development
Information and Asset Management
Business Continuity
Access Control and Identity Management
Network and Operations
Physical Security
Communication and Training
Activities to meet the privacy and security operational obligations

Privacy and Security Domains

The privacy and security domains are summarized briefly below. See Sections 4 and 5 for a more comprehensive understanding of them.

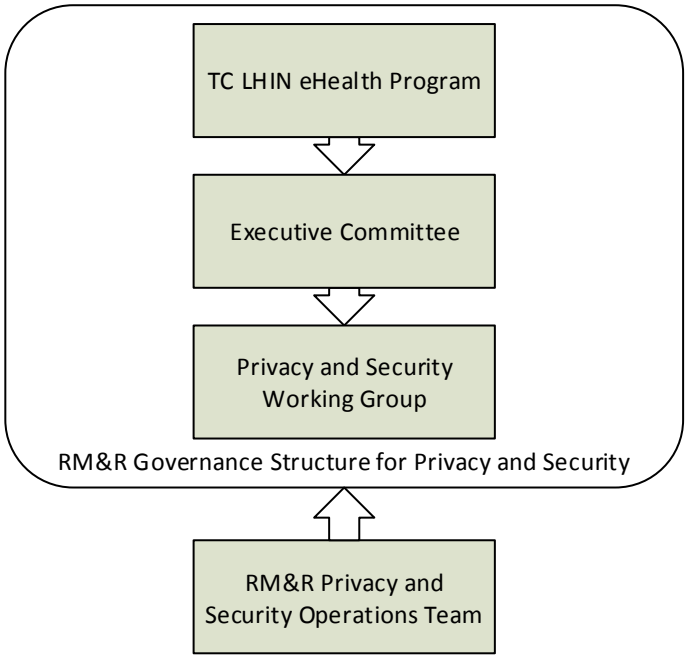
- **Governance Committees**
  - Authorities for privacy and security decision-making within the RM&R Program[6]
- **Privacy and Security Policies, Procedures, and Practices**
  - Define the Privacy and Security Program in accordance with legislation and Program objectives
  - RM&R Privacy Policies and associated sub-policies
  - RM&R Information Security Policies and associated sub-policies
- **Activities to Manage the RM&R Privacy and Security Program**
  - Planning of Program – planning for programmatic changes and enhancements to the Privacy and Security Program
  - Advising – provision of advisory and consultation services to the RM&R Program teams (e.g., PIAs, sitting in on design sessions)
  - Monitoring and Reporting – monitoring Program performance indicators and reporting back to the governance committees
  - Assurance – review of the effectiveness of the safeguards and controls, and whether those safeguards are being followed
- **Activities to Meet Operational Requirements**
  - Access and Correction – process of responding to an Individual's Request for Access to their own PHI and to have that PHI corrected if required
  - Privacy Logging and Auditing – ongoing review of system logs to review appropriateness of access and other indicators
  - Inquiries and Complaints – process of responding to an individual's inquiry about the RM&R Program or addressing a complaint about the RM&R Program
  - Privacy Breach Management - process of managing suspected or real breaches from initial identification to closure; some HICs may know it as incident management
  - Consent Management – process of both obtaining consent and managing consent directives
  - Security Logging and Monitoring – monitoring and reviewing security logs to identify and act upon threats to the confidentiality, availability, or integrity of the RM&R Solution

[6] The RM&R governance model includes other committees to oversee other areas of operation. This document only highlights those with direct involvement in the privacy and security governance.

- Information Systems Development Lifecycle – controlling development and changes to information systems to ensure that the feed of PHI into the RM&R Solution is not disrupted and the HIC's access to the RM&R solution is not disrupted
- Information and Asset Management – controls for protecting PHI throughout its information lifecycle
- Business Continuity – processes associated with maintaining the availability of the RM&R Solution by developing a resilient technical infrastructure
- Physical Security – controls associated with physically protecting information technology that is used to process, store, and transmit PHI
- Network and Operations – controls associated with implementing and maintaining secure networks and information systems used to process, store and transmit PHI
- Access Control and Identity Management – process for verifying identity and granting access to the functionality and PHI retained in the RM&R Solution
- Security Incident Management – identifying security events and managing them to resolution if they threaten or breach the security of the RM&R Solution

3 Privacy and Security Governance

The RM&R Program uses a representational model to govern the initiative. The RM&R Program encourages representation from all of its stakeholder groups to govern the initiative, and to ensure that the decisions reflect the collective needs and interests of the stakeholders responsible for delivering the RM&R Program[7]. This same approach is used for governing privacy and security within the RM&R Program.



The TC LHIN eHealth Program provides high-level direction and funding for the RM&R program.

The Executive Committee (EC) has overall accountability for the RM&R program, with privacy and security being a component of their oversight.

The EC works with the broader program governance framework and is supported by a Privacy and Security working group (PSWG) responsible for providing ongoing privacy and security advice and consultation. The PSWG is comprised of a representative from each Healthcare sector participating in RM&R, and makes decisions on behalf of all the HICs.

Each of these bodies has a distinct yet integrated role in governing the RM&R Privacy and Security Program. These roles are described in greater detail in the Terms of Reference (copies of which can be found in *Privacy Policy*), however at a high-level their roles are explained below.

RM&R Executive Committee (EC)

The RM&R Executive Committee has overall accountability for RM&R. Its role is to:

[7] The RM&R governance model includes other committees to oversee other areas of operation. This section only highlights those with direct involvement in the privacy and security governance.

- provide direction and sponsorship, including approving strategies, providing support for communications to stakeholders and escalating and/or resolving issues and risks;
- secure the required participation and engagement of the LHINs and participants;
- make decisions on key strategic objectives and deliverables; and
- consider and, as applicable, approve recommendations of advisory bodies.

Privacy and Security Working Group

The Privacy and Security Working Group (PSWG) is an ad hoc advisory committee providing expertise on operational privacy and security matters. The group includes healthcare sector privacy and security expertise provided by HICs participating in the RM&R Program, a representative of the RM&R program and one representative from the TC LHIN. The PSWG supports management of tactical operational planning and issues management role which includes to:

- identify, develop and validate privacy and security requirements;
- review and oversee the Privacy and Security Program, including any changes to address issues identified in audits and incident reports;
- report to the RM&R Steering Committee on the adherence of the RM&R Program to legislative and privacy requirements and privacy best practices; and
- carry out any additional responsibilities assigned from time to time by the RM&R Steering Committee.

Privacy and Security Operations Team

The EC and PSWG are supported by Privacy and Security Operations Team who are responsible for the day-to-day operations of RM&R's privacy and security programs. Their role includes:

- Develop and update privacy and security policies and procedures
- Review and update privacy and security provisions in agreements
- Monitor and provide dashboard-level reporting on privacy and security operations
- Manage privacy and security risks of the RM&R Solution
- Manage the compliance to legislation, agreements, and policies/procedures
- Manage and coordinate privacy and security operations of the RM&R Solution
- Manage the assessment of new HICs from a privacy and security perspective
- Perform research and analysis
- Prepare supporting and background materials for the privacy and security governance committees

4 Policies and Procedures Overview

RM&R has developed a comprehensive suite of policies and procedures to which HICs must adhere in RM&R to ensure a mutual level of protection and trust.

The policies, procedures, and practices will be reviewed from time to time by the PSC who may recommend changes based on the results of its review to the RM&R Executive Committee. Approved changes will be forwarded to HICs via an updated Privacy and Security Manual.

- Privacy Policy (PS.Pol.001)
- Access and Correction Policy (PS.Pol.002)
- Consent Management Policy (PS.Pol.03)
- Inquiries and Complaints Policy (PS.Pol.004)
- Logging and Auditing Policy (PS.Pol.005)
- Privacy Breach Management Policy (PS.Pol.006)
- Privacy and Security Training Policy(PS.Pol.007)
- Retention Policy (PS.Pol.008)
- Assurance Policy (PS.Pol.009)
- RM&R Information Security Policy (PS.Pol.101)

Privacy Policy (PS.Pol.001)

Summary

The purpose of this policy is to protect the privacy of Individuals whose personal health information (PHI) is retained in the RM&R System, and facilitate compliance of HICs, RM&R, and their agents and Electronic Service Providers with the Personal Health Information Protection Act, 2004 (PHIPA).

The core concepts addressed in this policy are:

Guiding Principles

Following the Privacy by Design principles, the RM&R Program will:

- be compliant with PHIPA and orders from Information and Privacy Commissioner of Ontario;
- respect the Individual's privacy and provide them with an easy and consistent experience; and
- ensure their trust through transparency and accountability.

Roles and Responsibilities

- HICs have custody and control over the PHI that they contributed to the RM&R System or viewed for health care purposes
- RM&R has multiple roles under PHIPA depending on the services being provided, including agent of the HICs, and health information network provider

Governance

- The RM&R Privacy and Security Working Group and RM&R Executive Committee each have a role in managing or overseeing privacy and security which are defined in their terms of reference

Sub-Policies

- The sub-policies govern the specific obligations of the HICs and RM&R

Policy

- Privacy Policy (PS.Pol.001)

Required Forms

The HIC is not required to use a RM&R form or document to support this policy.

Access and Correction Policy (PS.Pol.002)

Summary

The purpose of this policy is to define the policies and procedures that apply in receiving and responding to access and correction requests with respect to the RM&R System made by the Individual to whom the PHI relates. The key principles of the policy are:

If a HIC receives an access request

- If the request relates to PHI that was contributed or collected (i.e., viewed) by someone at your organization: respond to the request
- If the request relates to PHI that was contributed by one other HIC and that someone at your organization didn't previously collect (i.e., view): ask the person to contact the HIC that contributed the PHI to make the request
- If the request relates to PHI that was contributed by more than one other HIC and that some at your organization didn't previously collect (i.e., view): ask the person to contact RM&R

If the RM&R Program receives an access request

- If the request relates to PHI that was contributed by one HIC: RM&R will ask the person to contact the HIC that contributed the PHI to make the request
- If the request relates to logs (e.g., who accessed my PHI?): RM&R will respond to the request
- If the request relates to PHI that was contributed by more than one HIC: RM&R will coordinate the response and perform all the administrative functions

If a HIC receives a correction request

- If the request relates to PHI that was contributed by the HIC: respond to the request
- If the request relates to PHI that was contributed by one other HIC: ask the person to contact the HIC that contributed the PHI to make the request
- If the request relates to PHI that was contributed by more than one other HIC: ask the person to contact RM&R

If RM&R receives a correction request

- If the request relates to PHI that was contributed by one HIC: RM&R will ask the person making the request to contact the HIC that contributed the PHI to make the request
- If the request relates to PHI that was contributed by more than one HIC: RM&R will forward the request to the HIC(s) that contributed the PHI, coordinate the response and perform all the administrative functions

Policy

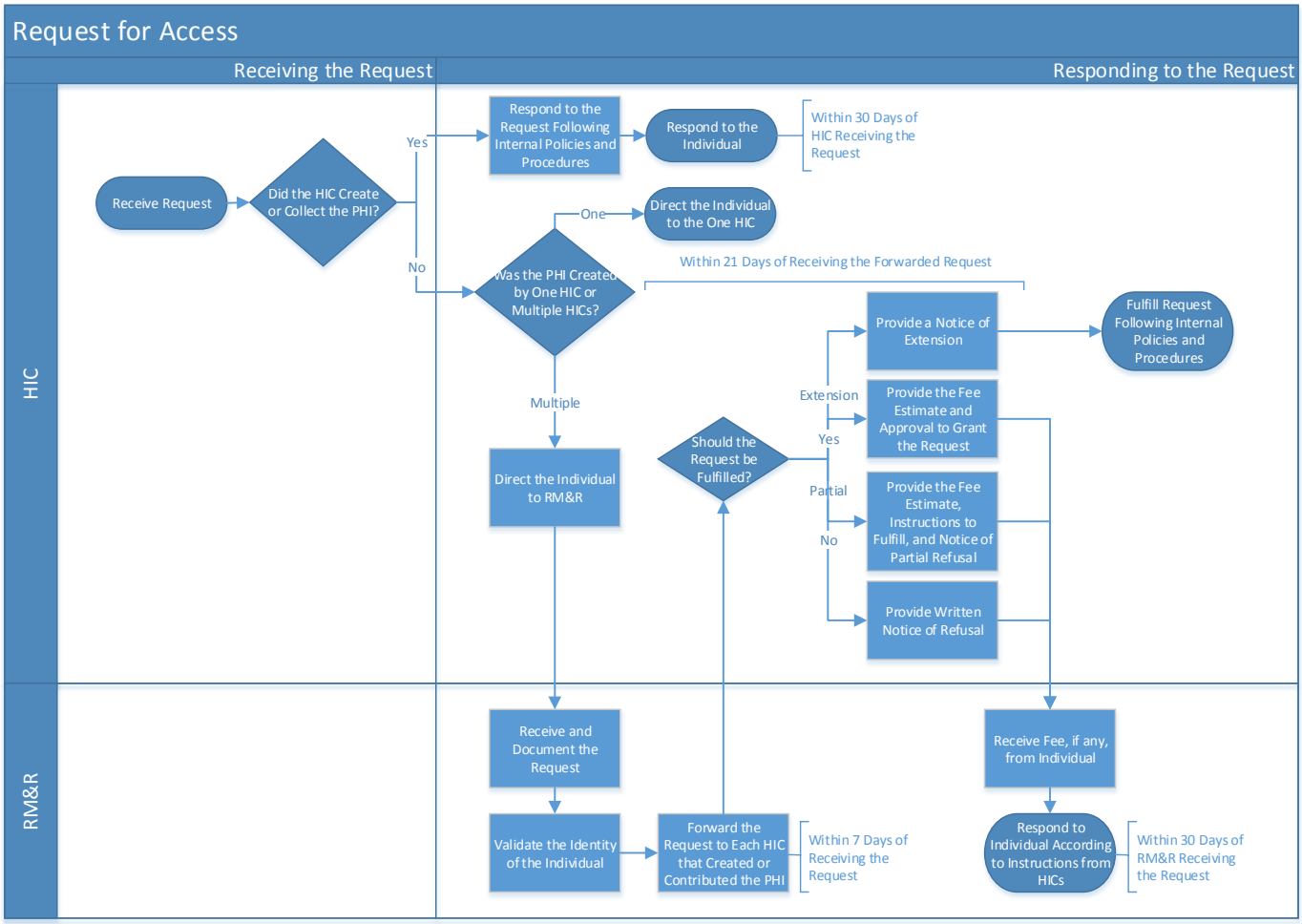
- Access and Correction Policy (PS.Pol.002)

Required Forms

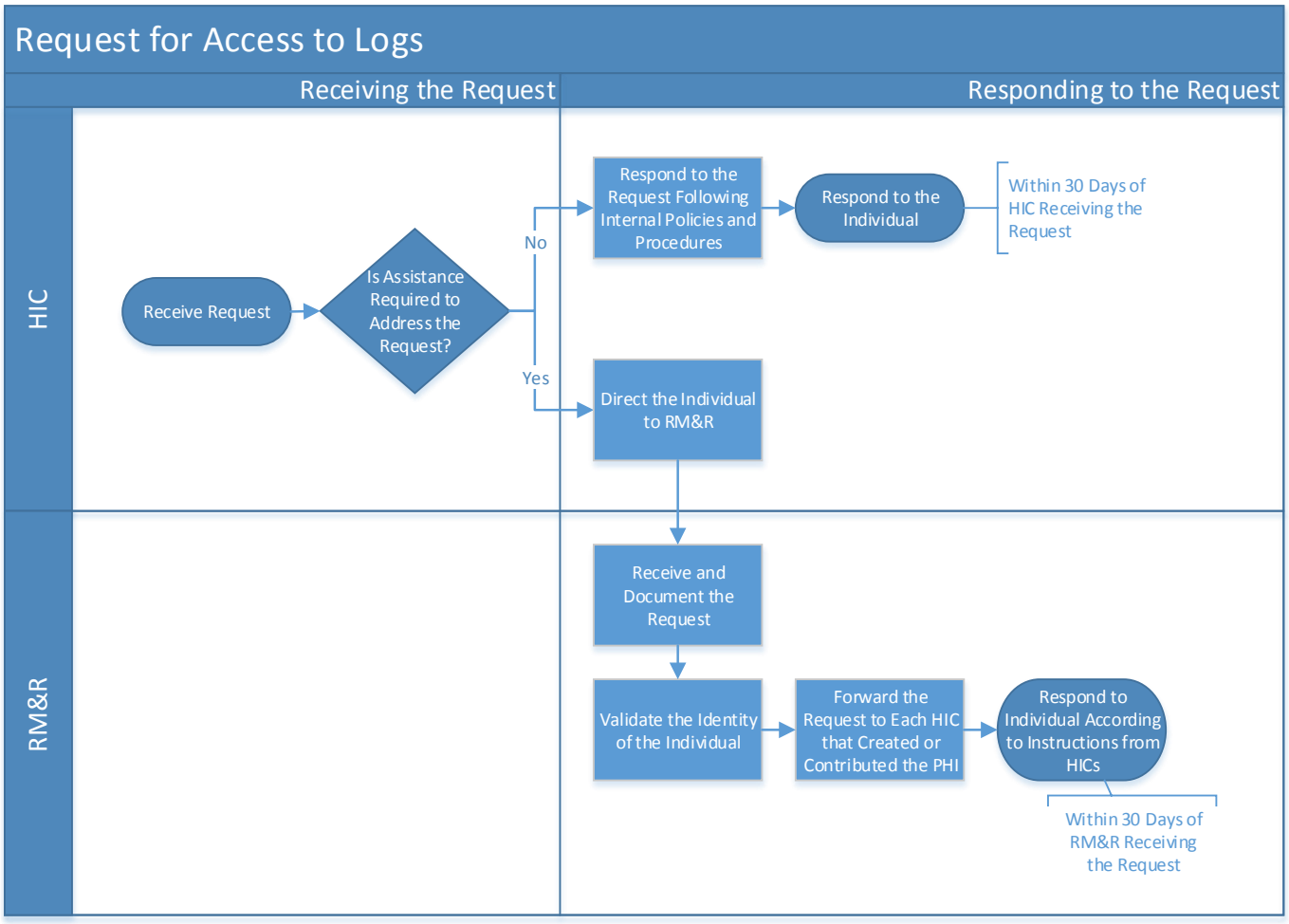
- Letter Refusing a Request for Access in Whole or in Part
- Letter Notifying of an Extension
- Instructions to RM&R to Notify HICs of a Correction to PHI

Process Summaries

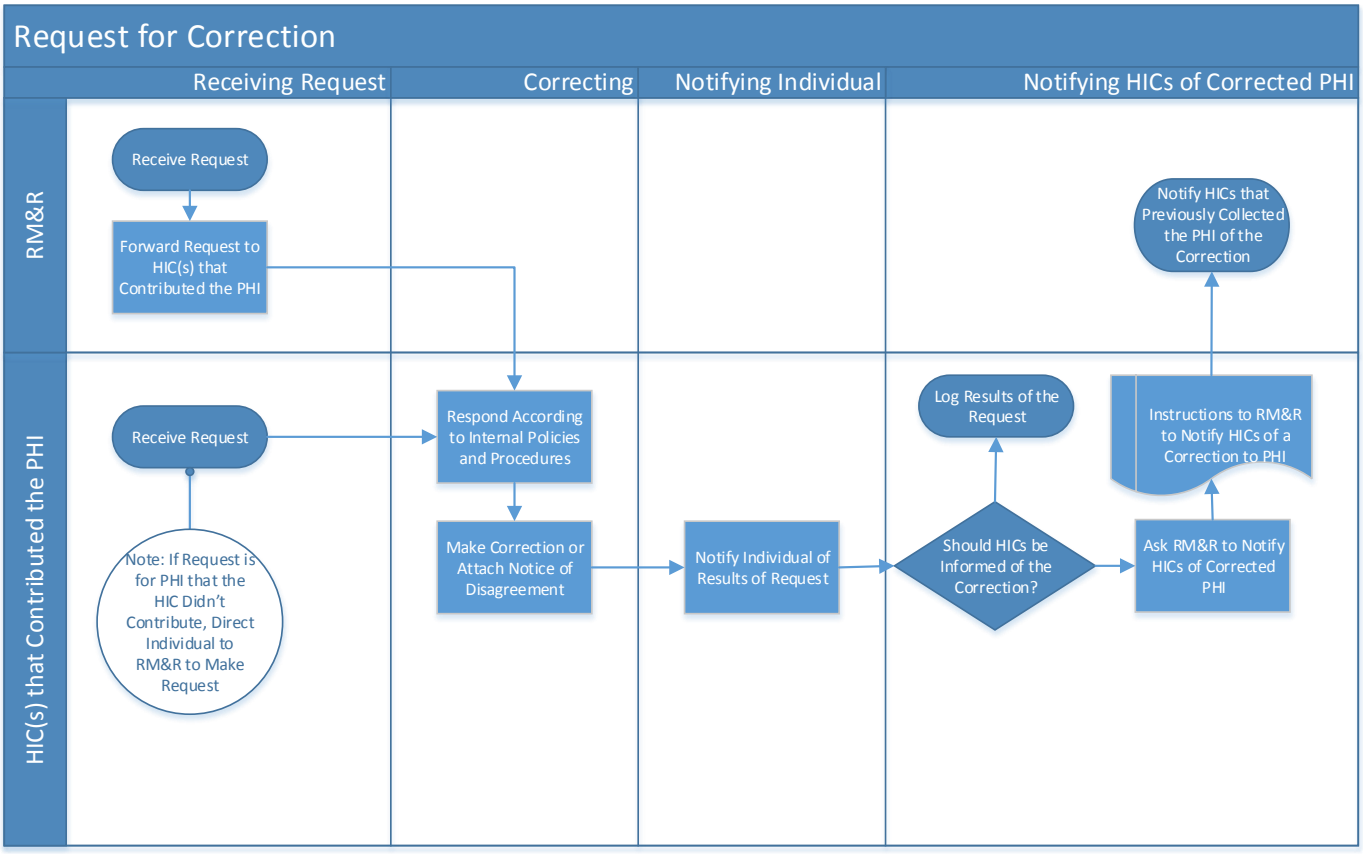
Managing a Request for Access



Managing a Request for Logs



Managing a Request for Correction



Consent Management Policy (PS.Pol.003)

Summary

The purpose of this policy is to define the policies and procedures that apply in obtaining the consent of the Individual in respect of the collection, use or disclosure of the Individual's PHI in the RM&R Solution, and that apply in making, modifying, withdrawing, or overriding consent directives in respect of PHI stored in the RM&R Solution. The key principles of the policy are:

Obtaining Consent

- HICs follow their existing policies and procedures regarding their approach to consent
- Need to add a generic statement to Notice of Purposes regarding participation in electronic health networks, and be able to provide patient with a brochure or direct them to the RM&R Program website for more information

Managing Consent Directives

- Follow internal policies and procedures to receive consent directive requests
- Apply, modify, or delete the consent directive if possible; if not, ask patient to contact the RM&R Program
- Provide notice to patient when request fulfilled

Consent Directive Override

- Review instances of overrides to ensure their appropriateness
- Provide notice to patient about override

Policy

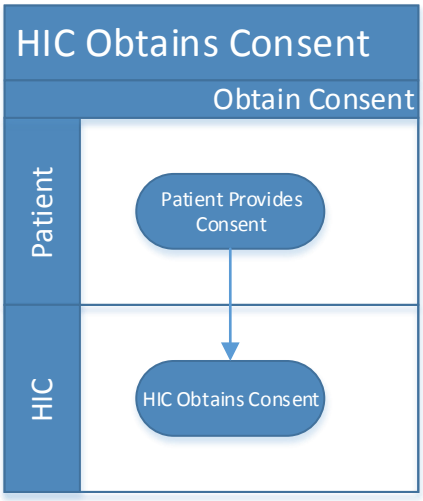
- Consent Management Policy (PS.Pol.003)

Required Forms

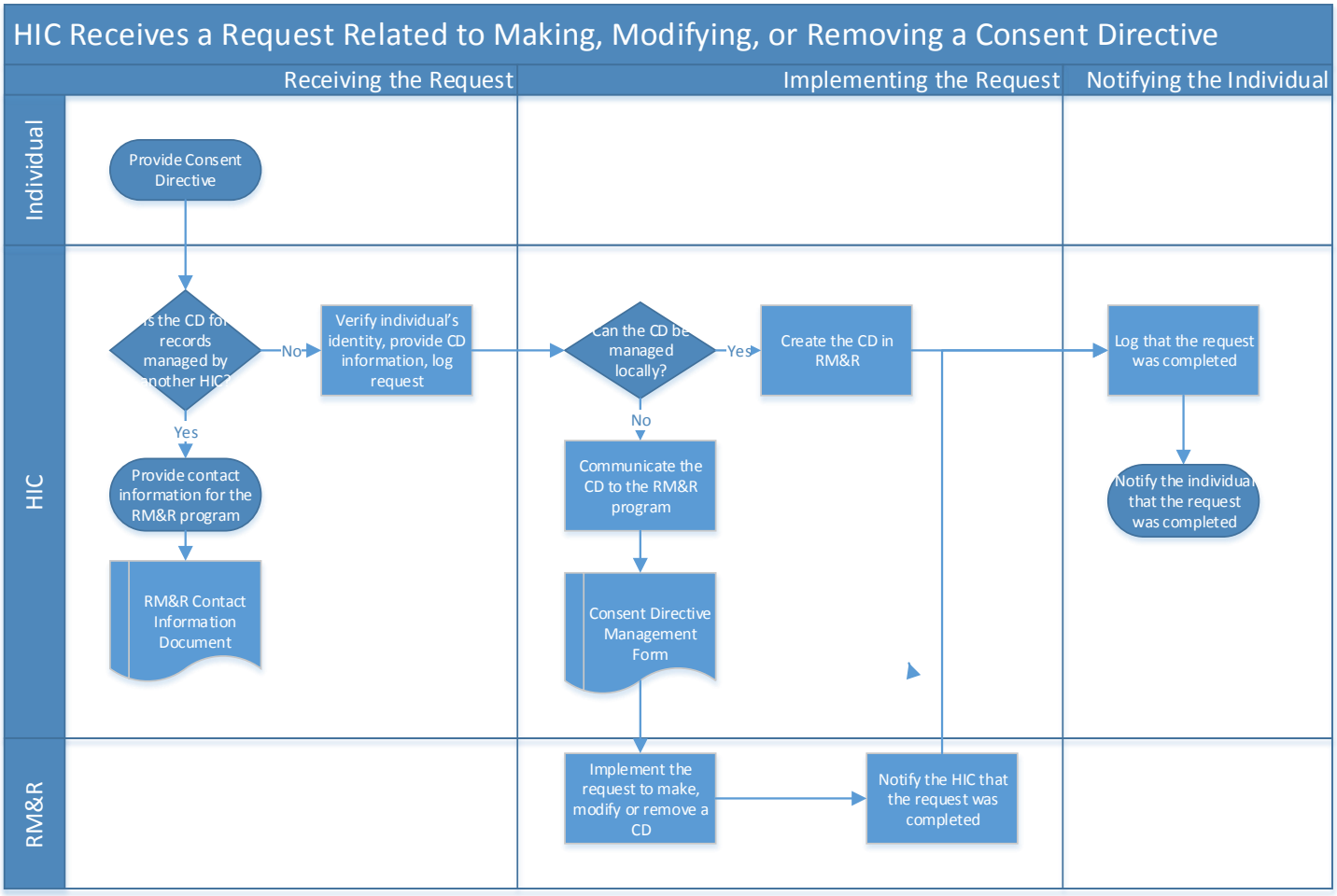
- The HIC is not required to use a RM&R form or document to support this policy.

Process Summaries

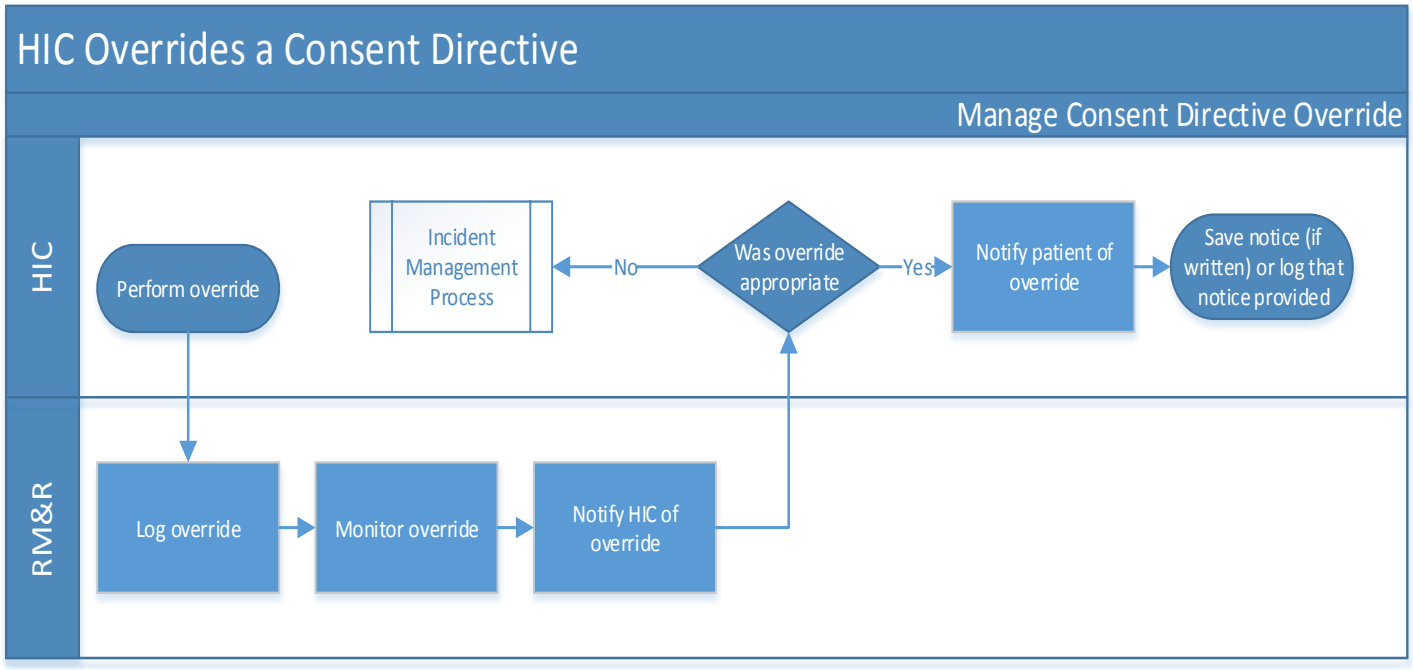
HIC obtains consent



HIC receives a Consent Directive



HIC overrides a Consent Directive



Inquiries and Complaints Policy (PS.Pol.004)

Summary

The purpose of this policy is to define the policies and procedures that apply in receiving, documenting, tracking, addressing and responding to Inquiries and Complaints in respect of the RM&R system. The key principles of the policy are:

If HIC or RM&R receives the Inquiry or Complaint

- Respond if it relates to your organization or if you can address it
- If the inquiry or complaint relates to one other organization and you can't address it, direct the individual to the other organization by providing the organization's contact information (See Contact List on RM&R Website)
- If the inquiry or complaint relates to multiple organization direct the individual to contact the RM&R Program (by phone at 1-844-653-1240, or by email at referrals@UHN.ca)

If RM&R receives an Inquiry or Complaint related to multiple organizations

- RM&R will notify each HIC to whom the Inquiry or Complaint relates of the Inquiry or Complaint
- Affected organizations will work together to determine a plan for responding to the Inquiry or Complaint, including timelines for drafting and review of response
- If the RM&R Program is responsible for coordinating a response, and a HIC does not respond within the agreed-upon timeframe, the Program will tell the patient there was no response and ask them to contact the HIC directly or make complaint to the IPC
- RM&R will provide a response to the Inquiry or Complaint
- Where a determination is made for a Complaint to be investigated, the investigation will be done according to the *Privacy Breach Management Policy (PS.Pol.003)*.

Policy

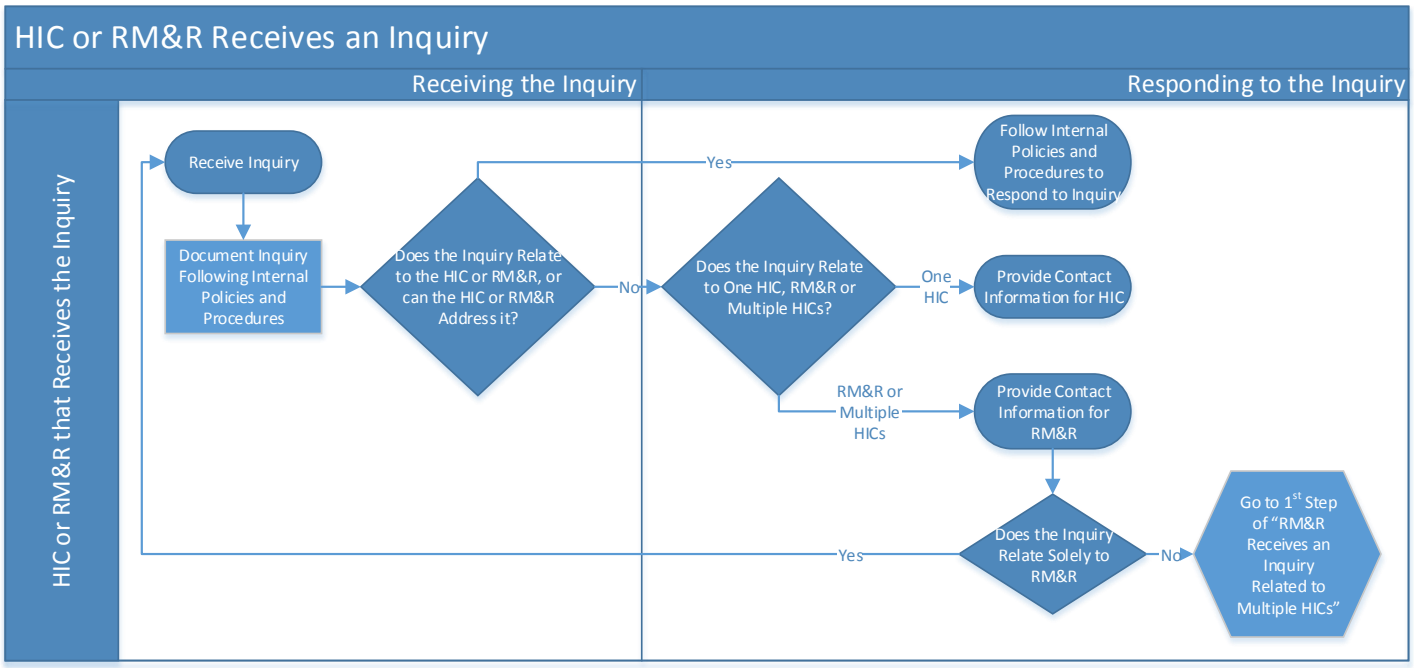
- Inquiries and Complaints Policy (PS.Pol.004)

Required Forms

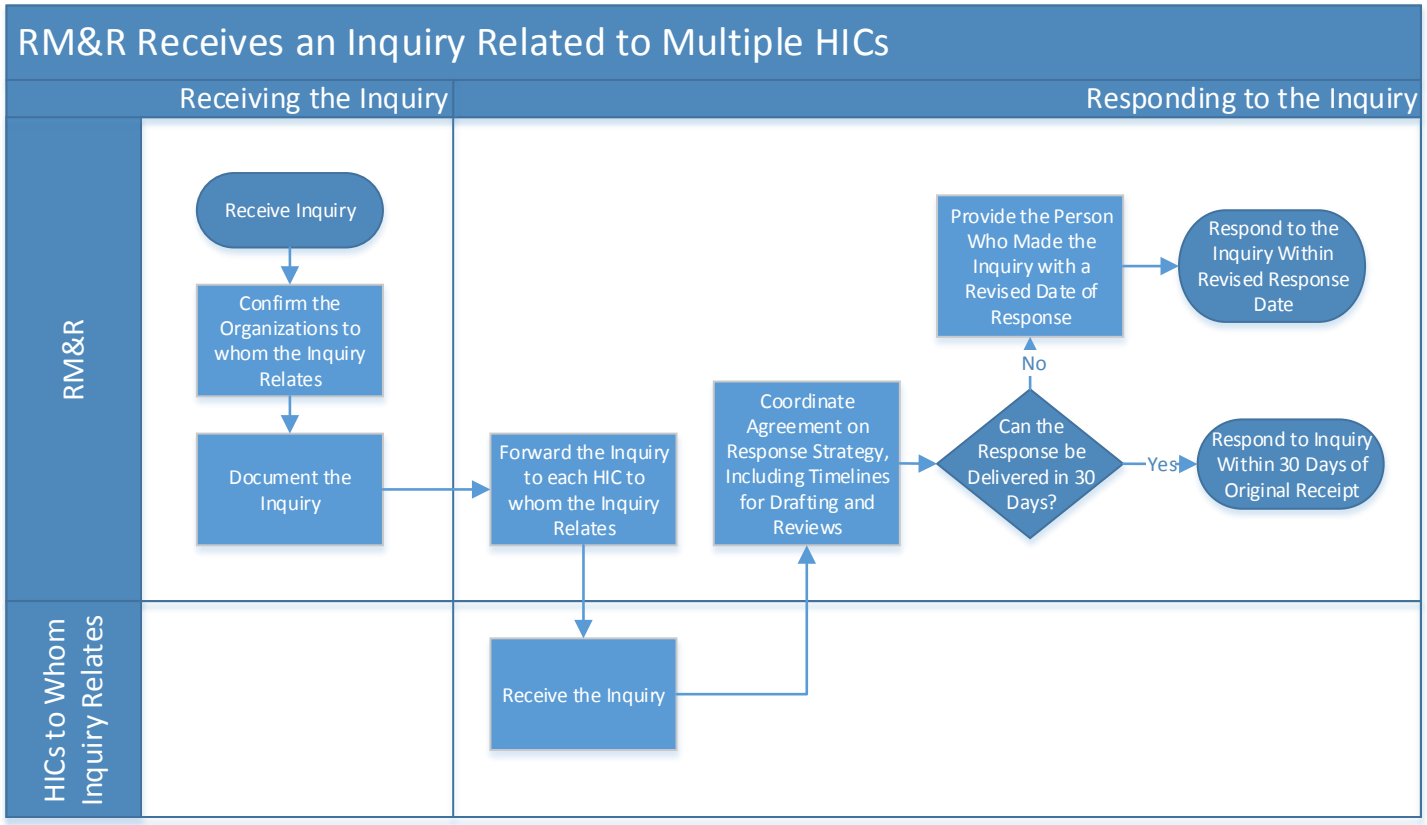
- The HIC is not required to use a RM&R form or document to support this policy.

Process Summaries

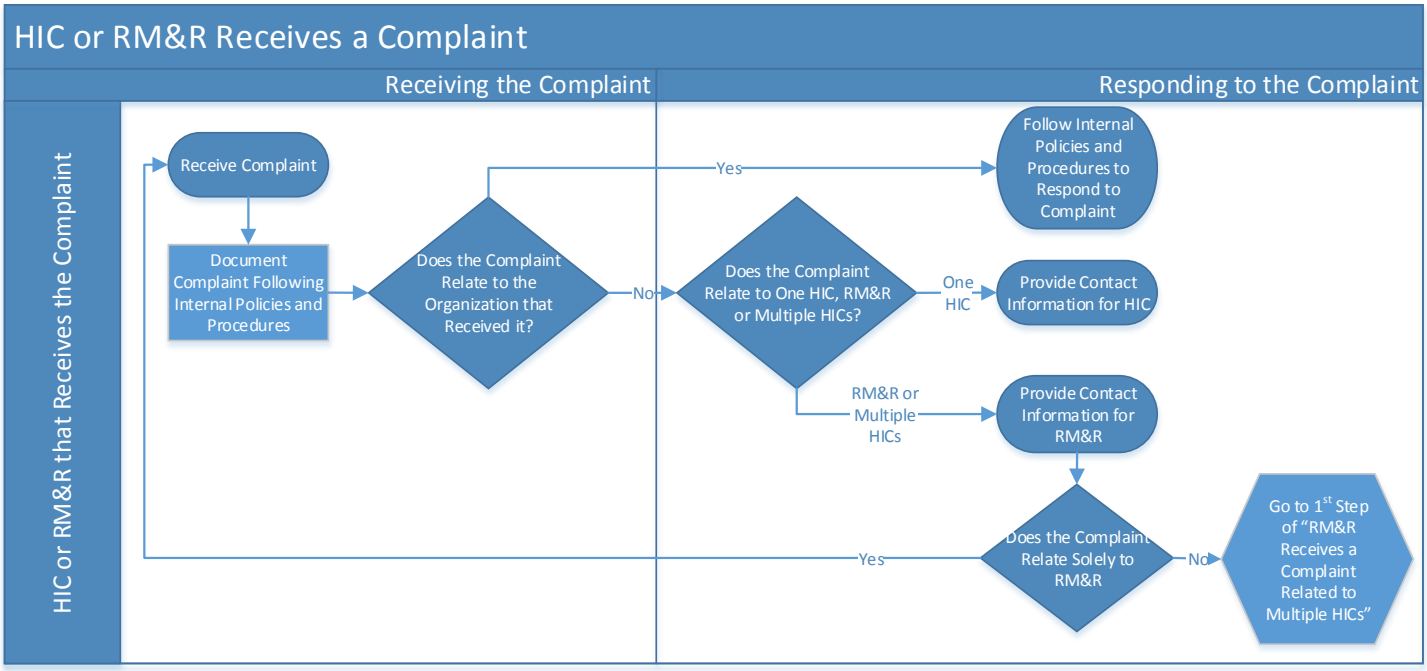
HIC or RM&R Receives an Inquiry



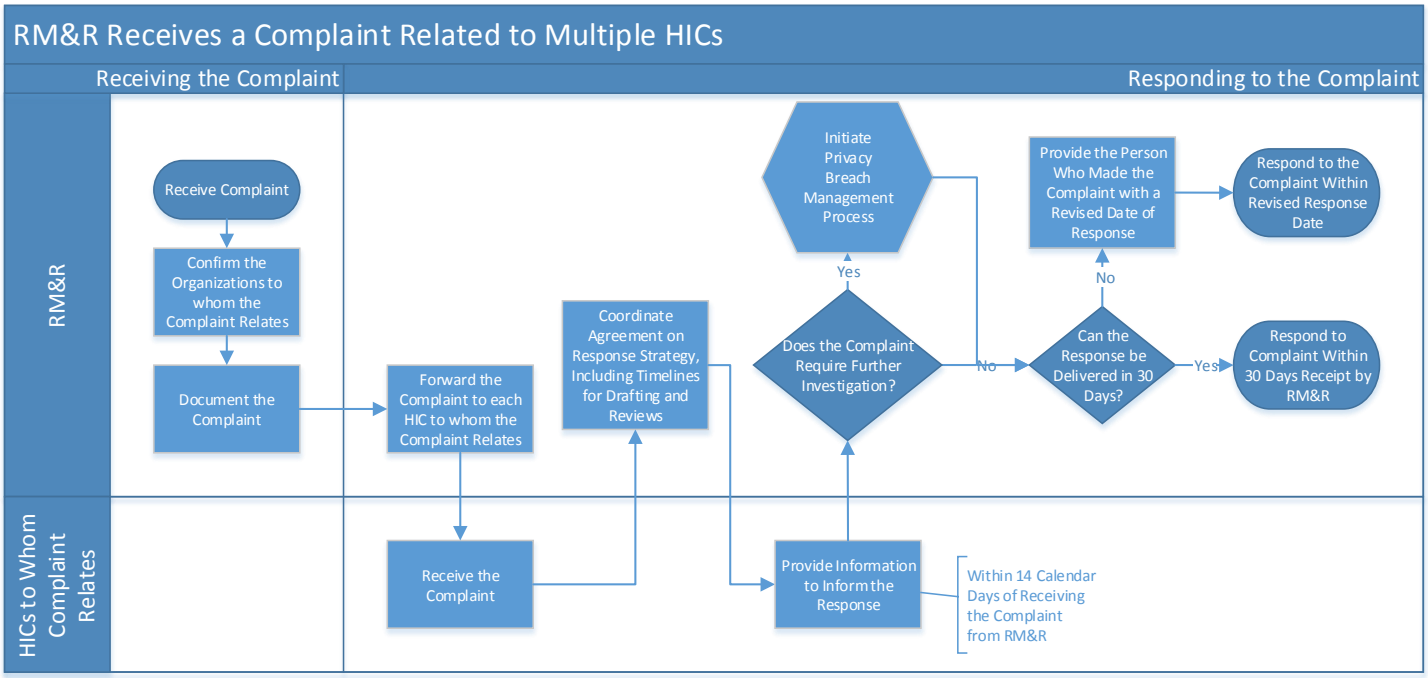
RM&R Receives an Inquiry Related to Multiple HICs



HIC or RM&R Receives a Complaint



RM&R Receives a Complaint Related to Multiple HICs



Logging and Auditing Policy (PS.Pol.005)

Summary

The purpose of this policy is to define the policies and procedures that apply in logging, auditing, and monitoring viewing, handling, and dealing with PHI, including the management and overriding of consent directives, stored in the RM&R System. The key principles of the policy are:

The Privacy and Security Working Group (PSWG) will:

- Define the standards associated with logging and auditing

HICs will review (based on standards to be established by PSWG):

- When one of their users views PHI
- When one of their users creates or overrides a consent directive
- When other users view PHI that the HIC contributed to the RM&R System to identify potentially suspicious activity
- When other users override a consent directive blocking disclosure of PHI that the HIC contributed to the RM&R System

The RM&R Program will review (based on standards to be established by PSWG):

- When their own users or those of their service providers (i.e., system administrators) view PHI in the RM&R System

Policy

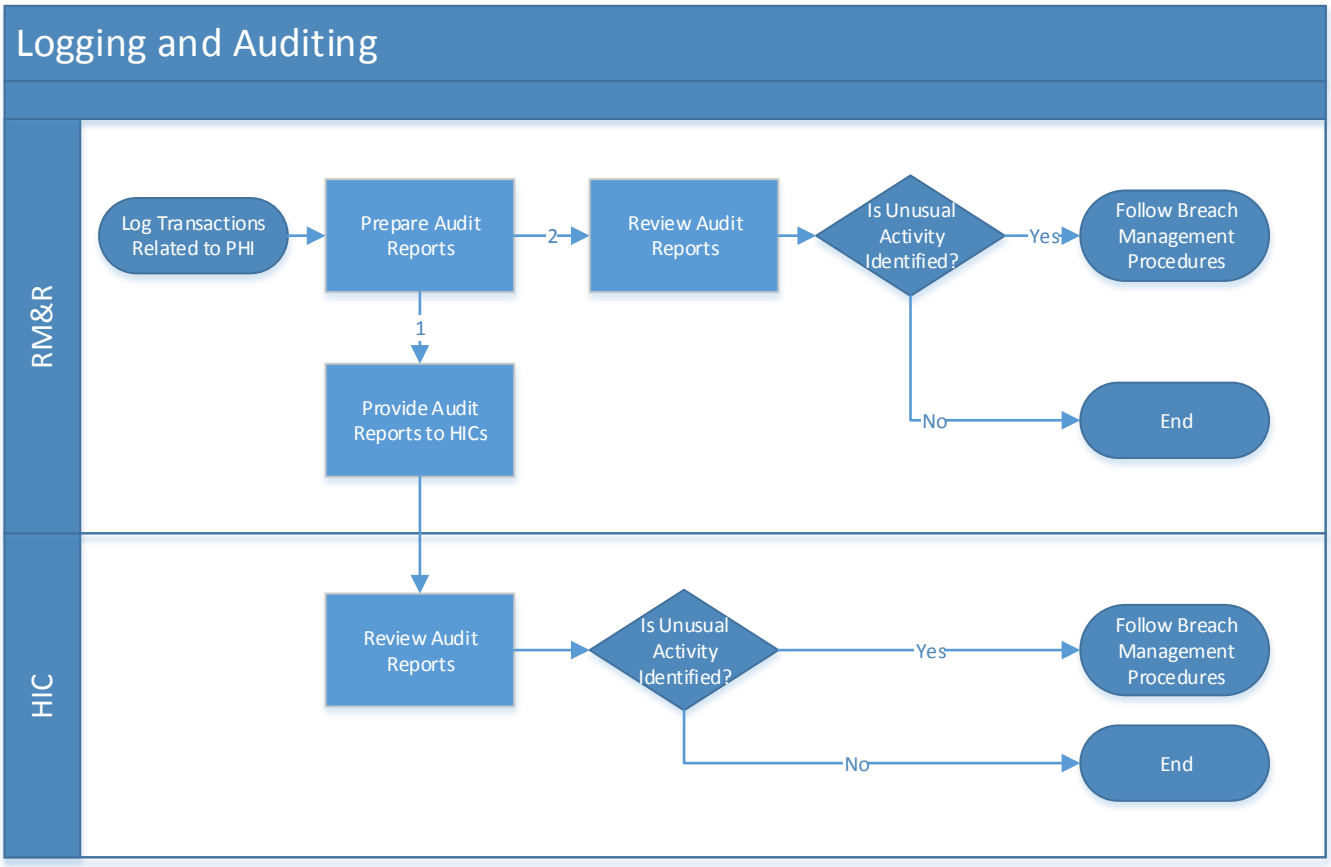
- Logging and Auditing Policy (PS.Pol.006)
- RM&R Information and Information Technology Policy (PS.Pol.101)

Required Forms

- The HIC is not required to use a RM&R form or document to support this policy.

Process Summaries

Logging and Auditing



Privacy Breach Management Policy (PS.Pol.006)

Summary

The purpose of this policy is to define the policies and procedures that apply in identifying, reporting, containing, notifying, investigating, and remediating Privacy Breaches in respect of the RM&R system. The key principles of the policy are:

- All breaches involving the RM&R system must be reported to RM&R (by phone at 1 (866) 556-5005, or by using the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx, the email to be directed to referrals@UHN.ca).
- All impacted HICs will be notified of the breach
- Impacted HICs and the RM&R program will choose a breach investigator and the appropriate HIC to notify the Individual as required
- The breach investigator will complete the breach report; impacted HICs will be able to comment on it
- The RM&R Program will provide the report to the RM&R Executive Committee for review and approval of remediation activities

Policy

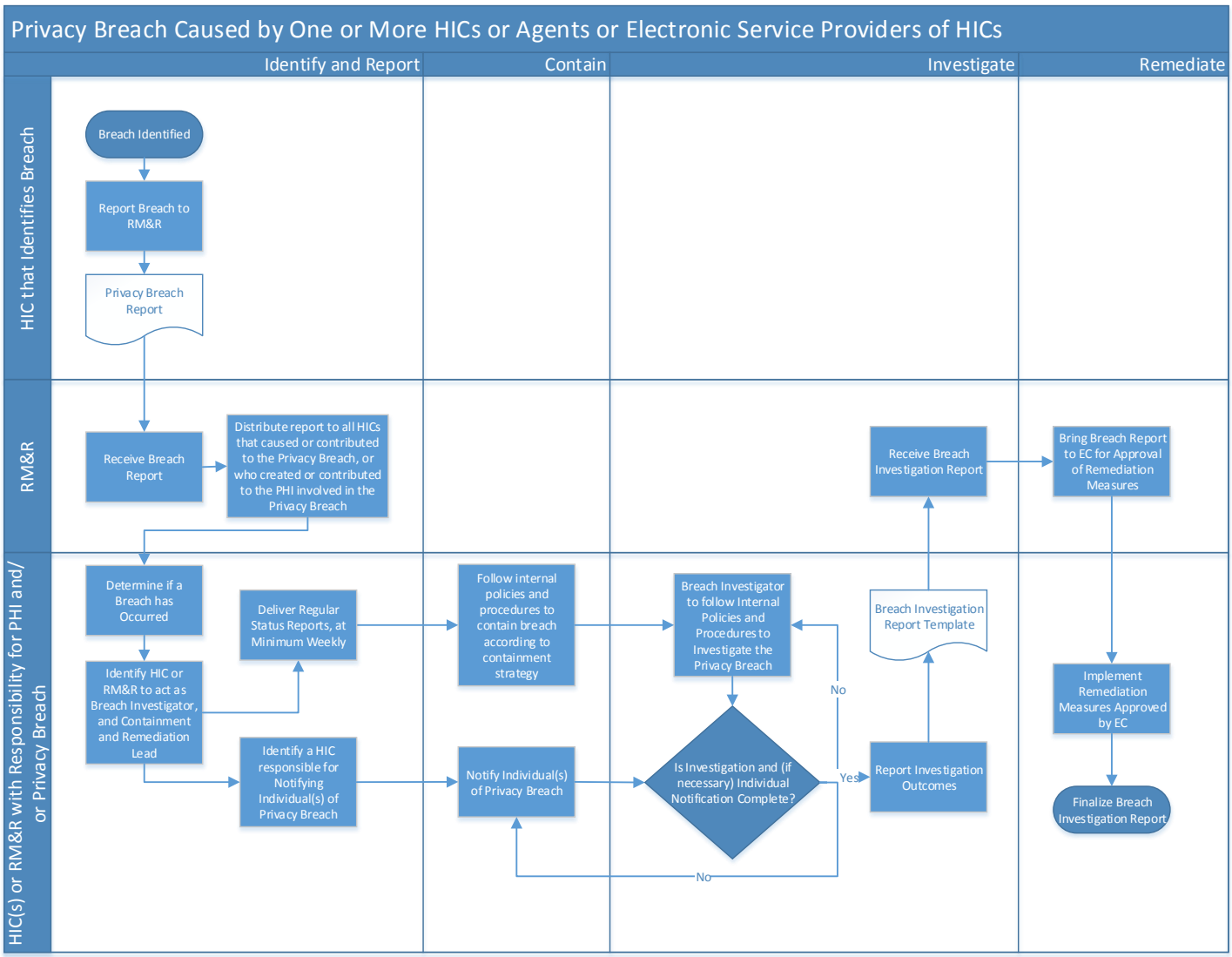
- Privacy Breach Management Policy (PS.Pol.006)

Required Forms

- Privacy Breach Report
- Privacy Breach Investigation Report
- Update on Status of Remediation Activities

Process Summaries

Privacy Breach Management Process



Privacy and Security Training Policy (PS.Pol.07)

Summary

The purpose of this policy is to define the policies and procedures for providing privacy and security training in respect to the RM&R system. The key principles of the policy are:

- All HICs and RM&R agents and electronic service providers must be made aware of their privacy and security obligations prior to being provisioned an account for the RM&R system
- HICs and the RM&R Program must be able to demonstrate on an ongoing basis that their agents and electronic service providers understand their obligations
- End-users sign an end-user agreement outlining base obligations

Policy

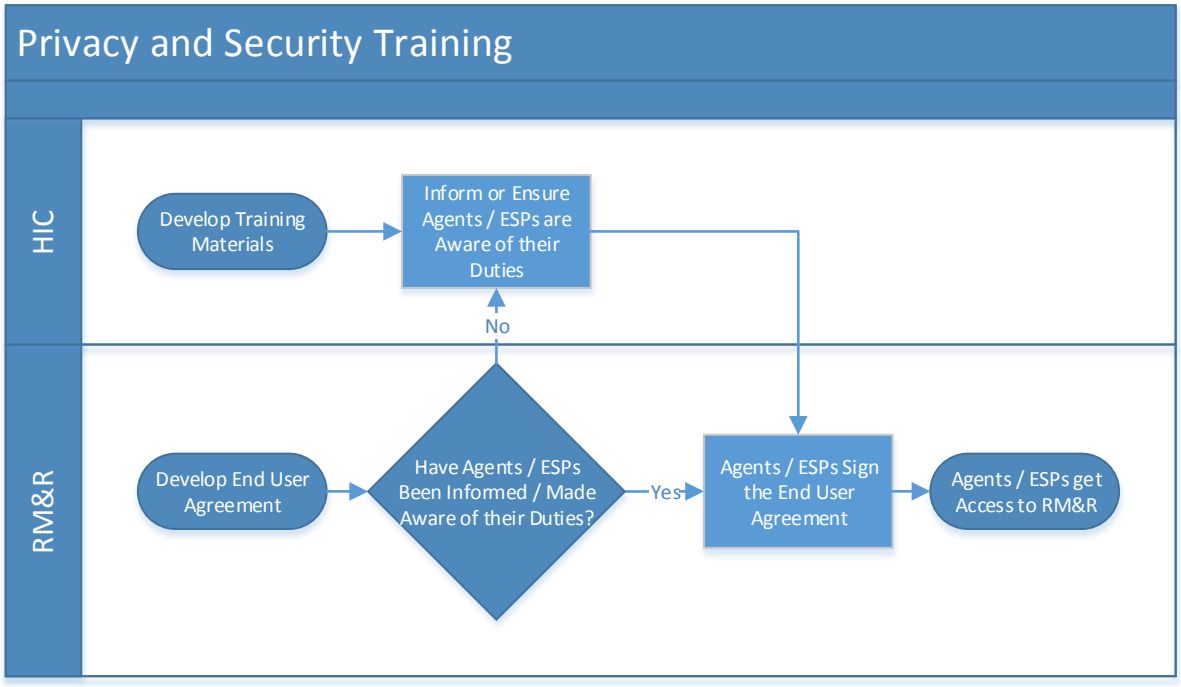
- Privacy and Security Training Policy (PS.Pol.07)

Required Forms

The HIC is not required to use a RM&R form or document to support this policy.

Process Summaries

Privacy and Security Training



Retention Policy (PS.Pol.008)

Summary

The key purpose of this policy is to define the policies and procedures that apply in retaining records of PHI in respect of the RM&R system and information collected from Individuals to assist in fulfilling their requests, responding to Inquiries or Complaints, or investigating a Privacy Breach. The key principles of the policy are:

Retention

- PHI in the RM&R System will be retained for 30 years or as long as the HIC retains the PHI, whichever is longer
- PHI that is collected or created about an Individual in response to a request, inquiry, complaint, or privacy breach will be retained for two years
- PHI will no longer be made available through the RM&R System if the HIC that contributed the PHI withdraws from the RM&R Program

Destruction

- PHI must be securely destroyed in accordance with the Information Security Policy after it is no longer required

Policy

- Retention Policy (PS.Pol.008)

Required Forms

The HIC is not required to use a RM&R form or document to support this policy.

Assurance Policy (PS.Pol.09)

Summary

The purpose of this policy is to outline the principles and activities that apply to the conduct of RM&R and the HICs who are contributing PHI, as well as those HICs subsequently collecting or viewing PHI, in the RM&R System. The key principles of this policy are:

- RM&R and HICs share a responsibility to undertake assurance activities that ensure the ongoing operations of the System and Program are compliant with law and are aligned with the expectations of patients.
- RM&R and HICs shall permit and cooperate with an audit or inspection in respect of the RM&R System and as aligned with relevant agreements.
- The RM&R and the Privacy and Security Working Group shall establish and maintain the assurance activities by/of all parties of RM&R.
- Instances of non-compliance, recommendations for responding to non-compliance and, if applicable mitigation plans to address non-compliance shall be reviewed by RM&R and the Privacy and Security Working Group (PSWG), who shall make recommendations to the RM&R Executive Committee (EC).

Policy

- Assurance Policy (PS.Pol.009)

Required Forms

- Privacy and Security Readiness Self-Assessment
- Privacy Assertion Survey
- Information Security Assertion Survey

RM&R Information Security Policy (PS.Pol.101)

Summary

The purpose of this policy is to define the behavioral requirements for all agents and Electronic Service Providers of RM&R, as well as all participating health information custodians (HICs), their agents and Electronic Service Providers who have access to the RM&R Solution. These requirements are intended to help protect the confidentiality, integrity, and availability of personal health information (PHI) stored in or processed by the RM&R Solution.

- All organizations will have a contact designated.
- All organizations will have a formal written policy that is implemented and communicated to all agents.
- All organizations will have a formal written Information Security Breach policy that will include notification to RM&R of any RM&R related security breaches by the end of the next business day of being identified.
- All organizations will provide scheduled, timely and consistent training on Information Security Protection and safeguarding best practices to their agents.
- All devices/computers used to store PHI will be secured with a username and complex password, and comply with policy requirements.
- All computers, systems and networks will be protected and protect data at rest and in transit according to policy requirements.
- All agents at integrated sites must meet or exceed RM&R password requirements, and are accountable to ensuring accuracy and security of information as it passes to the RM&R System.

Policy

- RM&R Information Security Policy (PS.Pol.101)
- Privacy Breach Management Policy (PS.Pol.006)

Required Forms

The HIC is not required to use a RM&R form or document to support this policy.

5 Policies

Privacy Policy (PS.Pol.001)

Purpose

To define the policies and procedures that apply in receiving and responding to Requests for Access and Requests for Correction of records of personal health information (PHI) in respect of the RM&R System made by the Individual8 to whom the PHI relates.

Scope

This policy and its associated procedures apply to Requests for Access and Requests for Correction of records of PHI in respect of the RM&R System.

This policy and its associated procedures do not apply to Requests for Access and Requests for Correction of records of PHI that have not been contributed to the RM&R System.

Policies and Procedures

1. Guiding Policies

1.1. The RM&R Solution will allow PHI to be seamlessly and securely collected, used, and disclosed to deliver better, timelier and more coordinated health care. It is a network involving collection, use, and disclosure of PHI by HICs and, as such, shall be compliant with the Personal Health Information Protection Act, 2004, Ontario Regulation 329/04, and orders and decisions of the Information and Privacy Commissioner of Ontario.

1.2. HICs and RM&R recognize that a core principle in health care is respect for privacy, and will strive to provide Individuals with an experience that is easy-to-use and consistent across the RM&R Program.

1.3. HICs and RM&R understand that an effective privacy program must proactively address privacy issues by building privacy throughout the program lifecycle and into the broader program operations. RM&R program will follow the Privacy by Design[9] principles within the program.

1.4. HICs and RM&R acknowledge that trust is a cornerstone of any multi-stakeholder initiative, and that trust can only be achieved through transparent privacy practices and ensuring that all parties are accountable for how they support privacy.

1.5. HICs and RM&R shall have in place and maintain policies, procedures and practices in respect of privacy and security that are necessary to enable them to comply with their obligations under PHIPA, and shall provide the training required for their agents and Electronic Service Providers to be familiar with those policies, procedures and practices.

1.6. HICs and RM&R shall take steps that are reasonable in the circumstances to ensure their agents and Electronic Service Providers comply with PHIPA, this policy and its procedures, and its associated sub-policies and procedures.

2. Roles and Responsibilities of HICs

[8] Note that "Individual" also includes the Individual's substitute decision-maker where applicable.

[9] See www.privacybydesign.ca for a discussion of the Privacy by Design principles.

2.1. A HIC has custody and control of PHI that it has created and contributed to the RM&R Solution and PHI that is has collected from the RM&R Solution.

2.2. A HIC shall commit to having in place and maintain policies, procedures and practices in respect of privacy and security that are necessary to enable them to comply with its obligations under PHIPA and this Policy and its associated sub-policies and procedures, including:

- Access and Correction Policy, as amended from time to time;
- Consent Management Policy, as amended from time to time;
- Inquiries and Complaints Policy, as amended from time to time;
- Logging and Auditing Policy, as amended from time to time;
- Privacy and Security Training Policy, as amended from time to time;
- Privacy Breach Management Policy, as amended from time to time; and
- Retention Policy, as amended from time to time.

3. Roles and Responsibilities of RM&R

3.1. RM&R shall have in place and maintain policies, procedures and practices in respect of privacy and security that are necessary to enable it to comply with their obligations under PHIPA and this policy and its associated sub-policies and procedures.

3.2. RM&R has the following roles under PHIPA:

3.2.1. the program office for the RM&R Solution with adequate capacity to provide information technology products and services required for the RM&R Solution from Electronic Service Providers and to conduct privacy impact and related assessments of the RM&R Solution;

3.2.2. an Agent of HICs in regard to RM&R Services that a HIC has authorized RM&R to engage in under the Participation Agreement, the Policies or by written direction and that require RM&R to,

- collect, use or disclose PHI for the purposes for which a HIC is permitted to collect, use or disclose PHI under PHIPA, and/or
- interact directly with Individuals to whom PHI relates.

3.2.3. an Electronic Service Provider that is not a health information network provider (HINP) in connection with the Registry Products and any additional RM&R Services that may be agreed to between the RM&R Executive Committee and RM&R after the Effective Date that are the services of an Electronic Services Provider that is not a HINP; and

3.2.4. With the exception of the Client and Provider Registries and related services, for such interim period as the Registries and related services are being made available by RM&R, RM&R's responsibility as a HINP is to procure (including identifying specifications for technology products and services and enforcing the obligations of Electronic Service Providers) rather than to provide information technology services to enable HICs to use electronic means to disclose PHI to one another.

4. Governance

4.1. The RM&R Program shall have a governance structure that attributes accountability for privacy to the appropriate individuals and organizations.

4.2. The following bodies comprise the privacy governance and operations structure for the RM&R program:

- RM&R Executive Committee
- Privacy and Security Working Group

4.3. The accountabilities, roles and responsibilities for each of these committees shall be defined in Terms of

Reference to be approved by the RM&R Executive Committee.

Accountabilities

4.4. RM&R Executive Committee shall have its privacy and security accountabilities, roles, and responsibilities defined in a Terms of Reference (*refer to the appendix for a summary of the Terms of Reference*).

4.5. Privacy and Security Working Group shall have its accountabilities, roles, and responsibilities defined in a Terms of Reference that are approved by the RM&R Executive Committee (*refer to the appendix for a summary of the Terms of Reference*).

5. Guiding Policies

Consent

5.1. HICs and RM&R shall have in place and maintain policies, procedures, and practices that are necessary to enable them to comply with their obligations under PHIPA and the *Consent Management Policy* and its associated procedures, as amended from time to time, and that enables an Individual to exercise his or her right under PHIPA to give, withhold, and withdraw consent for the collection, use, and disclosure of his or her PHI for the purpose of providing or assisting in the provision of health care to the Individual.

5.2. PHIPA permits a HIC to assume an Individual's implied consent to collect, use or disclose the Individual's PHI for the purpose of providing or assisting in the provision of health care to the Individual, unless the Individual to whom the PHI relates has expressly withheld or withdrawn such consent.

5.3. A HIC that collects PHI from the RM&R System for the purpose of providing or assisting in the provision of health care to the Individual is permitted to use or disclose the PHI for any purpose for which it is permitted to use or disclose PHI with or without consent under PHIPA, except research.

5.4. A HIC that collects PHI from the RM&R System for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons, shall not use or disclose that PHI except for the purpose for which the PHI was collected.

Refer to the *Consent Management Policy* and its associated procedures, as amended from time to time.

Collection, Use, and Disclosure

5.5. A HIC collects PHI on the initial instance on which it views, handles, or otherwise deals with the PHI that another HIC contributed to the RM&R Solution.

5.6. A HIC that views, handles or otherwise deals with PHI for a second or subsequent time is considered to be using that information, as long as no new or additional information is viewed, handled or otherwise dealt with.

5.7. A HIC that views, handles, or otherwise deals with PHI that it contributed to the RM&R Solution is considered to be using that information, as long as no new or additional information is viewed, handled or otherwise dealt with.

5.8. A HIC is permitted to collect PHI from the RM&R Solution for the purpose of providing or assisting in providing health care to the Individual to whom the PHI relates.

5.9. A HIC may use and disclose PHI that it has collected from or contributed to the RM&R Solution for any purpose for which it is permitted to use or disclose PHI without consent under PHIPA except research.

5.10. A HIC shall only collect, use, or disclose the least amount of PHI required for the purpose of fulfilling the collection, use, or disclosure.

Refer to the *Consent Policy* and its associated procedures, as amended from time to time.

Accuracy

5.11. A HIC collecting PHI from the RM&R Solution shall take reasonable steps to ensure that PHI is accurate, complete, and up-to-date as is necessary for the purposes for which it is using the PHI.

5.12. A HIC that has created and contributed PHI to the RM&R Solution shall take reasonable steps to ensure that PHI is as accurate, complete, and up-to-date as is necessary for the purposes of providing or assisting in the provision of health care to the individual.

Refer to *Access and Correction Policy* and its associated procedures, as amended from time to time.

Secure Retention, Transfer, and Disposal

5.13. HICs and RM&R shall have in place and maintain policies, procedures, and practices in respect of secure retention, transfer, and disposal of PHI that are necessary to enable them to comply with their obligations under PHIPA and under the *Retention Policy, RM&R Information and Information Technology Policy (PS.Pol.101)* and associated procedures, as amended from time to time.

Refer to the *Retention Policy, RM&R Information and Information Technology Policy (PS.Pol.101)* and associated procedures, as amended from time to time.

Safeguards

5.14. RM&R and HICs shall comply with the *RM&R Information and Information Technology Policy (PS.Pol.101)*, as amended from time to time.

Refer to the *RM&R Information and Information Technology Policy (PS.Pol.101)*.

Inquiries and Complaints

5.15. HICs and RM&R shall have in place and maintain policies, procedures, and practices in respect of Inquiries and Complaints related to the RM&R program that are necessary to enable them to comply with their obligations under PHIPA and the *Inquiries and Complaints Policy* and its associated procedures, as amended from time to time.

Refer to the *Inquiries and Complaints Policy* and its associated procedures, as amended from time to time.

Access and Correction

5.16. HICs and RM&R shall have in place and maintain policies, procedures, and practices in respect of Requests for Access and Requests for Correction related to the RM&R program that are necessary to enable them to comply with their obligations under PHIPA and the *Access and Correction Policy* and its associated procedures, as amended from time to time.

Refer to the *Access and Correction Policy* and its associated procedures, as amended from time to time.

Transparency

5.17. The policies, procedures, and practices of the RM&R program shall be publically available to ensure that Individuals are well-informed about the RM&R program and how it protects the privacy of the Individual and the security of his or her PHI.

Refer to the *Consent Management Policy* and its associated procedures, as amended from time to time.

Training

5.18. HICs and RM&R shall have in place and maintain policies, procedures, and practices in respect of training related to the RM&R program that are necessary to enable them to comply with their obligations under PHIPA and the *Privacy and Security Training Policy* and its associated procedures, as amended from time to time.

Refer to the *Privacy and Security Training Policy* and its associated procedures, as amended from time to time.

Logging and Auditing

5.19. HICs and RM&R shall have in place and maintain policies, procedures, and practices in respect of logging and auditing that are necessary to enable them to comply with their obligations under PHIPA and the *Logging and Auditing Policy* and its associated procedures, as amended from time to time.

Refer to the *Logging and Auditing Policy* and its associated procedures, as amended from time to time.

Privacy Breach Management

5.20. PHIPA requires HICs to ensure that records of PHI in their custody or control are retained, transferred and disposed of in a secure manner.

5.21. HICs and RM&R shall have in place and maintain policies, procedures and practices in respect of privacy breach management that are necessary to enable them to comply with their obligations under *PHIPA*, RM&R agreements and the Privacy Breach Management Policy and associated procedures, as amended from time to time, and shall provide the training required for their agents and electronic service providers to be familiar with those policies, procedures and practices.

Refer to the *Privacy Breach Management Policy* and its associated procedures, as amended from time to time.

Assurance

5.22. HICs and RM&R shall have in place and maintain policies, procedures, and practices in respect of assurance that are necessary to enable them to comply with their obligations under PHIPA and the Assurance Policy and its associated procedures, as amended from time to time.

5.23. Refer to the *Assurance Policy* and its associated procedures, as amended from time to time.

References

1. Legislative

- PHIPA, ss. 10, 15 and 17 and Part V.1
- PHIPA, Reg. 329/04, s. 6

Document Management

Policy Number	PS.Pol.001
Version	1
Version History	V1 – Initial draft
Effective Date	TBD
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Appendix 1: Terms of Reference – Executive Committee (EC)

Mandate
The purpose of the Toronto Central LHIN Resource Matching & Referral (TC LHIN RM&R) Executive Committee is to provide strategic oversight and direction for the TC LHIN RM&R Program.

Accountability
The Executive Committee is accountable to the Toronto Central LHIN eHealth Program.

Meeting Frequency and Attendance

- Meetings will be held on a monthly basis, or as required.
- The use of delegates is permitted on an occasional basis. The delegate will represent an executive/senior management position.

Communications
Records of discussion/action items will be disseminated to members and internal project teams via email.

Operational Management
SIMS Program Office to support operational management (e.g. preparing meeting material, liaise with committee members, schedule review meetings, develop and track discussion/action items).

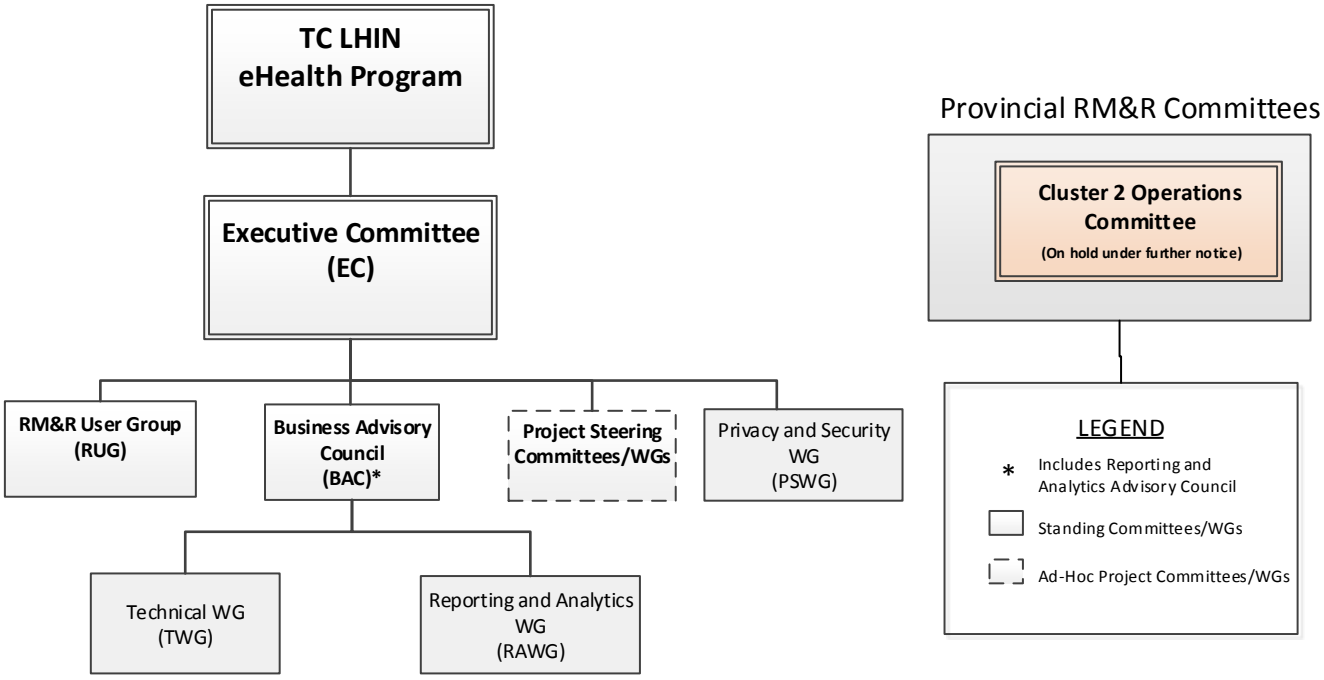
Responsibilities

- Provide strategic oversight and direction for the TC LHIN RM&R Program
- Ensure alignment with TC LHIN, Cluster 2 and Ministry of Health and Long Term Care eHealth principles and objectives
- Act as a discussion and decision-making forum for RM&R operations, expansion, and new funding activities
- Approve recommendations, resolve issues and risks, and make decisions on key strategic objectives and deliverables brought forward by RM&R Sub-Committees
- Monitor overall program performance and compliance with privacy laws

Membership
This document and committee membership will be reviewed, as requested by the Executive Committee.

Name	Title	Organization/Sector
Rachel Solomon	Senior Director, Toronto Central LHIN	Program Sponsor
Stacey Daub	CEO, Toronto Central CCAC	Business Lead
Shiran Isaacksz	Senior Director, Regional/Provincial Portfolio	Delivery Partner, SIMS
Stephanie Saull-McCaig	Director, Information Management	Delivery Partner, SIMS
Robin Gould-Soil	Corporate Privacy Officer	Delivery Partner, SIMS
Helen Cavanagh	Chair of TC LHIN RM&R Business Advisory Council	Toronto Central CCAC

RM&R Governance Structure



Appendix 2: Terms of Reference – Privacy and Security Working Group (PSWG)

Mandate
The purpose of the Toronto Central LHIN Resource Matching & Referral (TC LHIN RM&R) Privacy and Security Working Group (PSWG) is to provide privacy and security consultation and advice to the RM&R Program related to privacy and security processes and practices.

Responsibilities
Act as sector champions by providing privacy and security advice and consultation on TC LHIN's RM&R program as it relates to the following:

- Privacy and/or security artifacts such as policies, risk treatment plans, and training material
- Evaluating privacy and security risks when exceptions to policies are requested
- System or business model changes impacting privacy and/or security
- Issue resolution related to audit results, incident reports, and complaints
- Additional tactical or strategic assignments from the Executive Committee, as required

Accountability
The Privacy and Security Working Group is accountable to the TC LHIN RM&R Executive Committee (EC). All recommendations of the PSWG are subject to ratification by the EC.

When applicable, privacy issues may be shared with the Toronto Central Privacy Working Group (TCPWG) to elicit additional feedback and/or information sharing.

Meeting Frequency and Attendance

- Meetings will be held ad hoc, as required. Meetings may occur on a more regular basis, as determined by the RM&R program and PSWG during periods of high activity.
- The use of delegates is permitted on an occasional basis, at the discretion of the participating member.

UHN Operational Role
SIMS RM&R Operations team to support operational management (e.g. preparing meeting material, liaise with committee members, schedule review meetings, develop and track discussion/agenda items). SIMS Program Office is responsible to coordinate cross-committee communications and knowledge sharing activities.

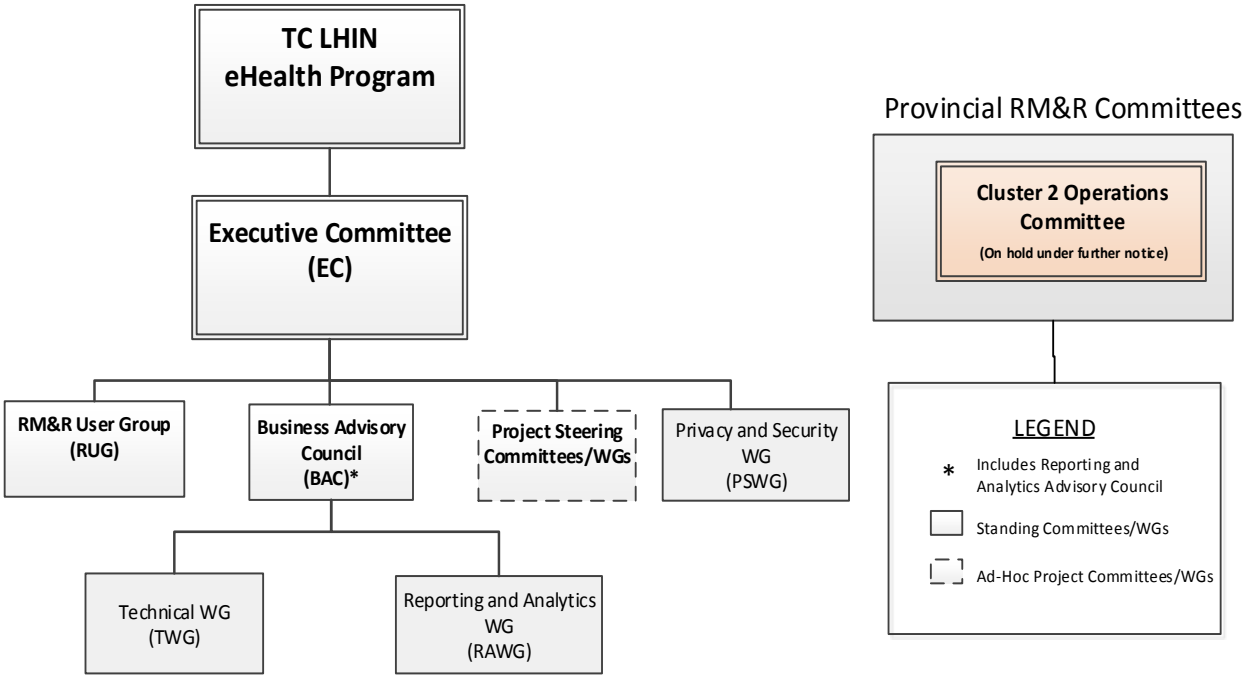
Communications
Records of discussion/agenda items will be disseminated to members via email. Meeting material will be shared within a timely manner and shared with other committees, as required.

Membership
This document and committee membership will be reviewed, as requested by the committee. PSWG membership will be nominated by the associated Business Advisory Council (BAC) sector lead. Voting membership is comprised of 1 representative from each of the 6 sectors with organizations participating in RM&R, as well as 1 person representing each of the Program Sponsor, and the Delivery Partner. Membership renewal including potential changes or expansion will be considered as part of the annual program planning or as otherwise determined by the RM&R Executive Committee.

Chair: Robin Gould-Soil, RM&R Program (HINP)

Name	Privacy/Security Representation	Title	Organization/Sector
Alvin Cheng	Privacy & Security	Manager, eHealth Program	TC LHIN
Jennifer Foster	Privacy	Director, Privacy Officer	TC CCAC
Kamini Milnes	Security	Director, IM/IT	TC CCAC
Robin Gould-Soil	Privacy	Director, Privacy and Information Access	RM&R Program (HINP)
Aaron Hendricks	Security	Manager, Information Security	RM&R Program (HINP)
Jeff Curtis	Privacy & Security	Chief Privacy Officer	Acute (Sunnybrook)
Terrie Tucker	Privacy & Security	Executive Director eHealth, Chief Privacy Officer	Rehab/CCC (Baycrest)
Narain Motwani	Privacy & Security	Manager of Client Services	CSS (St. Clair Services for Seniors)
TBD	Privacy & Security		LTC

RM&R Governance Structure



Access and Correction Policy (PS.Pol.002)

Purpose

To define the policies and procedures that apply in receiving and responding to Requests for Access and Requests for Correction of records of personal health information (PHI) in respect of the RM&R System made by the Individual10 to whom the PHI relates.

Scope

This policy and its associated procedures apply to Requests for Access and Requests for Correction of records of PHI in respect of the RM&R System.

This policy and its associated procedures do not apply to Requests for Access and Requests for Correction of records of PHI that have not been contributed to the RM&R System.

Definitions

For a fulsome list of definitions that apply to all RM&R Privacy and Security Policies and Procedures, see Definitions section of RM&R Privacy Policies.

Request for Access

A request made by an Individual to exercise the right under Part V of the *Personal Health Information Protection Act, 2004* (PHIPA) to access the Individual's records of PHI in the custody or control of a HIC.

Without limiting the generality of the foregoing, an Individual may make a request for access to the following records in respect of the RM&R Solution:

- Clinical records of the Individual;
- Records of all instances where all or part of the PHI of the Individual is viewed, handled or otherwise dealt with by HICs or their agents and Electronic Service Providers;
- Records of all instances where a consent directive is made, withdrawn or modified by the Individual; and
- Records of all instances where a consent directive made by the Individual is overridden and the purpose for which the consent directive is overridden.

Request for Correction

A request made by an Individual to exercise the right under Part V of PHIPA to request a correction of the Individual's records of PHI that the Individual believes are inaccurate or incomplete for the purposes for which the PHI has been collected or used or is being used.

Policies and Procedures

[10] Note that "Individual" also includes the Individual's substitute decision-maker where applicable.

1. Guiding Policies

1.1. HICs and RM&R shall have in place and maintain policies, procedures and practices in respect of privacy and security that are necessary to enable them to comply with their obligations under PHIPA, and shall provide the training required for their agents and electronic service providers to be familiar with those policies, procedures and practices.

1.2. RM&R shall have a program in place to enable RM&R and HICs to satisfy their obligations in receiving and responding to Requests for Access and Requests for Correction of records of PHI in the RM&R System in accordance with PHIPA and this policy and its associated procedures.

1.3. This policy and its associated procedures will support an Individual in exercising the Individual's legislative right to make a Request for Access and a Request for Correction of his or her records of PHI in respect of the RM&R System and will assist HICs in meeting their obligations under PHIPA in receiving and responding to such Requests for Access and Requests for Correction.

1.4. Without limiting the generality of paragraph **Error! Reference source not found.**, Individuals will ave the right to make a Request for Access to the following records of PHI in respect of the RM&R System:

- Clinical records of the Individual;
- Records of all instances where all or part of the PHI of the Individual is viewed, handled or otherwise dealt with by HICs or their agents and Electronic Service Providers;
- Records of all instances where a consent directive is made, withdrawn or modified by the Individual; and
- Records of all instances where a consent directive made by the Individual is overridden and the purpose for which the consent directive is overridden.

1.5. The *Freedom of Information and Protection of Privacy Act* (FIPPA) requires hospitals to provide annually to the Information and Privacy Commissioner of Ontario, the reports identified in section 34 of FIPPA. Each hospital responsible for responding to a Request for Access or a Request for Correction of records of PHI in the RM&R System shall include the number of requests and refusals in its report to the Information and Privacy Commissioner of Ontario, even if RM&R provided the records of PHI to the Individual making the request on behalf of the hospital.

2. Procedures for Responding to a Request for Access

Request Directly from Individual for Records Created and Contributed Solely by the HIC

2.1. Where a HIC receives a Request for Access directly from an Individual related to records of PHI that were created and contributed to the RM&R System solely by that HIC, the HIC shall follow its own internal policies, procedures, and practices to address the Request for Access.

Request Directly from Individual for Records Previously Collected by the HIC

2.2. Where a HIC receives a Request for Access directly from an Individual related to records of PHI that were previously collected by that HIC for the purpose of providing or supporting the provision of health care, the HIC shall follow its own internal policies, procedures, and practices to address the Request for Access.

Request Relates to Records Created and Contributed by Another HIC

2.3. Where a HIC receives a Request for Access directly from an Individual related to records of PHI that were created and contributed to the RM&R System by one or more other HICs and that the HIC that received the Request for Access has not collected, the HIC that received the Request for Access shall as soon as possible:

- Notify the Individual that the Request for Access involves PHI not within the custody or control of the HIC that received the request; and
- Provide the Individual with information on how to contact the HIC that created or contributed the PHI to make the request.

Request Received by RM&R and Relates to Records Created and Contributed by Solely One HIC

2.4. Where RM&R receives a Request for Access directly from an Individual related to the record of PHI in the RM&R System created and contributed by solely one HIC, RM&R shall:

- Notify the Individual that the Request for Access involves PHI not within the custody or control RM&R; and
- Provide the Individual with information on how to contact the HIC that created or contributed the PHI to make the request.

Request Received by RM&R and Relates to Records Created and Contributed by More than One HIC

2.5. Where RM&R receives a Request for Access directly from an Individual related to the record of PHI in the RM&R System created and contributed by more than one HIC, RM&R shall:

- Verify and validate the identity of the person making the Request for Access as the Individual to whom the records of PHI in respect of the RM&R System and that are subject to the Request for Access relate, or as the Individual's SDM;
- Notify the Individual that the Request for Access will be sent to each HIC that created and contributed the records of PHI to the RM&R System;
- Obtain from the Individual sufficient information to enable the HIC that created and contributed the records of PHI to the RM&R System to identify the Individual in the RM&R System, to locate the Individual's records in the RM&R System and to respond to the Request for Access; and
- Obtain from the Individual, an address for the delivery of the response to the Request for Access or other contact information as is appropriate in the circumstances.

2.6. Upon a request from RM&R, HICs shall assist RM&R in verifying and validating the identity of the person making the request as the Individual to whom the records of PHI in respect of the RM&R System and that are subject to the Request for Access relate, or as the Individual's SDM.

2.7. As soon as possible, but in any event no later than 7 days after receiving a Request for Access, RM&R shall identify each of the HICs that created and contributed the records of PHI to the RM&R System that are the subject of the Request for Access, and forward the Request for Access, in a secure manner, to the HICs that have been identified.

2.8. In forwarding the Request for Access, RM&R shall:

- Notify each HIC that the records of PHI subject to the Request for Access were created and

contributed by more than one HIC;

- Provide each HIC with information relating to the identity of the Individual to whom the records of PHI in respect of the RM&R System and that are subject to the Request for Access relate and sufficient information to enable each HIC that created and contributed the records of PHI to the RM&R System to identify the Individual in the RM&R System, to locate the Individual's records in the RM&R System and to respond to the Request for Access;
- Advise each HIC that the HIC must, as soon as possible, but in any event no later than 21 days after receiving the Request for Access from RM&R, take the following actions:
    - Notify RM&R whether the HIC will grant the Request for Access in whole or in part and provide RM&R with explicit instructions to respond to the Request for Access;
    - Where the HIC will grant the Request for Access in whole or in part, provide RM&R with an estimate of the fee, if any, for providing access to the records of PHI;
    - Where the HIC will refuse the Request for Access in whole or in part, provide RM&R with a written notice addressed to the Individual that has been prepared in accordance with Part V of PHIPA; and
    - Where the HIC is extending the time for responding to the Request for Access for a further period of time not exceeding 30 days, provide RM&R with a written notice addressed to the Individual that has been prepared in accordance with Part V of PHIPA.

2.9. As soon as possible, but in any event no later than 21 days after receiving the Request for Access from RM&R, the HIC shall take the following actions:

- Notify RM&R whether the HIC will grant the Request for Access in whole or in part and provide RM&R with explicit instructions to respond to the Request for Access;
- Where the HIC will grant the Request for Access in whole or in part, provide RM&R with an estimate of the fee, if any, for providing access to the records of PHI;
- Where the HIC will refuse the Request for Access in whole or in part, provide RM&R with a written notice addressed to the Individual that has been prepared in accordance with Part V of PHIPA; and
- Where the HIC is extending the time for responding to the Request for Access for a further period of time not exceeding 30 days, provide RM&R with a written notice addressed to the Individual that has been prepared in accordance with Part V of PHIPA.

2.10. Where the HIC does not respond to RM&R in accordance with the timelines in paragraph 2.9, RM&R shall provide written notice to the Individual that the HIC has failed to respond to the Request for Access and that the Individual may make a complaint to the HIC that failed to respond to the Request for Access and/or to the Information and Privacy Commissioner of Ontario.

2.11. Within 30 days from when the Individual made the Request for Access, RM&R shall, in accordance with Part V of PHIPA:

- Provide the Individual with an estimate of the fee, if any, to provide access to the records of PHI for which the Request for Access is granted in whole or in part;
- Collect the fee, if any, on behalf of the HICs to provide access to the records of PHI for which the Request for Access is granted in whole or in part;
- Provide the Individual with copies of the records of PHI for which the Request for Access is granted in whole or in part;
- Provide the Individual with any written notices refusing the Request for Access in whole or in part;

- Provide the Individual with any written notices extending the time for responding to a Request for Access; and
- Provide the Individual with any written notices required under paragraph 2.10.

2.12. Where written notice extending the time for responding to a Request for Access has been provided to the Individual, the HIC requesting the extension shall follow its own internal policies, procedures, and practices to address the Request for Access.

Request Relates to Logs

2.13. Where a HIC receives a Request for Access directly from an Individual related to the following records, the HIC shall follow its own internal policies, procedures, and practices to address the Request for Access:

- Records of all instances where all or part of the PHI of the Individual is viewed, handled or otherwise dealt with by HICs;
- Records of all instances where a consent directive is made, withdrawn or modified by the Individual; and
- Records of all instances where a consent directive made by the Individual is overridden and the purpose for which the consent directive is overridden.

2.14. Where the HIC that receives a Request for Access related to the records referred to in paragraph 2.13 is unable to generate and provide copies of the records in response to the Request for Access, the HIC that received the Request for Access shall as soon as possible:

- Notify the Individual that the HIC is unable to process the request; and
- Provide the Individual with information on how to contact RM&R to make the request.

2.15. Where RM&R receives a Request for Access directly from an Individual related to the records described in 2.13, RM&R shall respond directly to the Individual in respect of the Request for Access in accordance with Part V of PHIPA and its internal policies, procedures and practices.

2.16. Upon receiving a Request for Access related to the logs, RM&R shall:

- Verify and validate the identity of the person making the Request for Access as the Individual to whom the records of PHI in respect of the RM&R System and that are subject to the Request for Access relate, or as the Individual's SDM;
- Notify the Individual that the Request for Access will be sent to the HIC that created and contributed the records of PHI to the RM&R System;
- Obtain from the Individual sufficient information to enable the HIC that created and contributed the records of PHI to the RM&R System to identify the Individual in the RM&R System, to locate the Individual's records in the RM&R System and to respond to the Request for Access; and
- Obtain from the Individual, an address for the delivery of the response to the Request for Access or other contact information as is appropriate in the circumstances; and
- Respond directly to the Individual in respect of the Request for Access in accordance with Part V of PHIPA and its internal policies, procedures and practices.

2.17. Upon request from RM&R, HICs shall assist RM&R in verifying and validating the identity of the person making the request as the Individual to whom the records of PHI in respect of the RM&R

System and that are subject to the Request for Access relate, or as the Individual's SDM.

3. Procedures for Charging Fees for Access

3.1. HICs may charge a fee for providing access to records of PHI in respect of the RM&R System provided that:

- The HIC first gives an estimate of the fee;
- The fee does not exceed the amount of reasonable cost recovery; and
- Is consistent with applicable orders of the Information and Privacy Commissioner of Ontario.

3.2. HICs may exercise their discretion in determining to waive payment of all or any part of the fee in accordance with Part V of PHIPA and their own internal policies, procedures and practices.

3.3. Where the Request for Access relates to records of PHI that were created and contributed to the RM&R System by more than one HIC, RM&R is responsible for providing the individual making the request with an estimate of the fee, if any, as provided to RM&R by the HICs, that will be charged by the HICs that created and contributed the records and for collecting the fee.

3.4. Where the Request for Access relates to records of PHI that were created and contributed to the RM&R System solely by one HIC, that HIC is responsible for providing an estimate of the fee, if any, that will be charged by that HIC and for collecting the fee.

3.5. RM&R will not charge a fee for its services associated with co-ordinating responses to Requests for Access or responding to Requests for Access related to the records referred to in paragraph 2.11.

4. Procedures for Responding to a Request for Correction

Request Directly from Individual for Records Created and Contributed Solely by the HIC

4.1. Where a HIC receives a Request for Correction directly from an Individual related to records of PHI that were created and contributed to the RM&R System solely by that HIC, the HIC shall follow its own internal policies, procedures, and practices to address the Request for Correction.

4.2. Where the HIC will grant the Request for Correction or is required to append a Statement of Disagreement and the request relates to a record of PHI in the RM&R System that cannot be made directly by the HIC, the HIC shall instruct RM&R to make the correction or append the statement in accordance with Part V of PHIPA and to make the correction or append the statement as soon as possible after receiving the Request for Correction.

4.3. As soon as possible, but in any event no later than 7 days after receiving the instruction from the HIC, RM&R shall make the requested correction or append the Statement of Disagreement in accordance with Part V of PHIPA.

4.4. Upon making the requested correction or appending the Statement of Disagreement, RM&R shall immediately notify the HIC that RM&R has made the requested correction and how the requested correction was made to enable the HIC to fulfill its obligations under section 55(10) of PHIPA.

4.5. Upon granting a Request for Correction the HIC shall, in accordance with section 55(10) of PHIPA:

- Give notice to the Individual in respect of how the requested correction was made; and
- At the request of the Individual, given written notice of the requested correction, to the extent reasonably possible, to the persons to whom the HIC disclosed the PHI, except if the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or other

benefits to the Individual.

4.6. RM&R shall ensure that the RM&R System maintains a history of all corrections of records of PHI or Statements of Disagreement in the RM&R System, regardless of whether the correction is made by the HIC or RM&R.

4.7. HICs and RM&R shall ensure that all corrections of records of PHI in the RM&R System are made in accordance with section 55(10) of PHIPA.

Request Relates to Records Created and Contributed Solely by Another HIC or More Than One HIC

4.8. Where a HIC receives a Request for Correction directly from an Individual related to records of PHI that were created and contributed to the RM&R System solely by another HIC or by more than one HIC, the HIC that received the Request for Correction shall as soon as possible:

- Notify the Individual that the Request for Correction involves PHI not created and contributed by the HIC that received the request;
- **If the request is for PHI that was created and contributed to the RM&R System solely by one HIC:** provide the Individual with information on how to contact that HIC to make the request; and
- **If the request is for PHI that was created and contributed to the RM&R System by more than one HIC:** Provide the Individual with information on how to contact RM&R to make the request.

4.9. Where RM&R receives a Request for Correction directly from an Individual related to the record of PHI in the RM&R System created and contributed by more than one HIC, RM&R shall:

- Verify and validate the identity of the person making the Request for Correction as the Individual to whom the records of PHI in the RM&R System and that are subject to the Request for Correction relate, or as the Individual's SDM;
- Notify the Individual that the Request for Correction will be sent to the HIC or HICs that created and contributed the records of PHI to the RM&R System;
- Obtain from the Individual sufficient information to enable the HIC or HICs that created and contributed the records of PHI to the RM&R System to identify the Individual in the RM&R System, to locate the Individual's records in the RM&R System and to respond to the Request for Correction; and
- Obtain from the Individual an address for the delivery of the response to the Request for Correction or other contact information as is appropriate in the circumstances.

4.10. Upon request from RM&R, HICs shall assist RM&R in verifying and validating the identity of the person making the request as the Individual to whom the records of PHI in respect of the RM&R System and that are subject to the Request for Access relate, or as the Individual's SDM.

4.11. As soon as possible, but in any event no later than 7 days after receiving a Request for Correction, RM&R shall identify the HIC or HICs that created and contributed the records of PHI to the RM&R System that are the subject of the Request for Correction, and forward the Request for Correction, in a secure manner, to the HICs that have been identified.

4.12. In forwarding the Request for Correction, RM&R shall:

- Provide each HIC with the information received under paragraph 4.9; and
- Notify each HIC that the HIC is required to respond directly to the Individual in respect of the

Request for Correction in accordance with Part V of PHIPA and its internal policies, procedures and practices.

4.13. Upon receiving a Request for Correction from RM&R related to records of PHI that were created and contributed to the RM&R System by the HIC, the HIC shall follow its own internal policies, procedures, and practices to address the Request for Correction, within a timeframe that supports a response to the Individual within 30 days of RM&R receiving the request.

4.14. Where the HIC will grant the Request for Correction or is required to append a Statement of Disagreement and the request relates to a record of PHI in the RM&R System that cannot be made directly by the HIC, the HIC shall instruct RM&R to make the correction or append the statement in accordance with Part V of PHIPA and to make the correction or append the statement as soon as possible after receiving the Request for Correction.

4.15. As soon as possible, but in any event no later than 7 days after receiving the instruction from the HIC, RM&R shall make the requested correction or append the Statement of Disagreement.

4.16. Upon making the requested correction or appending the Statement of Disagreement, RM&R shall immediately notify the HIC that RM&R has made the requested correction or appended the Statement of Disagreement and how the requested correction was made to enable the HIC to fulfill its obligations under section 55(10) of PHIPA.

4.17. Upon granting the Request for Correction the HIC shall, in accordance with section 55(10) of PHIPA:

- Give notice to the Individual in respect of how the requested correction was made; and
- At the request of the Individual, give written notice of the requested correction, to the extent reasonably possible, to the persons to whom the HIC disclosed the PHI, except if the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or other benefits to the Individual.

4.18. The HIC shall log that it has responded to the Request for Correction.

4.19. RM&R shall ensure that the RM&R System maintains and displays a history of all corrections of records of PHI in the RM&R System regardless of whether the correction is made by the HIC or RM&R.

5. Complaints Related to Requests for Access, Requests for Correction and Fees

5.1. All complaints related to Requests for Access, Requests for Correction and fees for responding to Requests for Access shall be dealt with in accordance with the *Inquiries and Complaints Policy* and its associated procedures, as amended from time to time.

References

1. Legislation and Regulation

- PHIPA, Part V

2. IPC Decisions and Findings

- Order HO-009, October 13, 2010

Document Management

Policy Number	PS.Pol.002
Version	1
Version History	V1 – Initial draft
Effective Date	TBD

Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Consent Management Policy (PS.Pol.003)

Purpose

To define the policies and procedures that apply in:

- Obtaining the consent of the individual or their substitute decision maker (SDM) in respect of the collection, use or disclosure of the individual's personal health information (PHI) in the RM&R system, including Strata IQ, for the purpose of providing or assisting in the provision of health care to the individual.
- Implementing Consent Directives of the individual to give, withhold or withdraw consent to the collection, use or disclosure of the individual's PHI in the RM&R system, including Strata IQ, for the purpose of providing or assisting in the provision of health care to the individual.
- Overriding Consent Directives.

Scope

This policy and its associated procedures apply to obtaining consent, implementing Consent Directives and overriding Consent Directives in respect of the Individual's PHI in the RM&R system, including Strata IQ, for the purpose of providing or assisting in the provision of health care to the Individual.

This policy and its associated procedures do not apply to obtaining consent, implementing Consent Directives or overriding Consent Directives in respect of any other PHI or for any other purpose.

Definitions

For a fulsome list of definitions that apply to all RM&R Privacy and Security Policies and Procedures, see Definitions section of RM&R Privacy Policies.

Consent Directive

A directive made by the Individual to give, withhold or withdraw, in whole or in part, his or her consent to the collection, use or disclosure of the Individual's PHI in the RM&R System for the purpose of providing or assisting in the provision of health care to the Individual[11], and includes a directive to modify or withdraw a directive that has already been made.

The following demographic information cannot be made subject to a Consent Directive because it is required to uniquely identify the Individual in the RM&R System for the purpose of managing privacy procedures related to the Individual and to ensure accuracy of system data:

- First Name
- Last Name
- Gender
- Data of Birth

[11] Note that a consent directive only applies to collection, use, and disclosure of PHI for the purpose of healthcare or supporting the provision of healthcare. Consent directives cannot be applied for other uses or disclosures of PHI for which consent is not required.

- Primary Address (Street, post code, city, province, country)
- Health Card Number (if available)
- HIC ID and MRN assigned by the HIC (if available)
- Information on the RM&R dashboard when the individual is receiving care or treatment at the organization

Global Consent Directive

A Consent Directive made by the Individual to withhold or withdraw consent to the collection, use and disclosure of Individual's entire record of PHI in the RM&R System.

Policies and Procedures

1. Guiding Policies

1.1. RM&R shall have a program in place to enable RM&R and HICs to satisfy their obligations to implement requests from individuals to make, modify or withdraw Consent Directives in RM&R in accordance with PHIPA and this policy and its associated procedures.

1.2. RM&R shall have a program in place to enable RM&R and HICs to satisfy their obligations in respect of the overriding of Consent Directives in the RM&R system, in accordance with PHIPA and this policy and its associated procedures.

Collection, Use or Disclosure of PHI in RM&R

1.3. Subject to paragraph 1.9, a HIC is permitted to collect PHI from the RM&R system for the purposes of providing or assisting in the provision of health care to the individual.

Giving, Withholding or Withdrawing Consent Through Consent Directives

1.4. PHIPA gives the individual the right to give, withhold or withdraw consent to the collection, use or disclosure of the individual's PHI for the purpose of providing or assisting in the provision of health care to the individual

1.5. The individual may exercise the right to give, withhold or withdraw consent to the collection, use or disclosure of the individual's PHI in the RM&R system for the purpose of providing or assisting in the provision of health care to the individual by making, modifying or withdrawing a Consent Directive.

1.6. The individual may make, modify or withdraw Global Consent Directives in respect of the individual's PHI in the RM&R system.

1.7. HICs shall implement the request from an individual to make, modify, or withdraw a Consent Directive and send the notice required under paragraph 5 as soon as possible, but in any event, no more than 7 days after verifying and validating the identity of the person requesting to make, modify, or withdraw a Consent Directive.

1.8. This policy and its associated procedures will support the individual in exercising the right to give, withhold or withdraw consent to the collection, use or disclosure of the individual's PHI in the RM&R system for the purpose of providing or assisting in the provision of health care to the individual.

Overriding Consent Directives

1.9. A HIC shall only override a Consent Directive and shall only collect PHI in the RM&R system that is the subject of a Consent Directive where the HIC seeking to collect the PHI:

- Obtains the express consent of the individual to whom the PHI relates;
- Believes on reasonable grounds 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 PHI relates and it is

not reasonably possible to obtain the consent of the individual in a timely manner; or

- Believes on reasonable grounds 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 PHI relates or to a group of persons.

1.10. A HIC that overrides a Consent Directive and that collects PHI in the RM&R system that is the subject of the Consent Directive, shall only use or disclose that PHI for the purpose for which the PHI was collected.

1.11. All instances where all or part of the PHI in the RM&R system is collected as a result of an override of a Consent Directive shall be monitored and notice of the override shall be provided to the Privacy Contact for the HIC that collected the PHI in the RM&R system that is the subject of the Consent Directive as well as notice to the Individual to whom the PHI relates shall be provided.

2. Procedures for Obtaining Consent

2.1. HICs shall obtain consent from the individual in respect of the collection, use and disclosure of the individual's PHI in the RM&R system in accordance with PHIPA and their internal policies, procedures and practices.

3. Procedures for Receiving and Implementing Consent Directives

Receipt of Consent Directives

3.1. Where a HIC receives a request to make, modify or withdraw a Consent Directive in the RM&R system, the HIC shall receive the request in accordance with PHIPA, its internal policies, procedures and practices and the requirements under paragraph 3.3.

3.2. Where RM&R receives a request to make, modify or withdraw a Consent Directive in the RM&R system, RM&R shall direct the individual making the request to contact the HIC with whom the individual has had the most contact in respect to receiving health care.

3.3. Upon receiving a request to make, modify or withdraw a Consent Directive in the RM&R system from the individual, the HIC shall:

- Log receipt of the request;
- Verify and validate the identity of the person making the request as the individual to whom the PHI in the RM&R system that is the subject of the request relates or as the individual's SDM;
- Obtain from the individual, sufficient information to identify the individual in the RM&R system, to locate the individual's PHI in the RM&R system and to implement the request;
- If the request does not contain sufficient detail, offer assistance to the individual making the request;
- Inform the individual about the impact of making, modifying, or withdrawing a Consent Directive;
- Inform the individual about the circumstances in which a Consent Directive in the RM&R system may be overridden and in which PHI that is the subject of a Consent Directive may be collected;
- Inform the individual that he or she will receive a notice in all instances where all or part of the individual's PHI in the RM&R system is collected as a result of an override of a Consent Directive;
- Inform the individual that he or she may make, modify or withdraw a Consent Directive at any time; and
- Obtain from the individual an address for the delivery of the notice required under paragraph 5.

Implementation of Global Consent Directives

3.4. Where a HIC receives a request from the individual to make, modify or withdraw a Global Consent

Directive in the RM&R system, the HIC shall implement the request.

3.5. As soon as possible, but in any event no later than 2 business days after verifying and validating the identity of the person requesting to make, modify or withdraw a Consent Directive in paragraph 3.4, the HIC that received the request shall:

- Implement the request; and
- Take reasonable steps to confirm that the request has been implemented.

3.6. Immediately after implementing and taking reasonable steps to confirm that the request to make, modify or withdraw a Consent Directive in paragraph 3.4 has been implemented, the HIC shall deliver to the individual the notice required under paragraph 5.1.

4. Procedures for Confirming Consent Directives Implemented

4.1. HICs shall take reasonable steps to confirm that the requests to make, modify or withdraw Consent Directives that they have implemented in the RM&R system are properly implemented.

5. Procedures for Notifying Individuals of Consent Directive Implementation

5.1. Immediately after the HIC that received a request from the individual to make a Consent Directive has implemented and has taken reasonable steps to confirm that the request has been implemented in the RM&R system, the HIC shall securely provide to the individual a notice:

- Describing the request received from the individual;
- Identifying and describing the Consent Directive that was made, modified or withdrawn in the RM&R system;
- Confirming that the Consent Directive was made, modified or withdrawn, as the case may be, and the date that it was made, modified or withdrawn;
- Describing the impact of the Consent Directive that was made, modified or withdrawn;
- Describing the circumstances in which the Consent Directive may be overridden and in which PHI that is the subject of the Consent Directive may be collected;
- Indicating that the individual will receive a notice in all instances where all or part of the individual's PHI in the RM&R system is collected as a result of an override of the Consent Directive;
- Providing contact information for the person to whom individuals may direct inquiries or complaints related to the Consent Directive; and
- Indicating that the individual may make, modify or withdraw a Consent Directive at any time.

5.2. The HIC shall keep a record of the notification required under paragraph 5, and shall securely forward a copy of the record to RM&R (using the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx). The record shall either be a copy of the notification provided to the individual where the notice is written or a log of the notifications provided.

6. Procedures for Overriding a Consent Directive

6.1. RM&R shall ensure that the RM&R system is capable of logging all instances where all or part of the PHI in the RM&R system is disclosed to and collected by a HIC or an agent of a HIC as a result of an override of a Consent Directive.

6.2. RM&R shall ensure that the log of all instances where all or part of the PHI in the RM&R system is disclosed to and collected by a HIC or an agent of a HIC as a result of an override of a Consent Directive contains the information required under PHIPA and the Logging and Auditing policy and its associated procedures, as amended from time to time.

6.3. RM&R shall continuously audit and monitor all instances where all or part of the PHI in the RM&R system

is disclosed to and collected by a HIC or an agent of a HIC as a result of an override of a Consent Directive in accordance with the Logging and Auditing policy and its associated procedures.

6.4. RM&R shall provide notice to the HIC that overrode a Consent Directive in the RM&R system and that collected PHI that is the subject of the Consent Directive.

6.5. Upon request, RM&R will provide notice to the HIC that overrode a Consent Directive in the RM&R system and that collected PHI that is the subject of the Consent Directive the identity of the HIC(s) that disclosed the PHI that is the subject of the Consent Directive.

6.6. Upon receiving the notice under paragraph 6.4, the HIC that overrode or whose agent overrode the Consent Directive in the RM&R system and that collected PHI that is the subject of the Consent Directive shall, at the first reasonable opportunity, notify the individual to whom the PHI relates. At a minimum, the notice shall indicate that a Consent Directive was overridden and that the PHI that is the subject of the Consent Directive was collected and shall identify:

- The type of PHI subject to the Consent Directive that was collected;
- The HIC that collected the PHI that is the subject of the Consent Directive;
- The agent of the HIC that collected the PHI that is the subject of the Consent Directive;
- The date and time the PHI subject to the Consent Directive was collected;
- The purpose for which the Consent Directive was overridden and the PHI that is the subject of the Consent Directive was collected;
- The person to whom individuals may direct inquiries or complaints related to the override and contact information for this person; and
    - How to make a complaint to the Information and Privacy Commissioner of Ontario.

6.7. A HIC that overrode or whose agent overrode a Consent Directive in the RM&R system and that collected PHI that is the subject of the Consent Directive shall keep a record of the notice provided to the individual. The record shall either be a copy of the notice provided to the individual or a log of the notices sent.

6.8. A HIC that overrode or whose agent overrode a Consent Directive in the RM&R system and that collected PHI that is the subject of the Consent Directive for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons, shall not provide identifying information about the person or group of persons at significant risk of serious bodily harm in the notice required under paragraph 6.5.

References

1. Legislative

- *PHIPA*, *2004*, Part III and Part V.1

Document Management

Version	1
Version History	V1 – Initial draft
Effective Date	TBD
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Inquiries and Complaints Policy (PS.Pol.004)

Purpose	To define the policies and procedures that apply in receiving, documenting, tracking, addressing and responding to Inquiries and Complaints in respect of the RM&R system, including Strata IQ.
Scope	This policy and its associated procedures apply to Inquiries and Complaints in respect of the RM&R system. This policy and its associated procedures do not apply to Inquiries or Complaints in respect of any system other than the RM&R system or in respect of any information other than PHI in the RM&R system.
Definitions	For a fulsome list of definitions that apply to all RM&R Privacy and Security Policies and Procedures, see Definitions section of RM&R Privacy Policies. Complaint A concern raised by any person12 in respect of the RM&R system including, but not limited to, concerns raised in respect of compliance with the Personal Health Information Protection Act, 2004 (PHIPA) and the policies, procedures and practices implemented in respect of the RM&R System; Inquiry A question raised by any person in respect of the RM&R System including, but not limited to, questions raised in respect of: ○ When, how and the purposes for which PHI in the RM&R System is collected, used and disclosed; ○ The administrative, technical and physical safeguards and practices maintained with respect to PHI in the RM&R System; ○ The policies, procedures and practices implemented in respect of the RM&R System; and ○ Compliance with PHIPA.

Policies and Procedures

1. Guiding Policies

1.1. This policy and its associated procedures will support a person in exercising his or her right to make an Inquiry or Complaint in respect of the RM&R system, and will enable HICs and RM&R to meet their obligations under PHIPA in this regard.

[12] Note that "person" is used in this policy instead of "Individual" because "Individual" refers to a patient or his or her substitute decision maker; whereas, an inquiry or complaint may be made by anyone, including a person who is not a patient or his or her substitute decision maker.

1.2. HICs and RM&R shall have a program in place to enable RM&R and HICs to satisfy their responsibilities in respect of Inquiries and Complaints related to the RM&R system in accordance with PHIPA and this policy and its associated procedures.

2. Procedures Related to Inquiries

HIC or RM&R Receives Inquiry

2.1. Where a HIC or RM&R receives an Inquiry that it is able to address and respond to, the HIC or RM&R receiving the Inquiry shall follow its own internal policies, procedures, and practices to address the Inquiry.

2.2. Where a HIC or RM&R receives an Inquiry that it is unable to address and respond to related solely to RM&R or to one other HIC, the HIC receiving the Inquiry shall as soon as possible:

- Notify the person that the HIC is unable to respond to the Inquiry because RM&R or another HIC is the subject of the Inquiry; and
- Provide the person with information on how to contact RM&R or the other HIC to make the Inquiry

2.3. Where a HIC or RM&R receives an Inquiry that it is unable to address and respond to related to multiple organizations, the HIC receiving the Inquiry shall as soon as possible:

- Advise the person making the Inquiry that RM&R will coordinate the response to the Inquiry, and will respond directly to the person making the Inquiry; and
- Provide the person with information on how to contact RM&R to make the Inquiry.

RM&R Receives Inquiry Relating to Multiple Organizations

2.4. Where RM&R directly receives an Inquiry that it is unable to address and respond to related to multiple organizations RM&R shall receive and document the Inquiry in accordance with its internal policies, procedures and practices and in accordance with the requirements under paragraph 2.5.

2.5. Where RM&R receives an Inquiry under paragraph 2.4, RM&R shall:

- Log receipt of the Inquiry;
- Obtain sufficient information from the person making the Inquiry in order to facilitate the preparation of a response to the Inquiry;
- Notify the person making the Inquiry that the Inquiry will be forwarded to the HICs to whom the Inquiry relates;
- Advise the person making the Inquiry they will receive a response as soon as possible, but in any event no later than 30 days following RM&R's receipt of the Inquiry;
- Advise the person making the Inquiry that RM&R will coordinate the response to the Inquiry with the other HICs to whom the Inquiry relates, and will respond directly to the person making the Inquiry;
- Advise the person making the Inquiry that RM&R will provide the person with a revised date for response if the Inquiry cannot be responded to within 30 days following receipt of the Inquiry by RM&R; and
- Obtain from the person making the Inquiry the preferred method of contact and contact information for the response to the Inquiry.

2.6. Upon receiving an Inquiry related to more than one HIC, RM&R shall, as soon as possible, but in any event no later than 4 days following receipt of the Inquiry:

- Forward the Inquiry to each HIC to whom the Inquiry relates;
- Notify each HIC that the Inquiry received relates to more than one HIC;
- Provide each HIC with information about the identity of the person making the Inquiry; and
- Coordinate the development of a response strategy, including a timeline for response drafting and review by HICs to whom the Inquiry relates that supports a response to the person making the Inquiry within 30 days following receipt of the Inquiry by RM&R.

2.7. Where one or more HICs do not provide the information necessary to enable RM&R to respond to the Inquiry and do not provide comments on the proposed response in accordance with the agreed upon timelines in paragraphs 2.6, RM&R shall provide written notice to the person making the Inquiry that one

or more HICs have failed to respond to the Inquiry and that the person may make an Inquiry or Complaint directly to the one or more of the HICs that failed to respond or a complaint to the Information and Privacy Commissioner of Ontario.

2.8. RM&R shall provide the response agreed to by the HICs to whom the Inquiry relates to the person making the Inquiry.

3. Procedures Related to Complaints

HIC or RM&R Receives Complaint

3.1. Where a HIC or RM&R directly receives a Complaint related to their own organization, the HIC or RM&R receiving the Complaint shall respond to and address the Complaint according to internal policies and procedures.

3.2. Where a HIC or RM&R directly receives a Complaint related to one or more other organizations, the HIC or RM&R receiving the Complaint shall:

- Notify the person that the HIC is unable to respond to the Complaint because RM&R or one or more other HICs is the subject of the Inquiry; and
- **If the Complaint relates solely to one other HIC:** Provide the person with information on how to contact the other HIC to make the Complaint.
- **If the Complaint relates to more than one other HIC or to RM&R:** Provide the person with information on how to contact RM&R to make the Complaint.

RM&R Receives Complaint Relating to Multiple Organizations

3.3. Where RM&R directly receives a Complaint related to multiple organizations RM&R shall receive and document the Complaint in accordance with its internal policies, procedures and practices and in accordance with the requirements under paragraph 3.4.

3.4. Where RM&R receives a Complaint under paragraph 3.3, RM&R shall:

- Log receipt of the Complaint;
- Obtain sufficient information from the person making the Complaint in order to facilitate the preparation of a response to the Complaint;
- Notify the person making the Complaint that the Complaint will be forwarded to the HICs to whom the Complaint relates, in order to facilitate the preparation of a response to the Complaint; and
- Advise the person making the Complaint that RM&R will coordinate a response between the HICs to whom the Complaint relates, and respond directly to the person making the Complaint as soon as possible, but in any event no later than 30 days following receipt of the Complaint by RM&R;
- Obtain from the person making the Complaint the preferred method of contact and contact information for the response to the Complaint; and
- Advise the person making the Complaint that RM&R will provide the person with a revised date for response if the Complaint cannot be responded to within 30 days following receipt of the Complaint by RM&R.

3.5. Upon receiving a Complaint related to more than one HIC, RM&R shall, as soon as possible, but in any event no later than 4 days following receipt of the Complaint:

- Forward the Complaint to each HIC to whom the Complaint relates;
- Notify each HIC that the Complaint received relates to more than one HIC;
- Provide each HIC with information about the identity of the person making the Complaint; and
- Advise each HIC that it must, as soon as possible, but in any event no later than 14 days following receipt of the forwarded Complaint by the HIC, provide to RM&R the information necessary to enable RM&R to determine whether to investigate the Complaint and, if the Complaint will not be investigated, to draft a proposed response to the Complaint on behalf of each HIC.

3.6. Upon receiving a forwarded Complaint from RM&R related to more than one HIC, each HIC to whom the Complaint relates shall, as soon as possible, but in any event no later than 14 days following receipt of the forwarded Complaint by the HIC, provide RM&R with the information necessary to enable RM&R and the related HICs to determine whether to investigate the Complaint and, if the Complaint will not be

investigated, to draft a proposed response to the Complaint on behalf of each HIC.

3.7. RM&R shall, as soon as possible, but in any event no later than 4 days following receipt of the information under paragraph 3.6, determine whether to investigate the Complaint. A Complaint shall be investigated where the Complaint relates to an actual or suspected Privacy Breach that has occurred or is about to occur in respect of the RM&R system.

3.8. Where RM&R has made a determination not to investigate the Complaint under paragraph 3.7, RM&R shall:

- Notify each HIC to whom the Complaint relates that RM&R has made a determination not to investigate the Complaint; and
- Provide each HIC with a proposed response to the person making the Complaint; and
- Coordinate the development of a strategy to respond to the person making the Complaint, including a timeline for response drafting and review by HICs to whom the Complaint relates, that supports a response to the person making the Complaint within 30 days following receipt of the Complaint by RM&R.

3.9. Where RM&R has made a determination to investigate the Complaint under paragraph 3.7, RM&R shall:

- Notify each HIC to whom the Complaint relates that RM&R has made a determination to investigate the Complaint; and
- Notify each HIC that the Complaint will be investigated and remediated, if applicable, in accordance with the Privacy Breach Management policy and its associated procedures.
- Coordinate the development of a strategy to respond to the person making the complaint, including a timeline for response drafting and review by HICs to whom the Complaint relates, that supports a response to the person making the Complaint within 30 days following receipt of the Complaint by RM&R.

3.10. Where RM&R has made a determination to investigate the Complaint, the Complaint shall be investigated and remediated, if applicable, in accordance with the Privacy Breach Management policy and its associated procedures, as amended from time to time.

3.11. Where one or more HICs do not provide the information necessary to enable RM&R to respond to the Complaint and do not provide comments on the proposed response in accordance with the timelines agreed to in 3.8 and 3.9, RM&R shall provide written notice to the person making the Complaint that one or more HICs have failed to respond to the Complaint and that the person may make a Complaint to the one or more of the HICs that failed to respond and/or to the Information and Privacy Commissioner of Ontario.

3.12. RM&R shall respond to the person making the Complaint. At minimum, the response shall:

- Acknowledge receipt of the Complaint;
- Indicate that an investigation was undertaken in response to the Complaint;
- Provide a summary of the results of the investigation of the Complaint, including whether or not a Privacy Breach occurred and, if so, a description of the Privacy Breach and the scope of and circumstances in which the Privacy Breach occurred;
- Provide a summary of steps that have been or will be taken to address the Complaint and to remediate any actual or suspected Privacy Breach and the timeframe for the implementation of any steps that will be taken;
- Provide the name and contact information for the person or persons to whom the person making the Complaint may address inquiries or concerns; and
- Advise the person making the Complaint that he or she may make a Complaint to the Information and Privacy Commissioner of Ontario.

References	**1. Legislative** • PHIPA, ss. 15, 16(1) and 56.
Document Management	
Policy Number	1

Version	V1 – Initial draft
Version History	TBD
Effective Date	TBD
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Logging and Auditing Policy (PS.Pol.005)

Purpose

- To define the policies and procedures that apply in logging, auditing and monitoring all instances where:
    - All or part of the personal health information (PHI) in the RM&R System is viewed, handled or otherwise dealt with;
    - All or part of the PHI in the RM&R System is transferred to a health information custodian (HIC);
    - All or part of the PHI in the RM&R System is disclosed to and collected by a HIC as a result of an override of a Consent Directive; and
    - A Consent Directive is made, withdrawn or modified in the RM&R System.

To facilitate the identification and investigation of actual or suspected Privacy Breaches or Security Breaches.

Scope

This policy and its associated procedures apply to logging, auditing and monitoring in the RM&R System for the purpose of facilitating the identification and investigation of actual or suspected Privacy Breaches or Security Breaches related to PHI in the RM&R System.

This policy and its associated procedures do not apply to logging, auditing and monitoring in any other system other than the RM&R System.

Policy and Procedures

1. Guiding Policies

1.1. PHIPA requires HICs to retain, transfer and dispose of PHI in a secure manner and to take steps that are reasonable in the circumstances to ensure that PHI in their custody or control is protected against theft, loss and unauthorized use or disclosure.

1.2. RM&R shall have a program in place and provide tools to enable HICs to satisfy their auditing and monitoring requirements in accordance with PHIPA and this policy and its associated procedures.

1.3. RM&R shall have a program in place and provide tools to enable the RM&R System to satisfy its logging, auditing and monitoring requirements in accordance with PHIPA and this policy and its associated procedures.

1.4. This policy and its associated procedures will support HICs and RM&R in meeting their legislative obligations through logging, auditing and monitoring in the RM&R System in order to facilitate the identification and investigation of actual or suspected Privacy Breaches or Security Breaches.

2. Procedures Related to Logging by the RM&R System

2.1. RM&R shall ensure that the RM&R System is capable of logging all instances where:

- All or part of the PHI in the RM&R System is viewed, handled or otherwise dealt with;
- All or part of the PHI in the RM&R System is disclosed to and collected by a HIC as a result of an override of a Consent Directive; and

2.2. A Consent Directive is made, withdrawn or modified in the RM&R System. RM&R shall ensure that the log of all instances where all or part of the PHI in the RM&R System is viewed, handled or otherwise dealt with identifies:

- The individual to whom the PHI relates;
- The referral that is viewed, handled or otherwise dealt with;
- All persons who have viewed, handled or otherwise dealt with the PHI; and
- The date, time and location of the viewing, handling or dealing with the PHI.

2.3. RM&R shall ensure that the log of all instances where all or part of the PHI in the RM&R System is disclosed to and collected by a HIC as a result of an override of a Consent Directive identifies:

- The HIC that disclosed the PHI;
- The HIC that collected the PHI;
- Any agent that collected the PHI on behalf of the HIC;
- The individual to whom the PHI relates;
- The type of PHI that was disclosed;
- The date and time the PHI was disclosed; and
- The purpose of the disclosure.

2.4. RM&R shall ensure that the log of all instances where a Consent Directive is made, withdrawn or modified in the RM&R System identifies:

- The individual or the SDM for the individual who made, withdrew or modified the Consent Directive;
- The Consent Directive implemented in response to the instructions that the individual provided regarding the Consent Directive
- The HIC, agent or other person to whom the directive is made, withdrawn or modified; and
- The date and time the Consent Directive was made, withdrawn or modified.

2.5. RM&R shall provide the Information and Privacy Commissioner of Ontario with the logs set out in paragraph **Error! Reference source not found.** and containing the content set out in paragraphs 2.1 to REF _Ref401237235 \r \h * MERGEFORMAT 2.4 in the event of a review of a HIC, or one of its agents or Electronic Service Providers, by the Information and Privacy Commissioner of Ontario.

2.6. Prior to providing the logs described in paragraph 2.5**Error! Reference source not found.** to the nformation and Privacy Commissioner of Ontario, RM&R shall notify the HIC(s) that are the subject of the logs, that RM&R has been requested to provide the logs to the Information and Privacy Commissioner of Ontario..

2.7. RM&R shall, upon the request of a HIC who requires the logs to audit and monitor compliance with PHIPA, provide the HIC with the logs set out in paragraph 2.1 and containing the content set out in in paragraphs 2.1 to 2.4.

2.8. RM&R shall ensure that logs are securely retained, transmitted, and destroyed in accordance with the *RM&R Information and Information Technology Policy (PS.Pol.101)*.

3. Procedures Related to Auditing and Monitoring by RM&R

3.1. RM&R shall audit and monitor to enable compliance with PHIPA when conducting the auditing and monitoring described in paragraphs 3.2 to 3.5.

3.2. RM&R shall audit and monitor instances where all or part of the PHI in the RM&R System is viewed, handled or otherwise dealt with by agents or Electronic Service Providers to RM&R.

3.3. RM&R shall audit and monitor other instances where all or part of the PHI in the RM&R System is viewed, handled or otherwise dealt with.

3.4. RM&R shall monitor and alert the HIC that collected the PHI in the RM&R System in all instances where all or part of the PHI in the RM&R System is disclosed to and collected by a HIC as a result of an override of a Consent Directive in accordance with RM&R's obligations and the Consent Management Policy and its associated procedures, as amended from time to time.

3.5. RM&R shall audit and monitor all instances where a Consent Directive is made, withdrawn or modified in the RM&R System. Where RM&R identifies any actual or suspected Privacy Breaches, RM&R shall follow the Privacy Breach Management policy and its associated procedures, as amended from time to time. Where RM&R identifies any actual or suspected Security Breaches, RM&R shall follow the *RM&R Information and Information Technology Policy (PS.Pol.101)* as amended from time to time.

4. Procedures Related to Auditing and Monitoring Tools by RM&R

4.1. RM&R will make available to HICs, auditing and monitoring tools and reports to enable HICs to satisfy their auditing and monitoring responsibilities under PHIPA and paragraph 5.

4.2. The auditing and monitoring tools and reports that will be made available by RM&R will be in a secure, immutable and widely used format.

4.3. RM&R will automate auditing and monitoring in the RM&R system as technology becomes available to better support proactive auditing and monitoring in the RM&R system.

5. Procedures Related to Auditing and Monitoring by HICs

5.1. HICs shall audit and monitor to enable compliance with PHIPA and this policy when conducting the auditing and monitoring described in paragraphs **Error! Reference source not found.** to **Error! ference source not found.**

5.2. All HICs shall audit and monitor instances where all or part of the PHI in the RM&R System is viewed, handled or otherwise dealt with by the HIC and agents or Electronic Service Providers to the HIC, other than RM&R and agents or Electronic Service Providers to RM&R.

5.3. Where functionality for HICs to produce their own log reports for auditing purposes does not exist, RM&R will generate two log types for each organization, on a schedule decided and approved by the RM&R Privacy and Security Working Group, that:

5.3.1. Displays a list of all users at an organization who accessed PHI in the RM&R system during the quarter, and all the client/patient records that were accessed

5.3.2. Displays a list of all clients/patients at an organization whose records were accessed during the quarter, and the users who accessed those client/patient records

5.4. All HICs shall audit and monitor instances where the HIC implemented the instructions of an individual or his or her SDM to make a Consent Directive in the RM&R System.

5.4.1. HICs will log and monitor application of Consent Directives in the RM&R System according to internal policies and procedures

5.4.2. Ad-hoc reports documenting all Consent Directives applied by a HIC within a specified period of time can be generated by RM&R upon request

5.5. Upon receiving written electronic notice from RM&R that the HIC has collected all or part of the PHI in the RM&R System as a result of an override of a Consent Directive, the HIC shall comply with the HIC's obligations under PHIPA and the Consent Management policy and its associated procedures, as amended from time to time.

6. Procedures for Establishing Auditing and Monitoring Criteria

6.1. The Privacy and Security Working Group shall establish auditing and monitoring criteria that will be used by RM&R and participating HICs, as the case may be.

6.2. The criteria established shall enable HICs and RM&R to comply with their obligations under PHIPA, and be consistent with industry standards and best practices and shall be based on an assessment of the threats and risks posed to PHI in the RM&R System.

References	**1. Legislative** • PHIPA, ss. 12, 13 and Part V.1 • O. Reg. 329/04, s. 6
Document Management	
Policy Number	PS.Pol.005
Version	1
Version History	V1 – Initial draft

Effective Date	
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Privacy Breach Management Policy (PS.Pol.06)

Purpose

To define the policies and procedures that apply in identifying, reporting, containing, notifying, investigating, and remediating Privacy Breaches in respect of the RM&R system.

Scope

To define the policies and procedures that apply in identifying, reporting, containing, notifying, investigating, and remediating Privacy Breaches in respect of the RM&R system.

This policy and its associated procedures do not apply to Privacy Breaches in respect of any system other than the RM&R system or in respect of any information other than PHI in the RM&R system.

Definitions

For a fulsome list of definitions that apply to all RM&R Privacy and Security Policies and Procedures, see Definitions section of RM&R Privacy Policies.

Privacy Breach

A Privacy Breach includes circumstances where:

- A provision of the Personal Health Information Protection Act, 2004 (PHIPA) or its regulations has been or is about to be contravened;
- The privacy provisions of the Data Sharing Agreement or any other agreement in respect of the RM&R System have been or are about to be contravened;
- The privacy policies, procedures and practices implemented in respect of the RM&R System have been or are about to be contravened;
- Personal health information (PHI) in the RM&R System is lost or stolen or has been or is about to be accessed by an unauthorized person; or
- Records of PHI in the RM&R System have been or are about to be copied, modified or disposed of in an unauthorized manner.

Breach Response Lead

A HIC or RM&R who is chosen to act as a lead to direct and oversee investigation, containment, remediation and reporting activities for management of the Breach. The Breach Response Lead is identified by RM&R in collaboration with the HICs that contributed to PHI to the RM&R system and who were otherwise involved with the breach.

Policies and Procedures

1. Guiding Policies

1.1. PHIPA requires HICs to take steps that are reasonable in the circumstances to ensure that PHI in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records of PHI are protected against unauthorized copying, modification or disposal.

1.2. HICs, RM&R, and Individuals who are subject to the PHI, shall all be notified at the first reasonable opportunity if PHI in the RM&R system is stolen, lost or accessed by unauthorized persons.

1.3. Agents and Electronic Service Providers of RM&R shall, at the first reasonable opportunity, notify RM&R of actual or suspected Privacy Breaches in accordance with RM&R's internal policies,

procedures and practices.

2. Procedures for Identification of Privacy Breaches

2.1. In all cases, an actual or suspected Privacy Breach shall be reported to RM&R as soon as possible, but in any event no later than the end of the next business day after being identified.

2.2. The initial report by a HIC of an actual or suspected breach will be made by telephoning the RM&R program. This will be followed by sending a completed RM&R Breach Report Form to the RM&R program using a secure electronic method. The report shall include any information that is known to the HIC that may assist in the determination of whether a Privacy Breach has occurred, **excluding PHI**.

2.3. Agents and Electronic Service Providers of RM&R shall notify the RM&R program of an actual or suspected breach in person, by telephone or by sending a secure email. This will be followed by submitting a completed RM&R Breach Report Form to the RM&R program office using a secure electronic method. The report shall include any information that is known that may assist in the determination of whether a Privacy Breach has occurred, **excluding PHI**.

2.4. RM&R shall, as soon as possible, assist the HIC in determining whether a Privacy Breach has occurred.

2.5. Where a Privacy Breach is determined not to have occurred, RM&R will log the suspected Privacy Breach in writing, including:

- A description of the circumstances leading to the identification of a suspected Privacy Breach, including a description of the nature and scope of the suspected Privacy Breach; and
- A description of why the suspected Privacy Breach was identified as not an actual Privacy Breach.

2.6. If the suspected Privacy Breach is determined to be an actual Privacy Breach, RM&R will confirm whether the breach impacts only the organization that caused the breach or whether the PHI affected by the breach was created or contributed to by another organization or organizations. If the breach only impacts the HIC that caused the breach, then any further containment, investigation, and remediation will be completed by the HIC.

2.7. Upon determining that an actual Privacy Breach has occurred, RM&R shall notify all other impacted organizations, as soon as possible, but no later than the end of the next business day. The report of breach will be made by telephone by the RM&R program to the affected HIC(s). This will be followed by sending a completed RM&R Breach Report Form to the HIC(s) using a secure electronic method.

3. Identifying the Breach Response Lead

3.1. RM&R, with input and guidance from the HIC(s) who contributed the PHI or organizations otherwise involved in the Privacy Breach, will identify the HIC or RM&R to act as a Breach Response Lead, to lead investigation, containment, notification and remediation activities. The Breach Response Lead shall be identified as soon as possible, but in any event no later than the end of the next business day after the Privacy Breach was confirmed.

3.2. The criteria for identifying the Breach Response Lead will include:

- The HIC(s) that caused the Privacy Breach or the HIC(s) where the breach originated;
- Whether the HICs that caused the Privacy Breach have the capability to investigate the Privacy Breach, and;
- Whether another HIC or RM&R would be more suitable to investigate the Privacy Breach.

RM&R will act as the Breach Response Lead where a Privacy Breach was solely caused by RM&R, by agents or Electronic Service Providers of RM&R or by an unauthorized person who is not an agent or Electronic Service Provider or RM&R or a HIC.

4. Containment

4.1. The Breach Response Lead under section 3.1 shall identify the containment strategies and oversee their successful application.

4.2. The Breach Response Lead will draft and distribute a Breach Report, **excluding PHI,** to RM&R, all HIC(s) that contributed the PHI subject to the Privacy Breach, and any organization that is involved in the Privacy breach, including:

- An acknowledgement of the known custodianship of the PHI that was affected by the breach;
- An acknowledgement of the responsibility for the breach, as known or suspected at the time;
- The name of each agent and Electronic Service Provider of the HICs that caused or contributed to the Privacy Breach, where the name is determined to be relevant by the HIC identified under paragraph 2.3 (e.g., intentional unauthorized collection, use or disclosure of PHI by an agent);
- The date and time of the Privacy Breach;
- A description of the nature and scope of the Privacy Breach;
- The cause of the Privacy Breach;
- A description of the information in the RM&R system that was subject to the Privacy Breach, without disclosing any PHI;
- The measures implemented to contain the Privacy Breach;
- The measures that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in future; and
- The timelines and persons responsible for implementing measures to remediate the Privacy Breach and to prevent similar Privacy Breaches in future.

4.3. Where required, HIC(s) and RM&R will request assistance from other organizations in containing the Privacy Breach. Other organizations shall provide assistance, as needed.

5. Notification to Individual

5.1. The Breach Response Lead shall identify the HIC that will be responsible for notifying the individual(s) to whom the PHI related. Input may be solicited by the Breach Response Lead, on the choice of HIC to notify the individual, from other HICs whose information is involved in the privacy breach. In making the decision, the following criteria will be considered:

- The HIC that caused the Privacy Breach;
- The HIC where the individual(s) most recently received health care; and
- The HIC where the individual(s) received the most health care.

5.2. In notifying the individual(s) to whom the PHI relates, the HIC identified in paragraph 5.1 shall, at a minimum, provide the individual(s) with the following information:

- An indication that the HIC has been identified to notify the individual of the Privacy Breach, and provide the individual with a summary of the results of the investigation;
- The name of the HIC that caused the Privacy Breach;
- The name of each agent and Electronic Service Provider of the HIC that caused the Privacy Breach, where the name of the agent and Electronic Service Provider of the HIC is relevant to the Privacy Breach (e.g., inappropriate viewing, handling, or dealing with PHI);
- The name of each HIC that created and contributed the PHI to the RM&R;
- The date and time of the Privacy Breach;

- A description of the nature and scope of the Privacy Breach;
- A description of the PHI in the RM&R that was subject to the Privacy Breach;
- The measures implemented to contain the Privacy Breach;
- The HIC who will investigate the Privacy Breach;
- The steps that the individual(s) can take to protect their privacy or minimize the impact of the Privacy Breach, if applicable;
- The name and contact information for each HIC who created or contributed the information involved in the Privacy Breach to whom the individual(s) may address inquiries and concerns; and
- Information concerning how to make a complaint to the Information and Privacy Commissioner of Ontario.

5.3. The method for notifying the individual(s) to whom the PHI relates will be decided according to the internal policies and procedures of the HIC identified in paragraph 5.1,

5.4. RM&R and other HICs shall provide assistance in developing the notification to the individual(s) to whom the PHI relates when requested to do so by the HIC identified in paragraph 5.1.

6. Investigation

6.1. The Breach Response Lead shall, as soon as possible, but in any event no later than 7 days after the Privacy Breach has been confirmed, follow its own internal policies, procedures and practices to begin an investigation into the Privacy Breach in accordance with the requirements of paragraph 6.3.

6.2. The Breach Response Lead shall, as soon as possible, work with the organizations who created or contributed to the PHI involved with the Privacy Breach (as applicable) and the organizations that caused or contributed to the Privacy Breach, to document and agree upon a schedule and timeframe for drafting and distribution of status update reports and other formal documents (including their review and finalization timeline and procedure).

6.3. In conducting the investigation, the Breach Response Lead shall:

- Determine the nature and scope of the Privacy Breach;
- Determine the cause of the Privacy Breach;
- Ensure the Privacy Breach has been effectively contained or determine whether further measures to contain the Privacy Breach must be implemented;
- Evaluate the adequacy of the administrative, technical and physical safeguards;
- Determine what measures must be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in future; and
- Determine the timelines and persons responsible for implementing measures to remediate the Privacy Breach and to prevent similar Privacy Breaches in future.

6.4. Other HICs and RM&R shall provide assistance in investigating the Privacy Breach when requested to do so by the Breach Response Lead.

6.5. As soon as possible, but in any event no later than 7 days after the completion of the investigation of the Privacy Breach, the Breach Response Lead shall complete and distribute to each organization involved in the Privacy Breach the RM&R Breach Report, summarizing the results of the investigation, and setting out the remediation plan.

6.6. Each organization that caused the breach or contributed the PHI that was impacted by the breach will have an opportunity to review and revise the draft Breach Report, on a scheduled determined by the Breach Response Lead.

6.7. As soon as possible, but in any event no later than 3 days after receipt of other organization's revisions, the Breach Response Lead will submit the final Breach Report to RM&R.

7. Remediation of Privacy Breaches

7.1. As soon as possible, but in any event no later than 7 days after receipt of the final written Breach Report under paragraph 6.7, RM&R will forward the report to the Executive Committee for review and approval.

7.2. As soon as possible, but within 4 days of approval of the written Breach Report by the Executive Committee, RM&R shall forward the report to each organization involved in resolving the Privacy Breach, and to each organization with responsibilities for remediating the Privacy Breach or for preventing similar Privacy Breaches in future.

7.3. Organizations shall implement measures identified in the written report approved by the Executive Committee to remediate the Privacy Breach and to prevent similar Privacy Breaches in future.

7.4. Each organization responsible for implementing approved remediation measures shall provide, on a schedule determined in 8.1, a written report to RM&R setting out:

- The remediation measures that the organization is responsible for implementing as identified in the written report approved by the Executive Committee;
- In respect of each measure that the organization is responsible for implementing, the timeline for implementation set out in the written report approved by the Executive Committee;
- The status of implementation of each measure;
- For those measures that have yet to be implemented, the target date for implementation;
- For those measures that have been implemented, the date of implementation; and

7.5. The manner in which each measure was or is expected to be implemented.

7.6. As soon as possible upon completion of all remediation activities approved by the Executive Committee, the Breach Response Lead will complete and submit to RM&R a final breach report that sets out:

- A summary of the Privacy Breach and how it was managed;
- The remediation measures that were approved by the Executive Committee;
- The date of implementation of each measure; and
- The manner in which each measure was implemented.

8. Reporting to RM&R and HICs

8.1. The Breach Response Lead, in coordination with the organizations involved with management of the Privacy Breach, will determine a strategy and timeframe for providing regular updates on the status of Privacy Breach management activities to all HIC(s) who were responsible for or contributed to the Privacy Breach, to all HIC(s) who created or contributed to the PHI subject to the Privacy Breach, and/or to RM&R (as the case may be).

8.2. The Executive Committee will determine a strategy and timeframe for providing update reports on the status of Privacy Breach management activities to the Executive Committee (EC).

8.3. At a minimum, the written report in paragraphs 8.1 and 8.2 shall set out:

- The measures that RM&R and/or HICs were responsible for implementing as identified in the written report approved by the Executive Committee;
- The timelines for implementation of each measure as set out in the written report approved by the Executive Committee;
- The status of implementation of each measure;

- For those measures that have yet to be implemented, the target date for implementation;
- For those measures that have been implemented, the date of implementation; and
- The manner in which each measures was or is expected to be implemented

9. Procedures Related to the Maintenance of Privacy Breach Logs

9.1. RM&R shall keep a log of all Privacy Breaches which shall include, for each Privacy Breach:

- The name of each organization that was responsible for the Privacy Breach;
- The name of each person that was responsible for the Privacy Breach, where the name of the person is relevant to the breach (e.g., inappropriate viewing, handling, or otherwise dealing with PHI), if applicable;
- The name of each HIC that created and contributed the PHI to the RM&R system;
- The date and time of the Privacy Breach;
- The nature and scope of the Privacy Breach;
- The cause of the Privacy Breach;
- A description of the information in the RM&R system that was subject to the Privacy Breach, without disclosing any PHI;
- The measures implemented to contain the Privacy Breach;
- The measures that have been or will be implemented to remediate the Privacy Breach and to prevent similar Privacy Breaches in future;
- The timelines and persons responsible for implementing measures to remediate the Privacy Breach and to prevent similar Privacy Breaches in future;
- The status of implementation of the measures to remediate the Privacy Breach and to prevent similar Privacy Breaches in future and, for those measures that have yet to be implemented, the target date for implementation, and for those measures that have been implemented, the date of implementation; and

9.2. The manner in which each measure was or is expected to be implemented.

9.3. RM&R shall audit and monitor the log in paragraph 9.1 to:

- Identify patterns or trends in Privacy Breaches;
- Identify administrative, physical or technical safeguards that must be implemented to prevent or minimize the risk of Privacy Breaches; and

9.4. Ensure that measures to remediate Privacy Breaches and to prevent similar Privacy Breaches in future are implemented.

References	**1. Legislative** • PHIPA, ss. 12, 13, 17(3) and Part V.1 • O. Reg. 329/04, s 6 (3) 1. **2. IPC Guidance** • What to Do When Faced with a Privacy Breach: Guidelines for the Health Sector. IPC/Ontario.

Document Management	
Policy Number	PS.Pol.006
Version	1
Version History	v1 – Initial release

Effective Date	
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Privacy and Security Training Policy (PS.Pol.07)

Purpose	To define the policies and procedures for providing privacy and security training in respect of the RM&R Solution.
Scope	This policy and its associated procedures apply to the provision of privacy and security training to health information custodians (HICs), RM&R and agents and Electronic Service Providers of HICs and RM&R in respect of the RM&R system, including Strata IQ. This policy and its associated procedures do not apply to privacy and security training: • In respect of any other system other than the RM&R system; • In respect of any other information other than PHI in the RM&R system; • To any agents of HICs who do not collect, use or disclose PHI in the RM&R system; • To any Electronic Service Providers of HICs who do not view, handle or otherwise deal with PHI in the RM&R system; or • To any agents or Electronic Service Providers of RM&R who do not view, handle or otherwise deal with PHI in the RM&R system. This policy and its associated procedures also do not apply to basic privacy and security training, also known as privacy and security awareness training.

Policies and Procedures

1. Guiding Policies

1.1. PHIPA requires a HIC that is not a natural person to designate a contact person to facilitate the HIC's compliance with the *Personal Health Information Protection Act, 2004* (PHIPA) and to ensure that all agents of the HIC are appropriately informed of their duties under PHIPA.

1.2. PHIPA permits a HIC that is a natural person to designate a contact person to facilitate the HIC's compliance with PHIPA and to ensure that all agents of the HIC are appropriately informed of their duties under PHIPA. Where a HIC that is a natural person does not designate a contact person to perform these functions, the HIC is required to perform these functions on his or her own.

1.3. PHIPA requires RM&R to ensure that those acting on its behalf agree to comply with conditions and restrictions necessary to enable RM&R to comply with PHIPA.

1.4. HICs and RM&R shall have in place and maintain policies, procedures and practices in respect of privacy and security that comply with PHIPA and provide training to their agents and electronic service providers on the policies, procedures and practices as required by PHIPA.

1.5. HICs and RM&R shall take steps that are reasonable in the circumstances to ensure their agents and Electronic Service Providers comply with PHIPA and this policy and its associated procedures.

2. Procedures Related to Creating Privacy and Security Training Materials

2.1. RM&R shall develop and share privacy and security training materials that may be used by HICs to

support them in training their agents and Electronic Service Providers who collect, use and disclose PHI in the RM&R System or who view, handle or otherwise deal with PHI in the RM&R System, as the case may be, on their privacy and security duties and obligations.

2.2. RM&R shall ensure that the privacy and security training materials are role-based to enable HICs and agents and Electronic Service Providers of HICs and RM&R to understand how to meet their duties and obligations in respect of the RM&R system in their day-to-day operations.

2.3. At a minimum, the privacy and security training materials shall address the requirements described in paragraph 5.1. RM&R will review and refresh the privacy and security training materials in circumstances where amendments to the privacy and security policies, procedures and practices will impact the duties and obligations of HICs, RM&R and/or their agents and Electronic Service Providers in respect of the RM&R system.

3. Procedures Related to Delivering Privacy and Security Training

3.1. HICs shall ensure that all their agents and Electronic Service Providers, other than RM&R are appropriately informed of their relevant duties under PHIPA and the RM&R privacy and security policies, procedures and practices, prior to permitting the agents and Electronic Service Providers to collect, use or disclose PHI in the RM&R system or to view, handle or otherwise deal with PHI in the RM&R System, as the case may be.

3.2. RM&R shall ensure that all its agents and Electronic Service Providers are appropriately informed of their relevant duties under PHIPA and the RM&R privacy and security policies, procedures and practices, prior to permitting its agents and Electronic Service Providers to view, handle or otherwise deal with PHI in the RM&R System.

3.3. HICs and RM&R shall not permit their agents and Electronic Service Providers to continue to collect, use or disclose PHI in the RM&R system or to continue to view, handle or otherwise deal with PHI in the RM&R system, as the case may be, unless the agent or Electronic Service Provider has been appropriately informed of its relevant duties under PHIPA and the RM&R privacy and security policies, procedures and practices.

3.4. When informing their agents and Electronic Service Providers of their duties under PHIPA and the RM&R privacy and security policies, procedures, and practices, HICs and RM&R shall ensure that the agent or Electronic Service Provider is informed, if relevant to their day-to-day duties, of the information described in paragraph 5.1.

3.5. HICs and RM&R shall impose consequences on agents and Electronic Service Providers who do not understand their relevant duties under PHIPA and the RM&R privacy and security policies, procedures, and practices.

3.6. HICs and RM&R shall be able to demonstrate with evidence that their agents and Electronic Service Providers understand their relevant duties under PHIPA and the RM&R privacy and security policies, procedures, and practices.

4. Procedures Related to End User Agreements

4.1. RM&R shall ensure that the RM&R System requires HICs as well as agents and Electronic Service Providers of HICs and RM&R to acknowledge and agree to comply with the duties and obligations in the end user agreement prior to collecting, using or disclosing PHI in the RM&R System or prior to viewing, handling or otherwise dealing with PHI in the RM&R System, as the case may be, and at a minimum, every year thereafter.

4.2. RM&R shall ensure that the RM&R System does not permit agents and Electronic Service Providers of HICs and RM&R to collect, use or disclose PHI in the RM&R System or to view, handle or otherwise deal with PHI in the RM&R System, as the case may be, unless the agent or Electronic Service Provider has acknowledged and agreed to comply with the duties and obligations in the annual end user agreement.

4.3. RM&R shall develop and implement an end user agreement that, at a minimum:

- Sets out the purposes for which HICs and agents and Electronic Service Providers of HICs are permitted to collect, use or disclose PHI in the RM&R system or to view, handle or otherwise deal with PHI in the RM&R system, as the case may be;
- Sets out the purposes for which agents and Electronic Service Providers of RM&R are permitted to view, handle or otherwise deal with PHI in the RM&R system;
- Requires HICs and agents and Electronic Service Providers of HICs and RM&R to acknowledge that they have read, understood and agreed to comply with the privacy and security policies, procedures and practices in respect of the RM&R system;
- Requires HICs and agents and Electronic Service Providers of HICs and RM&R to agree to comply with PHIPA;
- Requires HICs and agents and Electronic Service Providers of HICs and RM&R to implement the administrative, technical and physical safeguards set out in the end user agreement to protect PHI in the RM&R system;
- Requires HICs and agents and Electronic Service Providers of HICs and RM&R to provide notification in accordance with the Privacy Breach Management Policy and its associated procedures, as amended from time to time, if they believe that an actual or suspected Privacy Breach has occurred or is about to occur in respect of the RM&R system; and
- Sets out the consequences of breach of the end user agreement.

5. Training Content

5.1. The content for training shall include the following information if the role of the agent or Electronic Service Provider requires it:

- The nature of PHI that is retained in the RM&R System;
- The status under PHIPA of RM&R and other organizations participating in the RM&R System and the duties and obligations arising from this status;
- All of the permitted and known purposes for which HICs and their agents and Electronic Service Providers are permitted to collect, use and disclose PHI in the RM&R System or to view, handle or otherwise deal with PHI in the RM&R System, as the case may be, and the limitations placed thereon;
- The authority for the collection, use and disclosure of PHI in the RM&R System or the viewing, handling or dealing with PHI in the RM&R System, as the case may be, by HICs and their agents and Electronic Service Providers;
- The purposes for which PHI in the RM&R System is permitted to be viewed, handled or otherwise dealt with by RM&R and its agents and Electronic Service Providers and the limitations placed thereon;
- The authority for viewing, handling or dealing with PHI in the RM&R System by RM&R and its agents and Electronic Service Providers;
- The processes or materials available to HICs and their agents to ensure that consent is knowledgeable;
- An overview of the privacy and security policies, procedures and practices that have been implemented in respect of the RM&R System and the duties and obligations of HICs and agents and Electronic Service Providers of HICs and RM&R arising from these policies, procedures and practices;
- The consequences of breach of the privacy and security policies, procedures and practices

implemented in respect of the RM&R System;

- The administrative, technical and physical safeguards put in place to protect PHI in the RM&R System against theft, loss and unauthorized use or disclosure and to protect records of PHI in the RM&R System from unauthorized copying, modification or disposal;
- The duties and obligations of HICs and agents and Electronic Service Providers of HICs and RM&R in implementing the administrative, technical and physical safeguards;
- The end-user agreement that HICs and agents and Electronic Service Providers of HICs and RM&R must acknowledge and agree to comply with; and
- The duties and obligations of HICs and agents and Electronic Service Providers of HICs and RM&R with respect to identifying, reporting, containing and participating in the investigation and remediation of Privacy Breaches and Security Breaches.

References	**1. Legislative** • PHIPA, ss. 10, 15 and 17 and Part V.1 • PHIPA, Reg. 329/04, s. 6

Document Management	
Policy Number	PS.Pol.051
Version	1
Version History	
Effective Date	
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Retention Policy (PS.Pol.008)

Purpose

To define the policies and procedures that apply in retaining records of personal health information (PHI) in respect of the RM&R system and information collected from Individuals to assist in fulfilling their requests, responding to Inquiries or Complaints, or investigating a Privacy Breach.

Scope

This policy and its associated procedures apply to retention of:

- PHI in respect of the RM&R system, including Strata IQ; and
- Information collected to respond to Individuals related to their:
  - Requests for Access or Requests for Correction under PHIPA;
  - Requests to make, modify, or withdraw a Consent Directive under PHIPA; and
  - Inquiries or Complaints under PHIPA.
- Information created about Individuals to investigate Privacy Breaches.

This policy and its associated procedures do not apply to copies of records of PHI that have been made from the RM&R system and retained by the HIC, or by the agents or Electronic Service Providers of the HIC, other than RM&R and its agents or Electronic Service Providers.

Policies and Procedures

1. Guiding Policies

1.1. The Personal Health Information Protection Act (PHIPA) requires a HIC to ensure that the records of PHI that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with any requirements under PHIPA.

1.2. PHIPA requires that a HIC retain records of PHI subject to a request for access under section 53 for as long as necessary to allow the individual to exhaust any recourse under PHIPA that he or she may have with respect to the request.

1.3. RM&R shall have a program in place to enable RM&R and HICs to satisfy their obligations in retaining records of PHI in accordance with PHIPA and this policy and its associated procedures.

1.4. HICs and RM&R shall maintain records of PHI in respect of the RM&R Solution in accordance with all applicable legal statutes, professional regulations, generally accepted industry practices, and policies, procedures, and practices.

1.5. This policy will not interfere with the retention requirements established in legislation or other policies of the HICs and RM&R.

2. Procedures Related to Retaining PHI

2.1. RM&R shall ensure that the RM&R Solution is capable of retaining records of PHI for as long as required under paragraph 2.2.

2.2. PHI shall be retained for the longer of the following time periods:

- as long as the HIC that created and contributed the PHI to the RM&R System retains the PHI in its local systems;
- in accordance with the retention schedule of the HIC that created and contributed the PHI to the RM&R System; or

- in accordance with the retention schedule in paragraph 4.1.

2.3. At the end of the retention schedule in paragraph 4.1, PHI will no longer be made available to HICs or RM&R, or their agents or Electronic Service Providers.

2.4. Despite paragraph 2.2, where the relationship between RM&R and the HIC that created and contributed the PHI to the RM&R Solution is terminated, the RM&R Privacy and Security Working Group will work with the HIC that created and contributed the PHI to the RM&R Solution to address the disposition of the PHI created and contributed by the HIC to the RM&R Solution in a manner that complies with PHIPA, the Data Sharing Agreement, and the RM&R Privacy and Security Policies and their associated procedures.

2.5. HICs and RM&R, and their agents and Electronic Service Providers, shall take steps that are reasonable in the circumstances to ensure that PHI is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the PHI are protected against unauthorized copying, modification or disposal at rest and during transit by adhering to the *RM&R Information and Information Technology Policy (PS.Pol.101)* as amended from time to time.

3. Procedures Related to the Secure Disposal of PHI

3.1. HICs and RM&R, and their agents and Electronic Service Providers, shall ensure that records of PHI are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstance in accordance with the policies and procedures established in the *RM&R Information and Information Technology Policy (PS.Pol.101)* and its associated policies and procedures.

4. Retention Schedule

4.1. RM&R shall retain for:

Information Type	**Retention Period**
PHI in the RM&R Solution	30 years after the most recent instance of PHI being viewed, handled, or otherwise dealt with for the purpose of providing or assisting in the provision of healthcare; or 10 years after the patient has expired.
Audit logs or reports containing PHI	The longer of 30 years or when PHI is removed from the RM&R System.
Archival copies of the RM&R solution, audit logs, or audit reports	Equals the retention period of the RM&R System or the audit logs and reports.
Backups of the RM&R solution, audit logs or reports	Securely destroyed according to the schedule of the Electronic Service Provider, but retained no longer than 2 years[13].
Information about an Individual in relation to a Request for Access, Request for Correction, request to make, modify, or withdraw a	2 years after the Request for Access, Request for Correction, request to make, modify, or withdraw a Consent Directive, or an Inquiry has been closed.

[13] NOTE that the retention schedule for external media must be established by the Electronic Service Provider. Although the HIC is accountable for any PHI contained on the external media, the external media is retained to support the backup or disaster recovery strategy that the Electronic Service Provider has developed. Therefore, the retention schedule for external media is left to the discretion of the electronic service provider, but no longer than 2 years.

Consent Directive, or an Inquiry	
Information about an Individual in relation to a Complaint or Privacy Breach	2 years after the Complaint or Privacy Breach has been closed by the HIC, RM&R or the Information and Privacy Commissioner of Ontario, whichever is longer.

References

1. Legislation and Regulation

- PHIPA, Part II

2. IPC Decisions and Findings

- Order HO-004, March 7, 2007.
- Order HO-007, January 14, 2010.
- Order HO-008, June 30, 2010.

3. IPC Guidance

- Get rid of it securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information, October 2009.

Document Management

Policy Number	PS.Pol.007
Version	1
Version History	v1 – Initial release
Effective Date	
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

Assurance Policy (PS.Pol.009)

Purpose	This document defines the policies, procedures and practices that health information custodians (HICs) and RM&R shall have in place to provide assurance that HICs and RM&R comply with their obligations under the Personal Health Information Protection Act, 2004 (PHIPA), the Data Sharing Agreement, as amended from time to time, and the policies, procedures and practices implemented in respect of the RM&R System.
Scope	This policy and its associated procedures apply to the conduct of RM&R, HICs who create and contribute or who collect, use or disclose personal health information (PHI) in the RM&R System, and agents and Electronic Service Providers of the HICs or RM&R.

Policies and Procedures

1. Guiding Policies

1.1. HICs and RM&R shall ensure alignment between the Data Sharing Agreement, as amended from time to time and the policies, procedures and practices implemented in respect of the RM&R System.

1.2. HICs and RM&R shall provide training to their agents and Electronic Service Providers on this policy and its associated procedures as well as on their internal policies, procedures and practices in respect of assurance.

1.3. HICs and RM&R shall identify and mitigate privacy and security risks and areas of non-compliance in respect of the RM&R System, including through privacy and security readiness self-assessments, privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents and Electronic Service Providers. RM&R shall additionally conduct privacy impact assessments and assurance of all third parties in respect of the RM&R System.

1.4. HICs and RM&R shall report any privacy or security risks and areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the RM&R System to the Executive Committee.

1.5. HICs and RM&R shall comply with the decisions and directions of the RM&R Executive Committee and shall cooperate in any audits conducted by the Executive Committee pursuant to this policy and its associated procedures.

2. Procedures for Privacy Impact Assessments and Threat Risk Assessments

2.1. RM&R shall monitor and identify significant changes in respect to::

- New PHI feed/source;
- New types or roles of HICs or agents of HICs who are collecting, using or disclosing PHI;
- New types or roles of RM&R or Electronic Service Providers who are viewing, handling or dealing with PHI;
- New collections, uses or disclosures of PHI by HICs and their agents;
- New viewing, handling or dealing with PHI by RM&R or Electronic Service Providers;
- Changes to existing front-end or back-end architecture or functionality that could be expected to impact the privacy of individuals or the security of their PHI;
- Any other significant technical change or addition to the solution;
- Changes to operational support model or operational systems, processes or parties that could be

expected to impact the privacy of individuals or the security of their PHI;

- Changes to the Data Sharing Agreement, as amended from time to time that could be expected to impact the privacy of individuals or the security of their PHI;
- Legislative changes to PHIPA that could be expected to impact the privacy of individuals or the security of their PHI; or
- A vulnerability that has or may result in a privacy breach within the meaning of the *Privacy Breach Management Policy* and its associated procedures, as amended from time to time.

2.2. RM&R shall provide a written report to the Executive Committee that shall:

- Describe the circumstance(s) and the impact of the circumstance(s) on the privacy of individuals or the security of their PHI; and
- Make a recommendation as to whether RM&R should conduct or revise a privacy impact assessment (PIA) or threat risk assessment (TRA), and if so, the timeline within which the documents should be completed.

2.3. The RM&R Executive Committee, shall, at its next meeting following receipt of the report and recommendation under paragraph 2.2:

- Review and approve the report and recommendation received; and
- Provide a written copy of its decision and directions to RM&R.

2.4. If the decision is to have a PIA and/or TRA completed, RM&R shall provide periodic written updates on the status of the PIA and/or TRA to the Executive Committee, as directed by the Executive Committee.

2.5. The person drafting the PIA shall establish criteria that will be used in determining whether each privacy and security risk and area of non-compliance identified in a PIA or TRA is a "high," "medium" or "low" risk. The RM&R Privacy Program shall be consulted by the person drafting the PIA in the establishment of the criteria.

2.6. The person drafting the PIA shall assign a risk rating to each privacy and security risk and area of non-compliance identified in the PIA or TRA, in accordance with paragraph 2.5.

2.7. RM&R shall:

- Develop a remediation plan[14];
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "high" risk rating; and
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating or provide a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance.

2.8. RM&R shall, as soon as possible, but in any event no later than 30 days after completing or updating a PIA or TRA, provide the RM&R Privacy and Security Working Group with:

- A copy of the PIA or TRA;

[14] For purposes of this policy and its associated procedures, a remediation plan shall, at a minimum, include the measures to mitigate the privacy and security risks and areas of non-compliance identified and the timelines and persons responsible for implementing the measures.

- The risk rating assigned to each privacy and security risk and area of non-compliance identified;
- The remediation plan; and
- A rationale for not mitigating one or more privacy and security risks and areas of non-compliance assigned a “medium” or “low” risk rating.

2.9. The Privacy and Security Working Group shall, as soon as possible, but in any event no later than at its next meeting following receipt of the information under paragraph 2.8:

- Review the information received;
- Ensure all privacy and security risks and areas of non-compliance have been identified;
- Ensure the risk rating assigned to each privacy and security risk and area of non-compliance identified accords with paragraph 2.5;
- Ensure the remediation plan adequately mitigates privacy and security risks and areas of non-compliance assigned a “high” risk rating;
- Ensure the remediation plan adequately mitigates privacy and security risks and areas of non-compliance assigned a “medium” or “low” risk rating or provides a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance; and
- Provide its written recommendations to the RM&R Program, including required changes and timeframes for revision.

2.10. If changes are required, RM&R shall amend and re-submit the PIA or TRA and remediation plan to the RM&R Privacy and Security Working Group for approval in accordance with the timeframe set out in the written directions under paragraph 2.9 when directed to do so.

2.11. RM&R shall, upon the approval of the PIA or TRA and remediation plan by the RM&R Privacy and Security Working Group:

- Provide a copy of the PIA or a written summary of the TRA, as well as a copy of the remediation plan, to each HIC who creates and contributes or who collects, uses or discloses PHI in the RM&R System;
- Provide an update on the PIA and/or TRA and remediation plan to the Executive Committee;
- Implement the remediation plan;
- Provide written updates on the status of implementation of the remediation plan at each meeting of the Privacy and Security Working Group; and
- Provide a written attestation to the Privacy and Security Working Group and the Executive Committee that the remediation plan has been fully implemented, as soon as possible, but in any event no later than 30 days after implementation.

2.12. The Privacy and Security Working Group shall monitor compliance of RM&R with the implementation of the remediation plan, and may require further documented evidence to demonstrate compliance. RM&R shall comply with any request from the Privacy and Security Working Group for documented evidence to demonstrate compliance.

3. Procedures for Privacy and Security Readiness Self-Assessment

3.1. A Privacy and Security Readiness Self-Assessment will be completed by an organization before joining RM&R.

3.2. The RM&R Privacy and Security Program, in consultation with the RM&R Executive Committee, shall establish:

- The requirements in the privacy and security readiness self-assessment that must be used to evaluate the privacy and security readiness and to identify the privacy and security risks and areas of non-compliance with PHIPA, the RM&R Data Sharing Agreement and RM&R Privacy and Security Policies and Procedures, posed by RM&R and HICs who create and contribute or who collect, use or disclose PHI in the RM&R System; and
- Whether a failure to satisfy each requirement is a "high," "medium" or "low" risk.

3.3. The RM&R Privacy and Security Program shall create, maintain and administer the privacy and security readiness self-assessments in respect of each HIC who creates and contributes or who collects, uses or discloses PHI in the RM&R System. RM&R will validate that the procedures reflect requirements agreed to through the RM&R Data Sharing Agreement.

3.4. Prior to a HIC contributing or collecting, using or disclosing PHI in the RM&R System, the HIC shall:

- Complete the privacy and security readiness self-assessment;
- Develop a remediation plan where outstanding risks are identified;
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "high" risk rating;
- Ensure the remediation plan includes measures to mitigate privacy and security risks and areas of non-compliance assigned a "medium" or "low" risk rating or provides a rationale for not mitigating one or more of these privacy and security risks and areas of non-compliance; and
- Ensure an Officer signs-off on the privacy and security readiness self-assessment and remediation plan.

3.5. As soon as possible, but in any event prior to a HIC contributing or collecting, using or disclosing PHI in the RM&R System, RM&R will assign a risk rating to each privacy and security risk and area of non-compliance identified in the privacy and security readiness self-assessment in accordance with paragraph 3.2.

3.6. As soon as possible, but in any event prior to RM&R viewing, handling or dealing with PHI or prior to a HIC contributing or collecting, using or disclosing PHI in the RM&R System, RM&R or the HIC, as the case may be, shall provide the Executive Committee with:

- A copy of the completed privacy and security readiness self-assessment;
- The risk rating assigned to each privacy and security risk and area of non-compliance identified;
- The remediation plan; and
- A recommendation for how to proceed.

3.7. The Executive Committee shall, as soon as possible, but in any event prior to RM&R viewing, handling or dealing with PHI or prior to a HIC contributing or collecting, using or disclosing PHI in the RM&R System review and approve the information received.

3.8. If changes are required, the HIC shall amend and re-submit the privacy and security readiness self-assessment and remediation plan to the RM&R Privacy and Security Program for approval in accordance with the timeframe set out in the written directions under paragraph 3.6 when directed to do so.

3.9. The HIC shall, upon the approval of the privacy and security readiness self-assessment and remediation plan by the RM&R Executive Committee:

- Implement the remediation plan prior to the HIC contributing or collecting, using or disclosing PHI in the RM&R System;
- Provide written updates on the status of implementation of the remediation plan to the RM&R

Privacy and Security Program, as directed by RM&R; and

- Provide a written attestation to the Executive Committee that the remediation plan has been fully implemented, as soon as possible, but in any event no later than 30 days after implementation.

3.10. RM&R shall monitor compliance of the HIC with the implementation of the remediation plan approved by the RM&R Executive Committee and may require further documented evidence to demonstrate compliance. The HIC shall comply with any request from RM&R for documented evidence to demonstrate compliance.

4. Procedures for Privacy and Security Operational Self-Attestation

4.1. The RM&R Privacy and Security Program, in consultation with the RM&R Privacy and Security Working Group, shall establish:

- The requirements in the privacy and security operational self-attestation that must be used to evaluate the ongoing operational privacy and security posture and to identify the privacy and security risks and areas of non-compliance with PHIPA, the RM&R Data Sharing Agreement and RM&R Privacy and Security Policies and Procedures, posed by RM&R and HICs who create and contribute or who collect, use or disclose PHI in the RM&R System;
- Whether a failure to satisfy each requirement is a “high,” “medium” or “low” risk; and
- The timeframe each year in which the privacy and security operational self-attestation must be administered and completed.

4.2. RM&R shall create, maintain and administer privacy and security operational self-attestations in respect of each HIC who creates and contributes or who collects, uses or discloses PHI in the RM&R System.

4.3. Within the timeframe each year stipulated by the Privacy and Security Working Group under paragraph 4.1, HICs creating and contributing or collecting, using or disclosing PHI in the RM&R System shall:

- Complete the privacy and security operational self-attestation;
- Develop a remediation plan for each area of non-compliance;
- Ensure an Officer signs-off on the privacy and security operational self-attestation and remediation plan; and
- Submit completed package to RM&R.

4.4. RM&R will review the completed privacy and security operational self-attestation and assign a risk rating to each privacy and security risk and area of non-compliance in accordance with paragraph 4.1.

4.5. As soon as possible, but in any event no later than 30 days after the timeframe stipulated under paragraph 4.1, RM&R shall provide the Privacy and Security Working Group with:

- A summary of the results of the completed privacy and security operational self-attestations for all HICs RM&R Participating HICs;
- A summary of the risk ratings assigned to each privacy and security risk and areas of non-compliance identified;
- A summary of the remediation plans; and
- Recommendations for next steps.

4.6. The Privacy and Security Working Group shall, as soon as possible, but in any event no later than at its next scheduled committee meeting after receipt of the information under paragraph4.5:

- Review and approve the information received; or

- Recommend changes and timeframe for amendment.

4.7. If required, the HIC shall amend and re-submit the privacy and security operational self-attestation and remediation plan to RM&R.

4.8. If required, RM&R will forward the amended privacy and security operational self-attestation and remediation plan to the Privacy and Security Working Group for approval in accordance with the timeframe set out in the written directions under paragraph 4.6 when directed to do so.

4.9. Each HIC shall, upon the approval of the privacy and security operational self-attestation and remediation plan by the RM&R Privacy and Security Working Group:

- Implement the remediation plan;
- Provide written updates on the status of implementation of the remediation plan, as directed by RM&R; and
- Provide a written attestation to the Privacy and Security Working Group that the remediation plan has been fully implemented as soon as possible, but in any event no later than 30 days after implementation.

4.10. RM&R shall monitor compliance of the HIC with the implementation of the approved remediation plan and may require further documented evidence to demonstrate compliance. The HIC shall comply with any request from RM&R for documented evidence to demonstrate compliance.

5. Assurance of Agents, Electronic Service Providers and Third Parties

5.1. RM&R shall ensure that any agents, Electronic Service Providers and third parties it retains to assist in providing services in respect of the RM&R System comply with the restrictions and conditions that are necessary to enable RM&R to comply with PHIPA, the Data Sharing Agreement, as amended from time to time and the policies, procedures and practices implemented in respect of the RM&R System.

5.2. HICs shall take steps that are reasonable in the circumstances to ensure that their agents and Electronic Service Providers comply with PHIPA, the Data Sharing Agreement, as amended from time to time and the policies, procedures and practices implemented in respect of the RM&R System.

6. Auditing and Monitoring

6.1. RM&R and HICs creating and contributing or collecting, using or disclosing PHI in the RM&R System shall conduct auditing and monitoring of activities in respect of the RM&R System in accordance with PHIPA, the Data Sharing Agreement, as amended from time to time and the policies, procedures and practices implemented in respect of the RM&R System, including the *Logging and Auditing Policy,* and *Privacy Breach Management Policy* and their associated procedures, as amended from time to time.

6.2. RM&R and HICs creating and contributing or collecting, using or disclosing PHI in the RM&R System shall, at the first reasonable opportunity, report to RM&R any privacy or security risks or areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the RM&R System that are not identified in PIAs, TRAs, privacy and security readiness self-assessments and privacy and security operational self-attestations.

6.3. RM&R shall determine whether any privacy or security risks or areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the RM&R System identified in PIAs, TRAs, privacy and security readiness self-assessments and privacy and security operational self-attestations may require an audit by RM&R.

6.4. RM&R will submit a written report of the reported privacy and security risk(s) and include recommendations for next steps.

6.5. The Privacy and Security Working Group shall, as soon as possible, but in any event no later than at its next meeting following receipt of the report under paragraph 6.4 or RM&R having identified privacy or security risks or areas of non-compliance under paragraph 6.3:

- Solicit comments from RM&R or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be;
- Assess whether there are privacy or security risks or areas of non-compliance that could be expected to impact the privacy of individuals or the security of their PHI in the RM&R System;
- Assess whether RM&R or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be, has or will be implementing measures to mitigate the privacy or security risks or areas of non-compliance;
- Assess whether an audit should be conducted;
- Provide the RM&R Executive Committee with the report received under paragraph 6.4, if applicable, and the comments received from RM&R or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be; and
- Provide the RM&R Executive Committee with its written recommendations.

6.6. In providing recommendations to the RM&R Executive Committee under paragraph 6.5, the Privacy and Security Working Group shall:

- Where it is recommended that an audit be conducted, include recommendations in respect of the nature and scope the audit, the process to be followed in conducting the audit and the timeframe within which the audit must be conducted; or
- Where it is recommended that an audit not be conducted, include recommendations, if any, in respect of proposed measures to mitigate the privacy or security risks or areas of non-compliance.

6.7. The RM&R Executive Committee shall, as soon as possible, but in any event no later than at its next meeting following receipt of the information and recommendations under paragraph 6.5:

- Review the information and approve recommendations received;
- Provide its decision and directions, in writing, to the Privacy and Security Working Group and to RM&R.

6.8. Where a HIC is suspected of posing the privacy or security risk or suspected non-compliance, RM&R will provide a copy of the Executive Committee decision and directions to the relevant HIC.

6.9. RM&R or the Privacy and Security Working Group (if an audit of RM&R is required) shall conduct an audit in accordance with the decision and directions of the RM&R Executive Committee.

6.10. RM&R or the HIC suspected of posing the privacy or security risks or suspected of non-compliance, as the case may be, shall comply with the decision and directions of the RM&R Executive Committee and shall remediate the privacy or security risks or areas of non-compliance or shall cooperate in any audit by the Privacy and Security Working Group, as the case may be.

6.11. RM&R or the Privacy and Security Working Group, as the case may be, shall, as soon as possible, but in any event no later than at its next meeting after completing the audit, report to the RM&R Executive Committee:

- The findings of the audit; and
- Its recommendations for remediating the privacy or security risks or areas of non-compliance identified, along with the timeframe for implementing the recommendations.

6.12. The RM&R Executive Committee shall, as soon as possible, but in any event no later than at its next meeting after receipt of the information and recommendations under paragraph 6.11:

- Review the information and the recommendations received; and
- Provide a written decision to approve the recommendations and provide directions in respect of the

timeframe for implementing the decision or provide written directions to RM&R or the Privacy and Security Working Group, as the case may be, to amend and re-submit the recommendations and to provide the timeframe within which they must be amended and re-submitted.

6.13. RM&R or the Privacy and Security Working Group, as the case may be, shall amend and re-submit the recommendations to the RM&R Executive Committee for approval in accordance with the timeframe set out in the written directions under paragraph 6.12 when directed to do so.

6.14. RM&R or the Privacy and Security Working Group, as the case may be, shall, upon the approval of the recommendations by the RM&R Executive Committee, provide a copy of the findings of the audit and the decision and directions of the RM&R Executive Committee to RM&R or the HIC, as the case may be, that posed the privacy or security risks or who is in non-compliance.

6.15. RM&R or the HIC that posed the privacy or security risks or who is in non-compliance, as the case may be, shall, upon receipt of the information under paragraph 6.14,:

- Implement the decision and directions within the timeframe approved by the RM&R Executive Committee;
- Provide written updates on the status of implementation of the decision and directions to RM&R or at each meeting of the Privacy and Security Working Group, as the case may be; and
- Provide a written attestation to RM&R or the Privacy and Security Working Group, as the case may be, that the decision and directions have been fully implemented, as soon as possible, but in any event no later than 30 days after implementation.

6.16. The Privacy and Security Working Group shall monitor compliance of RM&R or the HIC, as the case may be, with the implementation of the decision and directions of the RM&R Executive Committee and may require further documented evidence to demonstrate compliance. RM&R or the HIC, as the case may be, shall comply with any request from the Privacy and Security Working Group for documented evidence to demonstrate compliance.

7. Training

7.1. HICs and RM&R shall be able to demonstrate with evidence that their agents and Electronic Service Providers understand their relevant duties under PHIPA and the RM&R privacy and security policies, procedures, and practices, as described in the Privacy and Security Training policy.

7.2. HICs and RM&R shall provide evidence demonstrating that their agents and Electronic Service Providers are appropriately knowledgeable about their relevant duties under PHIPA and the RM&R privacy and security policies and procedures, as reasonably requested by HICs or RM&R (as the case may be).

7.3. Where gaps in knowledge exist, HICs and RM&R (as the case may be) shall provide evidence of a plan to remediate the gap and ensure all agents and Electronic Service Providers who have the ability to view PHI in the RM&R System understand their relevant duties under PHIPA and the RM&R privacy and security policies and procedures.

8. Non-Compliance

8.1. Non-compliance with PHIPA, the Data Sharing Agreement, as amended from time to time, and the policies, procedures and practices implemented in respect of the RM&R System will be identified, including through the following activities documented in this policy:

- PIAs and TRAs;
- Privacy and security operational self-attestations;
- Assurance of agents, Electronic Service Providers and third parties;
- Auditing and monitoring activities under paragraph 6.1; and
- Audits conducted by the Privacy and Security Committee.

References	**1. Legislative** • Personal Health Information Protection Act, 2004 **2. Other Policies** • Privacy Breach Management Policy and its associated procedures • Logging and Auditing Policy and its associated procedures • RM&R Information and Information Technology Policy (PS.Pol.101) and its associated procedures

Document Management	
Policy Number	PS.Pol.009
Version	1
Version History	V1 – Initial release
Effective Date	TBD
Last Review Date	September, 2014
Next Review Date	Annually or otherwise established by PSWG

RM&R Information Security Policy (PS.Pol.101)

Purpose

To define the behavioral requirements for all agents and Electronic Service Providers of RM&R, as well as all health information custodians (HICs), their agents and Electronic Service Providers who have access to the RM&R Solution. These requirements are intended to help protect the confidentiality, integrity, and availability of personal health information (PHI) stored in or processed by the RM&R Solution.

Scope

As RM&R is a web based system most of the Information Security controls and requirements are applied at the Electronic Service Provider level. Because of this implementation the number of requirements and policies for the RM&R HIC's have been reduced from what would otherwise be mandated.

This policy applies to:

- Agents and Electronic Service Providers of RM&R.
- All HICs, their agents and Electronic Service Providers who have access to the RM&R Solution.

Definitions

Information Technology

Any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

Integrated Environment

Refers to a Participating Organization that accesses the RM&R application via that organization's Hospital Information System, by way of a Single Sign-On protocol.

Non-integrated environment

Refers to a Participating Organization that accesses RM&R/ORBIT independent of any of that organization's Hospital Information Systems (see also integrated environment).

Policies and Procedures

1. Requirements for Health Information Custodians, their Agents and Electronic Service Providers

1.1. Information Security Contact

1.1.1. All organization will have a designated Information Security contact person. The contact information for this person will be provided to the RM&R program. This information will be kept up to date, and updates will be provided to the RM&R program within 24 hours of any changes being made.

1.2. Information Security Policy

1.2.1. All organizations will have a formal written information security policy and statement of information practices which is approved and signed off by management.

1.2.2. The following will apply to Information Security policies and procedures:

- The maintenance of information security policies and procedures are assigned to a group or individual;
- The information policies and procedures are part of day to day operations and practices;
- Policies and procedures are communicated to all agents (including employees, contractors, and volunteers etc.) of the organization who handle the PHI of the organization (i.e. through regular training).
- All policies and procedures are applied consistently within the organization.
- The organization designates an individual or individuals who are responsible for ensuring that the Information Security training is relevant and up-to-date based on RM&R policies and procedures, RM&R Agreements, legislative changes and regulatory findings;
- All Policies are reviewed annually;
- Security practice audits are performed on a regular interval, at least once a year, to ensure that day to day operations and practices reflect the information security practices; and
- If and when revised, changes to the Information Security policies and procedures are communicated in a timely manner to all Agents (including employees, contractors, and volunteers etc.) of the organization who handle PHI.

1.3. Information Security Breach Process

1.3.1. HICs must implement a formal written information security incident ("incident") management policy and process that covers all phases of the incident management process to deal with incidents related to the RM&R System:

- Identification/Triage
- Response
- Recovery, and
- Follow-up[15]

1.3.2. The processes described in the information security breach policy and procedure will mirror those required by RM&R's *Privacy Breach Management Policy (PS.Pol.06)*. The information security breach policy and procedures will add an Information Security contact/representative wherever a Privacy contact/representative is required by *the Privacy Breach Management policy (PS.Pol.06)*.

1.3.3. If at any point in the incident management process a HIC realizes that the incident has resulted in a privacy breach, then the incident must be handled in accordance with the *Privacy Breach Management Policy (PS.Pol.06)*.

1.3.4. Consistent with the *RM&R Privacy Breach Management Policy (PS.Pol.06)* RM&R will be notified of any security breach or potential security breach identified by a HIC or the Agents or Electronic Service Providers of that HIC that relates to RM&R. Notification to the RM&R program will occur as soon as possible, but in any event no later than the end of the next business day after the person at the HIC responsible for reporting the actual or suspected PHI Security Breach within RM&R has become aware the Breach, regardless of who it was caused by.

1.4. Information Security Training

1.4.1. All Employees and other agents with access to PHI in this organization are provided with training related to Information Security protection and Information Security best practices for safeguarding

[15] HICs may use alternative labels for each phase, or combine phases as long as all requirements of this policy are met.

that PHI.

1.4.2. This training:

- Takes place on a scheduled, timely and consistent basis;
- Includes a system for tracking and monitoring whether those who require training have completed it; and
- Is consistent with RM&R's Privacy and Security Training Policy (PS.Pol.07).

1.5. Usernames and passwords

1.5.1. All devices/computers used to store PHI are secured with a username and password to ensure security of the data and systems.

1.5.1.1. These usernames and passwords meet the following requirements:

- All users have a unique username;
- All users are not to share a username or password;
- Computer and PHI systems/programs/applications account passwords are changed every **90** days;
- All computer and systems account passwords are complex with a Capital, lower case letters, a number and special characters;
- All computer and systems account passwords are complex with a Capital, lower case letters, a number and special characters;
- All computers that access or host PHI are locked in secure areas off hours; and
- User accounts automatically lock after 10 failed attempts to log in and require calling an administrator to unlock.

1.6. Computers Networks and Systems

1.6.1. All computers, systems and networks are protected. All data at rest and in transit is protected. To meet this requirement the following is ensured.

1.6.1.1. All Mobile computers/systems and all removable storage is encrypted.

1.6.1.2. All organizations computer systems are behind a business class firewall, such as Sonicwall, Cisco or Checkpoint Safe@office, and not protected by a basic router, such as a Rogers or Bell internet access device.

1.6.1.3. All wireless access points, if applicable, are configured with WPA2 enterprise or WPA2 authentication and set with AES encryption.

1.6.1.4. All company computers are protected with Antivirus software that is kept up to date with latest patches and virus definitions

1.7. Integrated Sites Requirements

1.7.1. All Employees and other agents that are part of an integrated site are required to protect their username and password for the source EMR system to the same extent as set out in the requirements above.

1.7.2. All Integrated Sites Source EMR systems passwords meet or exceed the password requirements in section 1.5.

1.7.3. All Integrates sites that upload information directly from their EMR into RM&R ensure that their EMR data link to RM&R is secure and is working properly to ensure data is the same as the source and not intercepted when passed to the RM&R system.

Exceptions	Any exceptions to this Policy must be approved by the Executive Committee, who will authorize exceptions only where there is clear justification to do so and only to the minimum extent necessary to meet the justified need.

Enforcement	All instances of non-compliance will be reviewed by the Privacy and Security Working Group, which may recommend appropriate action to the Executive Committee.
References	**Legislative** • PHIPA, • O. Reg. 329/04, s. 6 **International Standards** • ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements. • ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management • ISO/IEC 27005: 2008 Information Technology – Security Techniques – Information Security Risk Management • ISO 27799:2008(E), Health Informatics – Information security management in health using ISO/IEC 27002 **Canada Health Infoway Reference** • Canada Health Infoway Electronic Health Record Privacy and Security Requirements (Version 1.1 Revised February 7, 2005)
Document Management	
Policy Number	PS.POL.101
Version	1.0
Version History	v1.0 – Initial draft
Effective Date	September, 2014
Last Review Date	
Next Review Date	Annually or otherwise established by the Privacy and Security Working Group.

6 Supporting Forms and Templates

Access and Correction Policy (PS.Pol.002) Forms

Letter Refusing a Request for Access in Whole or in Part

Instructions:

1. Use this template when communicating to the individual via RM&R that their Request for Access has been refused in whole or in part. Note: If the HIC is communicating directly with the individual, this template is not required.
2. Copy and paste the letter template onto the HIC's letterhead.
3. Complete the letter as required and create a PDF version of it.
4. Securely email the completed letter to the RM&R Program at referrals@UHN.ca. If the email is unsecure or you are unsure whether it is secure, email the RM&R Program for instructions on how to transmit a secure copy. RM&R will then provide this letter to the individual making the request on your behalf.
5. Please contact the RM&R Program if you have any questions about completing the letter template (by phone at 1-844-653-1240, or by email at referrals@UHN.ca).
6. The completed letter contains PHI. Any copies that you retain must be appropriately protected according to your HICs privacy and information security policies to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Letter Template:

Dear <<name of individual>>,

<<HIC name>> has received a Request for Access to health information from you. The Request for Access involves health information about <<individual name>>.

<<HIC name>> has decided to refuse this Request for Access <<in whole/in part>> as allowed by Personal Health Information Protection Act, s<<insert relevant section and paragraph number>> because <<provide reason that the access request is being denied as long as it does not expose the PHI being withheld>>.

If the request is being denied in part, briefly describe the nature of the records being withheld (e.g., mental health records, records from a particular encounter, all records) if it does not expose the PHI being withheld, and whether some records are still being released.

You have a right to make a complaint about not getting access to your information either by contacting our privacy department or Ontario's Information and Privacy Commissioner. The contact information is:

<<Name of Privacy Officer>>	Information and Privacy Commissioner of Ontario
<<HIC Name>>	2 Bloor Street East, Suite 1400
<<HIC Address>>	Toronto, Ontario M4W 1A8
<<HIC Phone>>	Telephone:(416) 326-3333 or (905) 326-3333
<<HIC Fax>>	Toll free:1 (800) 387-0073 (within Ontario)
	TDD/TTY:(416) 325-7539
	FAX:(416) 325-9195

Sincerely,

<<Name, Title>>

Letter Notifying of an Extension

Instructions:

1. Use this template when communicating to the individual via RM&R that the HIC requires an extension. Note: If the HIC is communicating directly with the individual, this template is not required.
2. Copy and paste the letter template onto the HIC's letterhead.
3. Complete the letter as required and create a PDF version of it.
4. Securely email the completed letter to the RM&R Program at referrals@UHN.ca. If the email is unsecure or you are unsure whether it is secure, email the RM&R Program for instructions on how to transmit a secure copy. RM&R will then provide this letter to the individual making the request on your behalf.
5. Please contact the RM&R Program if you have any questions about completing the letter template (by phone at 1-844-653-1240, or by email at referrals@UHN.ca).
6. The completed form contains PHI and must be appropriately protected according to your HICs privacy and information security policies to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Letter Template:

Dear <<name of individual>>,

<<HIC name>> has received a Request for Access to health information from you. The Request for Access involves health information about <<individual name>>.

<<HIC name>> has decided to refuse this Request for Access <<in whole/in part>> as allowed by Personal Health Information Protection Act, s<<insert relevant section and paragraph number>> because <<provide reason that the access request is being denied as long as it does not expose the PHI being withheld>>.

If the request is being denied in part, briefly describe the nature of the records being withheld (e.g., mental health records, records from a particular encounter, all records) if it does not expose the PHI being withheld, and whether some records are still being released.

You have a right to make a complaint about not getting access to your information either by contacting our privacy department or Ontario's Information and Privacy Commissioner. The contact information is:

<<Name of Privacy Officer>>	Information and Privacy Commissioner of Ontario
<<HIC Name>>	2 Bloor Street East, Suite 1400
<<HIC Address>>	Toronto, Ontario M4W 1A8
<<HIC Phone>>	Telephone:(416) 326-3333 or (905) 326-3333
<<HIC Fax>>	Toll free:1 (800) 387-0073 (within Ontario)
	TDD/TTY:(416) 325-7539
	FAX:(416) 325-9195

Sincerely,

<<Name, Title>>

Instructions to RM&R to Notify HICs of a Correction to PHI

Instructions:

1. Use this form when instructing RM&R to notify HICs that PHI they collected from the RM&R System has been corrected.
2. This form is available from the RM&R website (http://resourcematchingandreferral.com/).
3. Complete the form as required and create a PDF version of it.
4. Securely email the completed form to the RM&R Program at referrals@UHN.ca. If the email is unsecure or you are unsure whether it is secure, email the RM&R Program for instructions on how to transmit a secure copy. Note: you do not have to provide RM&R with information about the HICs that collected the PHI. RM&R will run an audit report to identify the relevant HICs.
5. Please contact the RM&R Program with any questions about completing the form (by phone at 1-844-653-1240, or by email at referrals@UHN.ca).
6. The completed form contains PHI. Any copies that you retain must be appropriately protected according to your privacy and information security policies to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Form:

Instructions to RM&R to Notify HICs of a Correction to PHI		
FORM TIPS: ● The form will open with the pointer in the start position. Begin typing your information. ● Use the **TAB** key on your keyboard to move to the next box. You can use **SHIFT + TAB** to move back. ● Click your left mouse button to fill in checkboxes.		
1. Contact Information (*To be completed by the individual submitting the instructions)*		
First Name *		Last Name *
Title * *(e.g., CPO)*	Business Telephone * *(include ext.)* ( )	Business Email *
Facility Name * *(e.g., XYZ Health System)*		Site/Hospital Name *(e.g., ABC Hospital)*
2. Patient Information		
Patient First Name *		Patient Last Name *
Date of Birth	Health Card Number	MRN*
3. Correction Made		
<<Describe the correction that was made, including the previous value, the new value, and the date associated with the original value. >>		
4. Special Instructions		
<<Include any special instructions that the Individual has given you related to the notification (e.g., only wanting the notification to go to particular providers). >>		

Consent Management Policy Forms

Consent Directive Intake and Communication Form

Instructions:

1. Use this form when providing RM&R with instructions on making, modifying, or deleting a Consent Directive.
2. This form is available on the RM&R website at http://resourcematchingandreferral.com.
3. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If the email is unsecure use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca. RM&R will use this information to make, modify, or delete the Consent Directive in the RM&R Solution, and notify you once the Consent Directive has been made, modified, or deleted.
4. Please Contact the RM&R Service Desk with any questions about completing the form (by phone at 1-844-653-1240, or by email at referrals@UHN.ca).
5. The completed form contains PHI. Any copies that you retain must be appropriately protected according to your privacy and information security policies to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Consent Directive Intake and Communication Form

Pre-procedure		
Date of initial contact with patient *		Date lockbox information and form sent to patient *
Date written request received from patient *		
FORM TIPS: ● The form will open with the pointer in the start position. Begin typing your information. ● Use the **TAB** key on your keyboard to move to the next box. You can use **SHIFT + TAB** to move back. ● Click your left mouse button to fill in checkboxes.		
1. HIC Agent Contact Information (*To be completed by the individual submitting this report)*		
First Name *		Last Name *
Title * *(e.g., CPO)*	Business Telephone * *(include ext.)* ( )	Business Email *
Facility Name * *(e.g., XYZ Health System)*		Site/Hospital Name *(e.g., ABC Hospital)*
Date of Request * *(yyyy-mm-dd)*		
2. Patient Contact Information (*To be completed by the individual submitting this report)*		
Patient Request: ☐ *If selected, enter patient information below*		SDM Request: ☐ *If selected, enter both patient and SDM information Below*
Legal First Name *	Middle Initial(s)	Legal Last Name *
Date of Birth	Health Card Number *	Hospital MRN
What is the best way to contact you/the patient?		Can a detailed voicemail/message be left? ☐ Yes ☐ No Details:
Can we send you a letter? ☐ Yes ☐ No Details:		
Patient's Contact Information *(telephone number, email and address)*		
3. Consent Directive Request Details (*Provide information about the individual's request)*		
Consent Directive Details (*Describe the consent directive requested by the individual, including if the request is to modify or remove the consent directive)*		

4. Assistance Request Details (*Provide information on your request for assistance)*
Request Change (choose one) ☐ Create a consent directive ☐ Modify an existing consent directive ☐ Remove an existing consent directive
Additional Details

Consent Directive Management Checklist

Instructions:

1. Use this form as needed to help track management of consent directives.
2. This form is available on the RM&R website at http://resourcematchingandreferral.com.
3. Please Contact the RM&R Service Desk with any questions about completing the form (by phone at 1-844-653-1240, or by email at referrals@UHN.ca).

Consent Directive Management Checklist

File Closed		☐	Date Closed
Action		✓	**Date Completed**
1.	Clarify Request • External disclosure? • Internal use? • Particular external recipient? • Particular internal user? • MDs/clinics visited?	☐	
2.	Create: a. Cover sheet for paper files b. Memo for MDs/clinics	☐ ☐	
3.	Notify ROI teams ***[Update List as Applicable to Organization]*** a. Send cover sheet for paper file to Health Records b. Notify Transcription Services (specify MD, where appropriate)	☐ ☐	
4.	Notify MDs/clinics ***[Update List as Applicable to Organization]*** a. Send memo & cover sheet for paper records b. Inform whole record is locked c. Inform individual to be locked out & determine if provides urgent care	☐	
5.	Notify HINP Management Office(s) ***[Update List as Applicable to Organization]*** a. RM&R b. cGTA c. Other	☐ ☐ ☐	
6.	Implement electronic locks (as appropriate) ***[Update List as Applicable to Organization]*** a. Lock whole record b. Add individual to locked list c. Insert detailed instructions d. Notify applicable system user of patient instruction and additional auditing frequency and focus.	☐ ☐ ☐ ☐	
7.	Place instruction re. internal use on affected records: a. Send addendum for notes to Transcription (cc. Health Records) b. Modify paper record cover sheet (& resend to MDs / Health Rec) c. Send Privacy Caution form for scanning	☐ ☐ ☐	
8.	Write and send response letter to patient	☐	

Consent Directive Application Letter Sample Template

Instructions:

1. Use this letter template when confirming to an individual that their consent directive instruction has been applied in RM&R.
2. This template is available on the RM&R website at http://resourcematchingandreferral.com.
3. Please Contact the RM&R Service Desk with any questions about completing the template.
4. The completed template contains PHI. Any copies that you retain must be appropriately protected according to your privacy and information security policies to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Consent Directive Application Letter Sample Template

CONFIDENTIAL – HIGH SENSITIVITY
FILE: #
[Date]

[Patient Name]
[Patient Address]

Re: Patient Consent Directive Application Notification

This letter is to acknowledge and respond to your consent directive instruction received by our office on [Date directive received].

As per your instruction, we have restricted your electronic referral record in the Resource Matching and Referral (RM&R) system. In future, under most circumstances, your express consent will be requested before your electronic referral record in RM&R is reviewed or updated. In addition, you will receive notification whenever anybody looks at this record.

If you wish to reinstate your consent, or if you have any questions or concerns, you may contact the [Hospital/HSP Name] Privacy Office at [Privacy Office contact information].

For more information about the RM&R system please visit the RM&R web site at www.resourcematchingandreferral.com

Sincerely,

[Name, Title]

Consent Directive Override Letter Sample Template

Instructions:

5. Use this letter template when notifying an individual that the information in RM&R that is restricted in response to their consent directive has been overridden.
6. This template is available on the RM&R website at http://resourcematchingandreferral.com.
7. Please Contact the RM&R Service Desk with any questions about completing the template (by phone at 1-844-653-1240, or by email at referrals@UHN.ca).
8. The completed template contains PHI. Any copies that you retain must be appropriately protected according to your privacy and information security policies to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Consent Directive Override Letter Sample Template

CONFIDENTIAL – HIGH SENSITIVITY
FILE: #
DATE

PATIENT NAME
ADDRESS

Re: Patient Consent Directive Override Notification - Health Care Provider Access to Resource Matching and Referral (RM&R) Health Information

---

The purpose of this letter is to inform you that access to your complete RM&R referral history was granted during your visit to a health care provider. The disclosure of your referral information was made with either your consent or the consent of your substitute decision-maker, or to mitigate a risk of serious harm. A summary of this access is provided below:

Date of Access	Reason for Access	Consented by (if applicable)

This temporary reinstatement of consent does not provide the right for [*Hospital/HSP Name*] to disclose your referral history information in the RM&R system to health care providers on an on-going basis.

If you wish to reinstate your consent on an ongoing basis, or if you have any questions, you may contact the [*Hospital/HSP Name*] Privacy Office at [*Privacy Office contact information*].

For more information about the RM&R system please visit the RM&R web site at www.resourcematchingandreferral.com

Sincerely,

[*Name, Title*]

Attachment

Consent Directive Management Log

Instructions:

9. Use this form when logging consent directives. Complete the template with as much information as known at time of reporting, **excluding any Personal Health Information (PHI)**.
10. This form is available on the RM&R website at http://resourcematchingandreferral.com/.
11. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If the email is unsecure use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.
12. Please contact the RM&R Service Desk (by phone at 1-844-653-1240, or by email at referrals@UHN.ca) with any questions about completing the form.

Consent Directive Management Log Sample

Patient Last Name	Patient First Name	MRN	Consent Directive Details	Reason for Consent Directive	Date of Receipt of Consent Directive	Related Electronic System	Date of notification to HINP	Date Consent Directive Applied	Restriction Type	Person Making the Change	Date of Notification to Individual that Consent Directive Has Been Applied

Privacy Breach Management Policy

Privacy Breach Report

Instructions:

1. Use this form when first reporting a breach to RM&R. Complete the template with as much information as known at time of reporting, **excluding any Personal Health Information (PHI)**.
2. This form is available on the RM&R website at http://resourcematchingandreferral.com/.
3. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If the email is unsecure use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.
4. Please contact the RM&R Service Desk (by phone at 1-844-653-1240, or by email at referrals@UHN.ca) with any questions about completing the form.

Privacy Breach Report Form:

Privacy Breach Report		
FORM TIPS: ● The form will open with the pointer in the start position. Begin typing your information. ● Use the **TAB** key on your keyboard to move to the next box. You can use **SHIFT + TAB** to move back. ● Click your left mouse button to fill in checkboxes.		
1. Contact Information (for reporter)		
First Name *		Last Name *
Title * *(e.g., CPO)*	Business Telephone * *(include ext.)* ( )	Business Email *
Facility Name * *(e.g., XYZ Health System)*		Site/Hospital Name *(e.g., ABC Hospital)*
2. Breach Information		
Time and date breach occurred (or when it was identified if occurrence unknown) *		
Organization responsible for the breach (if known) *		Person responsible for the breach (if relevant and known) *
HICs impacted by the breach (if known) *		
Description of the nature and scope of the breach *		
Description of the PHI that was involved in the breach*		
3. Breach Containment		
Description of any containment measures taken *		
Is support required from other HICs or RM&R to complete containment? If so, please provide a brief description *		
4. Breach Reporting		
Identify which if any of the following has been notified about the breach * *Group* — *Date of Notification* ☐ Impacted HICs ☐ Affected Individuals ☐ IPC / Ontario ☐ Law enforcement ☐ Regulatory College ☐ Other, explain		

Privacy Breach Investigation Report

Instructions:

1. Use this form to document the results of a breach investigation, **excluding any Personal Health Information (PHI)**.
2. This form is available on the RM&R website at http://resourcematchingandreferral.com/.
3. Complete the form as required and create a PDF version of it.
4. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If the email is unsecure use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.
5. RM&R will provide you with information about how and to whom you need to send the form during the course of the investigation. Please contact the RM&R Service Desk (by phone at 1-844-653-1240, or by email at referrals@UHN.ca) with any questions about completing the form.

Form:

Privacy Breach Investigation Report		
FORM TIPS: ● The form will open with the pointer in the start position. Begin typing your information. ● Use the **TAB** key on your keyboard to move to the next box. You can use **SHIFT + TAB** to move back. ● Click your left mouse button to fill in checkboxes.		
1. Investigator Information		
First Name *		Last Name *
Title * *(e.g., CPO)*	Business Telephone * *(include ext.)* ( )	Business Email *
Facility Name * *(e.g., XYZ Health System)*		Site/Hospital Name *(e.g., ABC Hospital)*
2. Breach Information		
Time and date breach occurred (or when it was identified if occurrence unknown) *		
Organization responsible for the breach (if known) *		Person responsible for the breach (if relevant and known) *
HICs impacted by the breach (if known) *		
Description of the nature and scope of the breach, without including any PHI or individual identifiers*		
Description of the cause of the breach *		
3. Breach Containment		
Description of any containment measures that were taken *		
4. Breach Reporting		
Identify which of the following was notified about the breach * *Group* *Date of Notification* ☐ Impacted HICs ☐ Affected Individuals ☐ IPC / Ontario ☐ Law enforcement ☐ Regulatory College ☐ Other, explain		
4. Investigation Approach		

Briefly describe the scope and nature of the investigation *
Briefly describe the steps followed in the investigation *
5. Remediation
Describe in full the steps that have been taken to remediate the breach *
Describe in full the recommended steps to further remediate the breach or prevent future instances of a similar breach. Provide recommendations regarding who would be most appropriate to carry out the steps and the timelines for doing so. *

Update on Status of Remediation Activities

Instructions:

1. Use this form when providing updates to RM&R on the status of remediation activities.
2. This form is available on the RM&R website at http://resourcematchingandreferral.com/.
3. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If the email is unsecure use the “Patient Information” setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.

Form:

1. Site Information		
First Name *		Last Name *
Title * *(e.g., CPO)*	Business Telephone * *(include ext.)* ( )	Business Email *
Facility Name * *(e.g., XYZ Health System)*		Site/Hospital Name *(e.g., ABC Hospital)*

2. Status Report

Ref. No.	Remediation Activity	Status (Open/Completed)	Date of Anticipated Completion or Completion	Comments of how the activity will be met
	<<Examples appear below>>			
1	Remind agents of appropriate PHI handling techniques	Completed	10/23/2013	Emailed staff members on how to appropriately transmit PHI
2	Inform electronic service providers of obligation to securely transmit PHI	Open	11/15/2013	Meeting scheduled with HIS provider to discuss transmission mechanisms

Assurance Policy

Privacy and Security Readiness Assessments

Instructions:

1. The readiness assessments are to be completed by a site prior to joining RM&R.
2. The readiness assessments are categorized according to the whether the site plans to be an integrated or non-integrated site. Choose the privacy and the security assessments appropriate for your organization. You must complete one privacy and one security assessment.
3. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If email is unsecured, use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.
4. Please contact the RM&R Service Desk (by phone at 1-844-653-1240, or by email at referrals@UHN.ca) with any questions about completing the form.

RM&R Readiness Assessment

Privacy Assertion Survey Template

Instructions:

1. The Privacy Assertion Surveys are to be completed by a site each year after joining RM&R.
2. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If email is unsecured, use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.
3. Please contact the RM&R Service Desk (by phone at 1-844-653-1240, or by email at referrals@UHN.ca) with any questions about completing the form.

Privacy Assertion Survey

A tool for asserting the Privacy Program of RM&R Participating Sites is compliant with PHIPA and the RM&R Data Sharing Agreement.

Date: August 6, 2013

Version 6.0

RM&R Privacy Assertion Survey

A tool for asserting that the Privacy Program of RM&R Participating Sites is compliant with PHIPA and the RM&R Data Sharing Agreement

The Privacy Assertion Survey Tool (the Survey Tool) is designed to assist those health information custodians (HICs) who are providing personal health information (PHI) to other HICs through RM&R, as well as those subsequently accessing PHI from RM&R, in assessing and asserting the level of maturity of their privacy practices. It is a key component of a comprehensive 'trust model' to ensure the ongoing privacy, confidentiality and security of PHI is adequately protected. The information provided in the Survey Tool will enable HICs to assess and communicate the stage of development of their privacy program from a quality assurance/privacy assurance perspective. All italicized words used in this document have the same meanings as those set out in the Personal Health Information Protection Act, 2004, Sch. A (PHIPA) and its regulations, as amended from time to time.

HIC's will assess their practices based on the following criteria:

Organizational Privacy Management

- Privacy Structure and Organization
- Privacy Policies and Procedures
- Privacy Training and Awareness

When finalized, the survey will assert to the RM&R program the level of maturity of the HIC's privacy program, and will include requirements for the following information: (i) the actions that the organization will undertake and implement to address any gaps in privacy procedure, policy, training etc. and (ii) a timeframe the remediation actions will be completed. You should also provide an explanation of why a particular question is "N/A".

The Survey Tool includes a “Comments” column associated with each question. The Comments are provided to assist the reader by referencing a legislative authority, a process or procedure agreed to through the RM&R Data Sharing Agreement and/or generally accepted industry practices that support the action being “tapped” by each question. The comments may also provide examples of situations that could occur and risks to which the organization may be exposed if compliance activities are not followed. The Comments also provide links and references to resources that may be of assistance in implementing any required remediation efforts. Note: this information is provided for assistance only and RM&R assumes no responsibility for the accuracy or currency of the information. Prior to relying on this information, organizations are responsible for independently confirming its accuracy and currency.

Organization Name: **Assertion Contact:** **Date Completed:**

Instructions: Please note, Site Privacy Officers (or delegates) are to indicate "Y" or "N" for those questions/requirements met or not met, respectively, include planned actions to eliminate or offset the risk or compliance and the target finish dates. The completed document is to be submitted to the RM&R program [Attn: NAME] by [DATE].

	Assertion	**Status**	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	**Comments**
1	This organization has a designated privacy contact person that has accountability for the privacy program, as it relates to the RM&R system.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	Where an organization is a HIC, the organization must designate an individual as a privacy contact person, under PHIPA, s.15. That person is authorized to perform several key duties in relation to privacy protection, as detailed in s.15. Having a designated individual within the organization who is responsible for privacy matters is a component of 'accountability'.
	a) Identify this individual	Name: Title:			

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
		Email: Phone:			
	b) Do you have an alternate privacy contact? If yes, identify this individual.	Name: _____ Title: _____ Email: _____ Phone: _____			
2	The organization has privacy policies and procedures, both generally for the organization and specifically for the PHI in RM&R, that include the following:				
	a) PHI is collected, used and disclosed in accordance with PHIPA, the RM&R Data Sharing Agreement and other applicable legislation.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	Relevant requirements are set out in ss. 29, 30, 36, 37, 38-48 and 50 of PHIPA. Sections 1 through 5 of the TC-LHIN Resource Matching & Referral Application Data Sharing Agreement (Appendix 1) set out the stipulations about collecting, using, and disclosing PHI through the

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
					RM&R system.
	b) Individual consent is obtained appropriately, where consent is required.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	PHIPA, s.29 sets out when consent is required. When a HIC must obtain consent, the type of consent that must be obtained, and the requirements for obtaining valid consent, are set out in s.18. Sections 2.3 and 2.4 of the TC-LHIN Resource Matching & Referral Application Data Sharing Agreement (Appendix 1) sets out the provisions for consent.
	c) Ensure a written public statement about the organization's information practices includes information about PHI in shared systems, including RM&R, and is readily available.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	PHIPA, s.16 sets out the requirements. TC-LHIN Resource Matching & Referral Application Data Sharing Agreement (Appendix 1), s. 5.4 sets out the requirement.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
	d) To respond to requests by individuals for access to and correction of records of their own PHI, subject to certain exceptions.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	PHIPA, ss.52-55 sets out how a HIC must manage requests from individuals for access to and correction of records of their PHI. It is important for a HIC to develop and implement a process to manage access and correction requests to ensure that, among other matters, it can meet the required timelines for responding to such requests. Access and correction requirements have been stipulated in the TC-LHIN Resource Matching & Referral Application Data Sharing Agreement, s. 2.6 (Appendix 1).
	e) For the management of privacy breaches, including the notification of individuals when PHI has been stolen, lost or accessed by unauthorized persons.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20,	<u>Privacy Breaches</u> HICs must notify individuals in the event of a privacy breach [s.12(2)]. Similarly, agents of HICs have an obligation to notify the HIC if PHI managed by the agent on behalf of the HIC is subject to a breach. In addition, a HINP is required to notify every applicable HIC in the event of a breach. Accordingly, HICs should have in place policies and procedures to deal with

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
				2014	'internal' breaches as well as 'external' breaches. For the latter case, a HIC should consider including these requirements in any services agreements with their agents and their HINPs. See the following publications of the IPC for assistance on developing a Privacy Breach Protocol: *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector* at: http://www.ipc.on.ca/images/Resources/hprivbreach-e.pdf ; and *Breach Notification Assessment Tool* at: http://www.ipc.on.ca/images/Resources/ipc-bc-breach-e.pdf TC-LHIN Resource Matching & Referral Application Data Sharing Agreement, s. 5.5 (Appendix 1) outlines the requirements.
	f) Privacy audits related to users' access to RM&R are conducted based on RM&R audit logs.	☐ Fully implemented ☐ Partially implemented ☐ Planned		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014	Audits are an essential tool for ensuring privacy compliance. TC-LHIN Resource Matching & Referral Application

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
		☐ Undefined		☐ After Sep. 20, 2014	Data Sharing Agreement, s. 3.3 (Appendix 1) outlines the requirements.
	g) confidentiality agreements are entered into with agents who will have access to RM&R.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	These agreements help ensure that agents are aware of their duties under PHIPA and comply with those duties. TC-LHIN Resource Matching & Referral Application Data Sharing Agreement, s. 3.2 (Appendix 1) outlines the requirements.
	h) Receiving, investigating and responding to privacy complaints and inquiries.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	A documented process for handling complaints and inquiries helps ensure responsiveness to patients and clients and facilitates improving the quality of privacy protection. TC-LHIN Resource Matching & Referral Application Data Sharing Agreement, s. 2.7 (Appendix 1) outlines

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
					the requirements.
	i) Managing and applying patient consent directives, including the withdrawal of consent.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	PHIPA, s.19, sets out the patient right to withdraw or restrict consent for a HIC to collect, use or disclose their PHI. TC-LHIN Resource Matching & Referral Application Data Sharing Agreement, s. 2.4 (Appendix 1) outlines the requirements.
	j) The list of RM&R Authorized Staff is kept current and is maintained according to the RM&R Policy on Site End User Account Management (see Appendix 2).	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	TC-LHIN Resource Matching & Referral Application Data Sharing Agreement, s. 3.2 (Appendix 1) outlines the requirements.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
3	The privacy policies and procedures relating to the RM&R system, described in question 2 above,:				
	a) Are communicated to all agents (including employees, contractors, and volunteers etc.) of the organization who handle the PHI in RM&R (i.e. through regular training).	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	To improve the effectiveness of their privacy policies and procedures, a HIC should consider adopting practices to address the following: • employees and other agents having access to PHI to which the policies and procedures relate understand their obligations and the consequences if they are not followed • as part of their orientation, new employees and other agents are made aware of and trained on the organization's privacy policies and procedures Privacy breaches may occur inadvertently because employees and other agents are not aware of the applicable policies and/or do not understand their responsibilities. Requirements for training of Authorised Staff are stipulated in the RM&R Data Sharing Agreement (Appendix 1), s.1.7.
	b) Are regularly reviewed and revised if required.	☐ Fully implemented		Finish by:	There are many reasons why privacy policies and procedures should be reviewed on a regular basis.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
		☐ Partially implemented ☐ Planned ☐ Undefined		☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	Applicable laws and regulations may be amended or new laws introduced. Orders may be issued by the Information and Privacy Commissioner of Ontario interpreting a provision of PHIPA; e.g. requiring the encryption of PHI held on mobile devices. The organization may change its business practices, implement new programs and/or restructure its business departments; and newly emerging technologies may present new privacy risks. HICs should consider conducting these reviews on an annual basis.
	c) If and when revised, are communicated in a timely manner to all Agents (including employees, contractors, and volunteers etc.) of the organization who handle the PHI in RM&R.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	Communication of requirements with Authorised Staff is stipulated in the RM&R Data Sharing Agreement (Appendix 1), s.1.7.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
	d) Are subject to an internal review and development process with appropriate sign-off by senior management.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	From a governance and accountability perspective, organizations may wish to consider implementing a formal process for the development and amendment of all policies and procedures, including those related to management of PHI. This helps ensure that all agents of the organization understand who may initiate the process, what internal stakeholders should be consulted and the appropriate level of management sign-off. It also ensures that policies have a consistent 'look and feel', which may make them easier for agents to understand.
	e) Are assigned ownership and accountability to an individual or group of individuals within the organization.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	"Ownership and accountability" for a policy or procedure entails responsibility for the creation and updating of the policy or procedure, as well as responsibility for communication and implementation of the policy or procedure throughout the organization, and for assessing and auditing compliance. Compliance enforcement is normally a joint responsibility of line management, the organization's privacy office and its human resources department.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
	f) Are applied consistently within the organization.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	An organization may have developed and implemented privacy policies and procedures but not be aware of how or if they are being applied consistently. In order to assess compliance, the organization should consider undertaking a regular internal review or audit of the application of their privacy policies and procedures. This may minimize the risk that, for example, certain employees do not adequately understand how to apply what they have learned in their privacy training to the business processes involving handling of PHI for which they are responsible.
4	Employees and other agents with access to RM&R PHI in this organization are provided with training that:				
	a) Relates to privacy protection and privacy best practices for safeguarding that PHI.	☐ Fully implemented ☐ Partially implemented ☐ Planned		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014	Privacy training and communication is a cornerstone for facilitating the HIC's compliance with PHIPA. Employees and other agents of the HIC must know and understand privacy requirements in order to meet them.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
		☐ Undefined		☐ After Sep. 20, 2014	Because a HIC is responsible for PHI under its custody or control, it is prudent for the HIC to provide training not only to its employees, but also to its other agents that will have access to PHI. Ensuring that all agents of a HIC are appropriately informed of their duties under PHIPA is one of the authorized activities of a HIC's designated contact person [s.15(3)b)]. HICs are encouraged to employ regular training and communication of privacy policies and procedures. This is of particular importance for new agents, and those agents returning from a leave.
	b) Provides for specific training for selected employees or other agents depending on their roles and responsibilities.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	While an organization should provide general privacy training to all its agents, some agents will require training that is more specialized. As examples, these may be agents who handle PHI on a regular basis as part of their daily responsibilities, deal with extremely sensitive information and/or have specific responsibilities for data analysis and disclosure, or fulfilling requests for access to and correction of records of PHI.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
	c) Takes place on a scheduled, timely and consistent basis.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	
	d) Includes a system for tracking and monitoring whether those who require training have completed it.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	Organizations should consider how to ensure that all those who work with PHI have met their privacy training requirements. One tactic is to have managers track their direct reports' attendance at privacy training sessions.

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
	e) Designates an individual or individuals who are responsible for ensuring that the privacy training is relevant and up-to-date based on policy, RM&R Data Sharing Agreement, and legislative changes and regulatory findings.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	The content of privacy training should be assessed on an ongoing basis to ensure that it includes current developments in legislative requirements, best practices, Orders or findings of the Information and Privacy Commissioner of Ontario, and emerging technologies.
	f) Provides for 'remedial' training in the event that a privacy breach occurs.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Dec. 20, 2013 ☐ Mar. 20, 2014 ☐ Sep. 20, 2014 ☐ After Sep. 20, 2014	If, for example, an organization experiences a privacy breach because of an agent's access to PHI to which they are not entitled, the organization should require that the agent and any other agents deemed appropriate receive remedial training which focuses on the policies, procedures etc. that have not been followed. See for example, Order HO-010 in which the Information and Privacy Commissioner ordered the organization to conduct privacy retraining for the employee and all other agents working in the department of the individual who inappropriately accessed PHI. At:

	Assertion	Status	Actions Planned to eliminate or offset risk of 'partially implemented', 'planned' or 'undefined' items	Target Finish Date for Actions	Comments
					http://www.ipc.on.ca/images/Findings/ho-010.pdf

Information Security Assertion Survey Template

Instructions:

1. The Information Security Assertion Surveys are to be completed by a site each year after joining RM&R.
2. Securely email the completed form to the RM&R Service Desk at referrals@uhn.ca. If email is unsecured, use the "Patient Information" setting on the UHN file portal - https://fileportal.uhn.ca/Upload.aspx and direct the report to referrals@UHN.ca.
3. Please contact the RM&R Service Desk (by phone at 1-844-653-1240, or by email at referrals@UHN.ca) with any questions about completing the form.

Information Security Assertion Survey

A tool for asserting the Information Security Program of RM&R Participating Sites is compliant with PHIPA and the RM&R Data Sharing Agreement.

Date: May 2014

Version 3.0

RM&R Information Security Assertion Survey

A tool for asserting that the Information Security Program of RM&R Participating Sites is compliant with PHIPA and the RM&R Data Sharing Agreement

The Information Security Assertion Survey Tool (the Survey Tool) is designed to assist those health information custodians (HICs) who are providing personal health information (PHI) to other HICs through RM&R, as well as those subsequently accessing PHI from RM&R, in assessing and asserting the level of maturity of their Information Security practices. It is a key component of a comprehensive 'trust model' to ensure the ongoing Information Security, confidentiality and security of PHI. The information provided in the Survey Tool will enable HICs to assess and communicate the stage of development of their Information Security program from a quality assurance/Information Security assurance perspective. All italicized words used in this document have the same meanings as those set out in the Personal Health Information Protection Act, 2004, Sch. A (PHIPA) and its regulations, as amended from time to time.

HIC's will assess their practices based on the following criteria:

Organizational Information Security Management

- Information Security Structure and Organization
- Information Security Policies and Procedures
- Information Security Training and Awareness

When finalized, the survey will assert to the RM&R program the level of maturity of the HIC's Information Security program, and will include requirements for the following information: (i) the actions that the organization will undertake and implement to address any gaps in Information Security procedure, policy, training etc., and (ii) a timeframe the remediation actions will be completed. Note: When completing the survey, please provide an explanation of why a particular question is "N/A".

The Survey Tool includes a “Comments” column associated with each question. The Comments are provided to assist the reader by referencing a legislative authority, a process or procedure agreed to through the RM&R Data Sharing Agreement and/or generally accepted industry practices that support the action being “tapped” by each question. The comments may provide examples of situations that could occur and risks to which the organization may be exposed if compliance activities are not be followed. The Comments also provide links and references to resources that may be of assistance in implementing any required remediation efforts. Note: this information is provided for assistance only and RM&R assumes no responsibility for the accuracy or currency of the information. Prior to relying on this information, organizations are responsible for independently confirming its accuracy and currency.

Organization Name: **Assertion Contact:** **Date Completed:**

Instructions: Please note, Site Information Security Officers (or delegates) are to indicate "Y" or "N" for those questions/requirements met or not met, respectively, include planned actions to eliminate or offset the risk or compliance and the target finish dates. The completed document is to be submitted to the RM&R program [Attn: NAME] by [DATE].

	Assertion	Status	Actions Planned to eliminate or offset risk of 'planned' or 'undefined' items	Target Finish Date for Actions (Choose Earliest Option)	Comments
1	This organization has a designated Information Security contact person.	☐ Fully implemented ☐ Partially implemented ☐ Planned ☐ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Having a designated individual within the organization who is responsible for Information Security matters is a component of 'accountability'. This may be shared with another role.
	a) Identify this individual	Name: Title: Email: Phone:			

2	This organization has a formal written Information Security policy and statement of information practices, both of which have been approved by the organization's management.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	PHIPA requires HICs to have publicly available a written public statement that includes a general description of their information practices [s. 16(1)(a)]. Doing this fosters transparency with respect to how the organization manages PHI collected, used, disclosed and retained. s. 10(1) and s. 10(2) of PHIPA, together with the definition of "information practices" in s. 2, spell out HICs' obligations in relation to information practices.

3	This organization has developed detailed procedures for implementing its Information Security policy in its day-to-day operations.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	The development of policies and procedures for an organization's different operations is, in effect, a means by which the organization can provide its baseline for compliance with its obligation under s. 10(2) of PHIPA to "comply with its information practices". In addition, policies and procedures are a mechanism for a HIC to comply with its security requirements (which include administrative safeguards) as per ss. 12(1) and 13(1) of PHIPA.
4	The Information Security policies or procedures that were identified in response to questions 2 and 3 ensure, both generally for the organization and specifically for the PHI in RM&R, the following:				
	a) Information Security audits are conducted.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Audits are an essential tool for ensuring Information Security compliance.
5	The Information Security policies and procedures:				

	a) Are communicated to all agents (including employees, contractors, and volunteers etc.) of the organization who handle the PHI of the organization (i.e. through regular training).	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	To improve the effectiveness of their Information Security policies and procedures, a HIC should consider adopting practices to address the following: 1. employees and other agents having access to PHI to which the policies and procedures relate understand their obligations and the consequences if they are not followed 2. as part of their orientation, new employees and other agents are made aware of and trained on the organization's Information Security policies and procedures 3. Information Security breaches may occur inadvertently because employees and other agents are not aware of the applicable policies and/or do not understand their responsibilities.

	b) Are subject to an internal review and development process with appropriate sign-off by senior management.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	From a governance and accountability perspective, organizations may wish to consider implementing a formal process for the development and amendment of all policies and procedures, including those related to management of PHI. This helps ensure that all agents of the organization understand who may initiate the process, what internal stakeholders should be consulted and the appropriate level of management sign-off. It also ensures that policies have a consistent 'look and feel', which may make them easier for agents to understand.
	c) If and when revised, are communicated in a timely manner to all Agents (including employees, contractors, and volunteers etc.) of the organization who handle the PHI of the organization.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	

	d) Are assigned ownership and accountability to an individual or group of individuals within the organization.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	"Ownership and Accountability" for a policy or procedure entails responsibility for the creation and updating of the policy or procedure, as well as responsibility for communication and implementation of the policy or procedure throughout the organization, and for assessing and auditing compliance. Compliance enforcement is normally a joint responsibility of line management, the organization's Information Security office and its human resources department.

	e) Are applied consistently within the organization.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	An organization may have developed and implemented Information Security policies and procedures but not be aware of how or if they are being applied consistently. In order to assess compliance, the organization should consider undertaking a regular internal review or audit of the application of their Information Security policies and procedures. This may minimize the risk that, for example, certain employees do not adequately understand how to apply what they have learned in their Information Security training to the business processes involving handling of PHI for which they are responsible.

	f) Employees and other agents with access to PHI in this organization are provided with training related to Information Security protection and Information Security best practices for safeguarding that PHI.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Information Security training and communication is a cornerstone for facilitating the HIC's compliance with PHIPA. Employees and other agents of the HIC must know and understand Information Security requirements in order to meet them. Because a HIC is responsible for PHI under its custody or control, it is prudent for the HIC to provide training not only to its employees, but also to its other agents that will have access to PHI. Ensuring that all agents of a HIC are appropriately informed of their duties under PHIPA is one of the authorized activities of a HIC's designated contact person [s.15(3)b)]. HICs are encouraged to employ regular training and communication of Information Security policies and procedures. This is of particular importance for new agents, and those agents returning from a leave.

6	This organization's Information Security training:				
	a) Provides for specific training for selected employees or other agents depending on their roles and responsibilities.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	While an organization should provide general Information Security training to all its agents, some agents will require training that is more specialized. As examples, these may be agents who handle PHI on a regular basis as part of their daily responsibilities, deal with extremely sensitive information and/or have specific responsibilities for data analysis and disclosure, or fulfilling requests for access to and correction of records of PHI.
	b) Takes place on a scheduled, timely and consistent basis.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	

	c) Includes a system for tracking and monitoring whether those who require training have completed it.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Organizations should consider how to ensure that all those who work with PHI have met their Information Security training requirements. One tactic is to have managers track their direct reports' attendance at Information Security training sessions.
	d) Designates an individual or individuals who is responsible for ensuring that the Information Security training is relevant and up-to-date based on legislative changes and regulatory findings.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	The content of Information Security training should be assessed on an ongoing basis to ensure that it includes current developments in legislative requirements, best practices, Orders or findings of the Information and Information Security Commissioner of Ontario, and emerging technologies.
7	Systems access security				

	a) All computers and systems, that host or access PHI, are secured with a Username and password.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Systems should be secured to prevent unauthorized access.
	b) All account passwords are changed every 90 days.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Passwords should be changed regularly.
	c) All computer and systems account passwords are required to be complex with a Capital, lower case letters, a number and special characters.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Passwords should be complex in nature to prevent password guessing.

	d) All users are instructed to not share passwords and protect their login information.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	User account information should be kept secret and secure.
	e) All computers that access or host PHI are locked in secure areas off hours.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	Systems should be protected during off-hours.
	f) User accounts automatically lock after 10 failed attempts to log in and require calling an administrator to unlock.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	User accounts are protected from password guessing/hacking attempts.

	g) All Mobile computers/systems and all removable storage is encrypted.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	In accordance with Health Order 008 all removable and portable media is to be encrypted to protect PHI.
	h) All user systems are behind a business class firewall, such as Sonicwall, Cisco or Checkpoint Safe@office, and not protected by a basic router, such as a Rogers or Bell internet access device.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	This is to ensure that outside users cannot access internal computers.

	i) All wireless access points are configured with WPA2 enterprise authentication and set with AES encryption.	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	This is to prevent access to the internal network from a malicious user who is within the wireless network range.
	j) All company computers are protected with Antivirus software that is kept up to date with latest patches and virus definitions	□ Fully implemented □ Partially implemented □ Planned □ Undefined		Finish by: ☐ Sept. 30, 2014 ☐ Dec 31, 2014 ☐ Mar. 31, 2015 ☐ After Mar. 31, 2015	This is to ensure that malware and other viruses will not acquire user login information and access the site without authorization.

7 Additional Supporting Materials

The following materials and templates provide HICs with support in meeting their obligations. Note that these templates are optional. The HIC is not required to use them. Any templates that the HIC is required to use appear after the relevant policy in Section 4: Policies and Procedures.

HICs participating in the RM&R program

The following HICs contribute PHI to and view PHI from the RM&R Solution:

Long Term Care

Baycrest Centre
Belmont House
Castleview Wychwood Towers
Chester Village Home for the Aged
Christie Gardens
Copernicus Lodge
Dr. Paul & John Rekai Centre
Elm Grove Living Centre
Fairview Nursing Home Ltd.
Fudger House
Garden Court Nursing Home
Hellenic Home for the Aged
Heritage Nursing Home
Isabel & Arthur Meighen Manor
Ivan Franko Home
Kensington Gardens
Lakeshore Lodge
Lakeside Long Term Care Centre
Leisureworld Caregiving Centre - St. George
Leisureworld O'Connor Court
Leisureworld O'Connor Gate
Lincoln Place Nursing Home
Maynard Nursing Home
Mon Sheong Home for the Aged
Nisbet Lodge
Norwood Nursing Home
Providence Centre
Rose of Sharon
St. Clair O'Connor
Suomi Koti Nursing Home
The O'Neil Centre
True Davidson Acres
Vermont Square
Versa-Care Centre
Wellesley Central Place
West Park Long Term Care
White Eagle Nursing Home

Acute Care

Baycrest
Bridgepoint Health
Mount Sinai Hospital
Providence Healthcare
Runnymede Healthcare Centre
Salvation Army Toronto Grace Health Centre
St John's Rehabilitation Hospital
St Joseph's Health Centre
St Michael's Hospital
Sunnybrook Health Sciences Centre
Toronto Central Community Care Access Centre
Toronto East General Hospital
Toronto Rehabilitation Institute
University Health Network
West Park Healthcare Centre

Community Services Sector

Alzheimer Society of Toronto
Better Living Health & Community Services
Community Care East York
Central Neighbourhood House
Dixon Hall
East York Meals on Wheels
Etobicoke Services for Seniors
Family Service Toronto
Good Neighbours' Club
Greek Social Services
Harmony Hall Centre for Seniors
Hospice Toronto
Humber Community Seniors' Services
Les Centres D'Accueil Heritage
Mid-Toronto Community Services
Native Canadian Centre of Toronto
Neighbourhood Link Support Services
Parkdale Golden Age Foundation
Philip Aziz Centre
Second Mile Club of Toronto
SPRINT

Mental Health

Centre for Addiction and Mental Health

St. Christopher House
St. Clair West Services for Seniors
St. Stephen's Community House
Storefront Humber
True Davidson Meals on Wheels
Warden Woods Community Centre
West Toronto Support Services for Seniors
WoodGreen Community Services
Yorkminster Park Meals on Wheels

Inventory of Personal Health Information

The following is an inventory of the types of PHI that are currently contributed to the RM&R Solution. HICs that contribute PHI to the RM&R Solution determine the scope of PHI that they send so the type of PHI that an organization transmits to the RM&R Solution may vary.

Name
Gender
Health Card Number Information
Supplementary Health Card Information
Client ID
Date of Birth/ Age
Marital Status
Patient Phone Number
Permanent Address (including postal code, telephone number, treatment address)
First Nations
Next of Kin
Faith and Religion
Ethno-cultural Preference
Medical Record Number
Social Situation Details
Living Situation
Preferred Accommodation
Emergency Contact
Alternate Contacts (POA Personal Care and Financial Affairs, SDM, non-legal contacts)
Primary Language
Interpreter Required
Preferred Language
Family Aware of Diagnosis/ Prognosis
Health Insurance Information
Responsibility for Payment (e.g. OHIP, Insurance Plan)
Community Primary Health Care Providers
Physician Information (Hospital)
Family Physician Information (Community)
Pharmacy Information
Last Visit Information
Referred By Information
Precautions/ Risks (to patient and/or provider)
Occupational History
Surgical History
History of Falls Information
Current Medications
Current Treatments/ Special Needs
Current Diet
Vision Information
Hearing Information
Speech Information
Respiratory Information
Mobility/ Ambulation Information
Height
Weight
Medical Health Report
Primary Diagnosis
Cancer Diagnosis
Co-morbidities
Palliative Performance Scale
Chronic Pain
Alzheimer, Dementia Diagnosis
Reason for Referral
Date of Referral
Service Requested (e.g. Community, CNAP)
Urgency Requirements of Admission
Services Currently Receiving
Estimated Date of Discharge/ Discharge Date
Goals of Care (e.g. convalescent care goals, rehabilitation goals)
Medical Order
Medication Administration Information
Wound Care
FARM Status
Client Choice Information
Resuscitation Status
Special Care Needs
Rehab/ CCC Population Requested (e.g. ABI, Amputee, Burns)
Alternate Level of Care Status Information
Dietitian Report (nutrition history, nutrition intervention, goals of nutrition care)
Nursing Intervention Information

Physical and Mental Health, Surgical, Family, Social Condition
Drug Sensitivities, Allergies, Addictions
Infection Control
Substance abuse History
Psychiatric History
Mental Health and Addiction Services
Tracheostomy
IV
Oxygen
Enteral Feed
Dialysis
Equipment Needs
Bladder Management
Bowel Management
Ostomy
Feeding Requirements
Dietary Needs
A patient's instructions to block healthcare providers and staff from viewing their personal health information in the information system
Implied/ expressed consent for CNAP application
Consent for placement to Convalescent Care
Consent for placement to Long Term Care
Consent/ Evaluator Questionnaire (Capacity Assessment)
Occupational Therapy (functional status, suggested community goals)
Physiotherapy Report (surgical procedure, home therapy program, ambulation details)
Social Work Intervention Information
Speech Language Pathology Information (communication and/or swallowing disorders, hearing, assessments, therapy)
Doctor's notes on images such as x-rays, MRI, CT scan
Chest X ray (date, result, action taken)
Smoking Assessment
Behavioral Assessment
Symptom Assessment (Edmonton Symptom Assessment System score)
Functional Assessment
Respiratory Assessment
Excretion Assessment
Cognitive Status (Rancho Los Amigos Cognitive Scale Score)
Ambulatory Status
Weight Bearing Status
Assessment of Patient Capability
Palliative Performance Scale
Eligibility for Convalescent Admission Assessment
Eligibility for Long Term Care Admission Assessment
Eligibility for Respite Care Admission Assessment

Notice of Purposes

Information Practices Notification Sample Including Updated Notice of Purposes

INFORMATION PRACTICES NOTIFICATION

NOTE TO USERS OF THIS NOTIFICATION POSTER:

The language in this poster is a sample only. Please ensure that all details are carefully reviewed and updated (as required) to reflect all of the possible uses and disclosures of PHI at your organization. In addition, please ensure that the applicable processes of your organization are appropriately described.

Our Privacy Commitment

At **[*insert organization name*]**, your personal health information is treated with respect and sensitivity, in accordance with the Ontario Personal Health Information Protection Act and all other applicable laws.

We collect your personal health information from you or a person acting on your behalf. We may also collect personal health information about you from other sources if we have obtained your consent to do so or if the law permits. The personal health information that we collect may include, for example, your contact information, medical history, records of the care you received during prior visits to our organization or to other organizations. The people at **[*insert organization name*]** who provide and support your care are allowed to see your health information.

Once we have collected your personal health information, we (sample language below):

- take steps to protect it from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal
- conduct audits and complete investigations to monitor and manage our privacy compliance
- take steps to ensure that everyone who performs services for us protects your privacy and only uses your personal health information for the purposes you have consented to

Uses and Disclosures of Personal Health Information

We use and share your personal health information as is necessary to (sample language below):

- provide you with healthcare
- get payment for your treatment and care (from OHIP, or with your consent from your private insurer or others);
- make our health services better and more efficient;
- Teach;
- conduct research; and
- comply with legal and regulatory requirements.

We may share your health information with other healthcare providers to continue to care for you. This includes healthcare providers at other organizations who can view your information through shared electronic systems/databases to continue to care for you.

We sometimes also share your personal health information with (sample language below):

- Health regulatory agencies (for example, agencies that track wait times)
- Public authorities as permitted and required by law (for example, Public Health to track infections)

We would share your personal health information with another person that you ask us or give your consent to share with.

In order to provide you with the best care or treatment, we sometimes collect health information about you from other healthcare organizations using electronic systems. We sometimes also use these electronic systems to share your information with other healthcare organizations in order to support them in providing you with care.

Your Rights

We respect your right to see and, if necessary, correct your personal health record. To do so, speak to your care provider or contact our **[*insert department name*]** at **[*insert contact information*]**.

You may also choose to withdraw your consent (subject to legal exceptions) for some of the above uses and disclosures. To do this, contact our **[insert department name]**.

How to Contact Our [*insert department name*]

If you have questions or concerns, contact the **[*insert organization name*] [*insert department name*]** at:

Telephone: **[*insert Contact telephone number*]**, Email: **[*insert Contact email*]**

How to Contact Our Privacy Office

If you have questions or concerns, contact the **[*insert organization name*]** Privacy Office at:

Telephone: **[*insert organization's Privacy Contact telephone number*]**, Email: **[*insert organization's Privacy Contact email*]**

For inquiries and requests related to your PHI regional or provincial systems, please contact the following (sample language below –update as more information becomes available)**:**

For information about your referrals contact: **Resource Matching and Referral (RM&R)** at referrals@uhn.ca, or telephone at 416-340-4030 or Toll-Free at: 1- 844-653-1240

For information about your regional electronic health contact: **ConnectingGTA (cGTA)** at tbd

For information about your laboratory results contact: **Ontario Laboratories Information System (OLIS)** please call the Service Desk/ONE Support at 1-866-250-1554 or email at servicedesk@ehealthontario.on.ca

For information about your diagnostic imaging within LHINs 5, 6, 7, 12 and parts of LHIN 8 contact: **GTA West Document Imaging Repository (GTA West DI-r)** by telephone at 416-340-4030 or Toll-Free at: 1-844-653-1240.

For information about your eHealth Ontario managed diagnostic imaging repository across all of Ontario contact: **Document Imaging Common Services (DI CS)** at tbd

For information about your electronic assessments contact: **Integrated Assessment Record (IAR)** by email at iar@ccim.on.ca, or telephone at 1-866-909-5600

Further questions and concerns may be directed to the Ontario Information and Privacy Commissioner at:

Ontario Information and Privacy Commissioner
2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8
Telephone: **416-356-3333** Website: **www.ipc.on.ca**

Notice of Purposes Addition to Information Notice

The following statement can be added to a HIC's Notice of Purpose to address the information requirements in the Consent Management Policy to support and enhance what is already required by *PHIPA, 2004* and guidance from Information and Privacy Commissioner of Ontario. The following statement would be put into the section describing how your HIC uses and discloses PHI:

> We may share your health information with other healthcare providers to continue to care for you. This includes healthcare providers at other organizations who can view your information through shared electronic systems/databases to continue to care for you.